Problem 1 (Section 1.2, Exercise 12)**.** Show that both cancellation laws hold in a group. That is, $ax = ay \implies x = y$ and $xa = ya \implies x = y$. Show that any finite semigroup in which both cancellation laws hold is a group.

Proof. Before beginning, we'll need a claim.

Claim 1. Let X be a set such that $|X| < \infty$. If $f : X \to X$ is a well-defined function such that f is injective, then it is bijective.

Proof. For it to be bijective, we need f to also be surjective. Assume for contradiction that f is *not* surjective. Then there is at least one $y \in X$ such that $f(x) \neq y$ for all $x \in X$. Since the set is finite, and the codomain and the domain are the same, we use the Pidgeonhole principle to deduce that there must be $x_1, x_2 \in X$ so that $x_1 \neq x_2$, $f(x_1) = f(x_2)$. But this then contradicts our assumption that f is injective; hence, we must have that f is surjective, and so bijective. □

We first start with showing that both cancellation laws hold in a group. Let G be our group, and take $a, x, y \in G$. Assume that we have $ax = ay$. Then since we are in a group, there exists an $a^{-1} \in G$. Multiplying to the left, we have

$$a^{-1}(ax) = a^{-1}(ay).$$

Associativity then gives

$$(a^{-1}a)x = (a^{-1}a)y.$$

Since a^{-1} is an inverse, we have $a^{-1}a = e$, where $e \in G$ is the identity element. So we rewrite this as

$$ex = x = y = ey.$$

So we have the cancellation law; that is, $ax = ay \implies x = y$. Doing the same operations on the right gives us the same result; that is, multiplying a^{-1} to the right, we have

$$(xa)a^{-1} = x(aa^{-1}) = x = y = y(aa^{-1}) = (ya)a^{-1}.$$

We now need to show that any finite semigroup in which *both* cancellation laws hold is a group. Let S be a finite semigroup satisfying this. We would like to first establish that there is an identity element; i.e. an element e such that

$$ae = ea = a$$

for all $a \in S$. Fix arbitrary $a \in S$, and let $f_a : S \to S$ be a function where

$$f_a(b) = ab.$$

We see that this functions is well defined, since if $c = b$ then

$$f_a(c) = ac = ab = f_a(b).$$

We also see that the function is injective, since

$$f_a(b) = f_a(c) \leftrightarrow ab = ac,$$

and the left cancellation law tells us that $b = c$. Thus, $f_a : S \to S$ must be a bijection by **Claim 1**, since $|S| < \infty$. Therefore, we have that there is a $e_a \in S$ so that $f_a(e_a) = a$, or $ae_a = a$. Now, take $b \in S$ arbitrarily. We have that

$$ab = (ae_a)b = a(e_a b),$$

and so the left cancellation law gives

$$b = e_a b$$

for all $b \in S$. In particular, taking $b = a$, we have

$$ae_a = e_a a = a.$$

Finally, take $c \in S$ arbitrarily again. Then we have

$$cb = c(e_a b) = (ce_a)b,$$

and so

$$c = ce_a$$

by the right cancellation law. Since this works for all $c \in S$, we have that e_a is a left and right identity for all $x \in S$. Hence, it is an identity element, and we can rewrite it as e. Thus, we have S is a monoid.

To get that S is a group, we need to establish that every element admits an inverse. Again, let $f_a : S \to S$ be the function

$$f_a(b) = ab.$$

Since this is a bijection, we have that there is some element $b \in S$ so that

$$f_a(b) = ab = e.$$

Denoting $b = a_R^{-1}$, we have that every element admits a right inverse. Letting $g_a : S \to S$ be the function

$$g_a(b) = ba,$$

we can analogously get that every element admits a left inverse, a_L^{-1} (the argument that this is a bijection is the same as the argument for f_a, except we flip multiplication and use the right cancellation law). We then want to establish that

$$a_L^{-1} = a_R^{-1}.$$

To see this, notice that

$$a_L^{-1} = a_L^{-1}(aa_R^{-1}).$$

By associativity, we can rewrite this as

$$a_L^{-1}(aa_R^{-1}) = (a_L^{-1}a)a_R^{-1} = a_R^{-1}.$$

So we have

$$a_L^{-1} = a_R^{-1} = a^{-1},$$

as desired. Since this works for arbitrary $a \in S$, we get that every element has an inverse. Since every element admits an inverse and we have an identity, we get that S must be a group. □

Problem 2 (Section 1.3, Exercise 4)**.** Is the additive group of integers, $(\mathbb{Z}, +, 0)$, isomorphic to the additive group of rationals, $(\mathbb{Q}, +, 0)$?

Proof. Assume that we could find a homomorphism $f : \mathbb{Z} \to \mathbb{Q}$ which is bijective. Then, in particular, we have that there is a rational number p/q such that

$$f(1) = \frac{p}{q}.$$

Now, we have that

$$f(n) = f(1 + 1 + \cdots + 1) = f(1) + \cdots + f(1) = nf(1) = \frac{np}{q}$$

for all positive integers n using the homomorphism property of f. So this says that every positive rational number can be expressed by an integer multiple of p/q. But this is not the case; take, for example, $p/(2q)$. Then we have that n satisfies

$$\frac{np}{q} = \frac{p}{2q} \leftrightarrow 2n = 1,$$

but this forces $n = 1/2$, a contradiction. So there is no such isomorphism. Furthermore, this tells us that $(\mathbb{Q}, +, 0)$ is not a cyclic group, since all infinite cyclic groups are isomorphic to $(\mathbb{Z}, +, 0)$. $\square$

Problem 3 (Section 1.4, Exercise 3)**.** Show that any group in which every a satisfies $a^2 = 1$ is abelian. What if $a^3 = 1$ for every a?

Proof. If $a^2 = 1$ for all $a \in G$, then in particular we have that

$$(ab)^2 = 1$$

for all $a, b \in G$. That is, we have

$$ab = b^{-1}a^{-1}.$$

But $b^2 = 1$ implies that $b = b^{-1}$ (multiply b^{-1} to the left of both sides), and $a^2 = 1$ implies $a = a^{-1}$ (multiply a^{-1} to the left of both sides), so we get that

$$ab = ba.$$

Thus, the group is commutative.

Consider the group

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \ : \ a, b, c \in \mathbb{Z}/3\mathbb{Z} \right\}$$

under matrix multiplication, where the coefficients are in $\mathbb{Z}/3\mathbb{Z}$.First, let's see that this is indeed a group. Notice that we have the natural identity, I_n, inherited from normal matrix multiplication. Next, notice that it's closed under multiplication. Finally, notice that there are inverses; we have

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a + a' & b' + ac' + b \\ 0 & 1 & c' + c \\ 0 & 0 & 1 \end{pmatrix}.$$

Setting $a' = -a$, $c' = -c$, and solving

$$b' + ac' + b = 0,$$

we get

$$b' = ac - b.$$

So our inverse is then

$$\begin{pmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

So it satisfies all of the axioms to be a group, and we're done.

Next, we see that, for arbitrary $M \in G$, we have

$$M^3 = \begin{pmatrix} 1 & 3a & 3ac + 3b \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix},$$

which, after taking these coefficients mod 3, gives us

$$M^3 = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

So every element cubes to the identity; however, examining

$$M = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

we have

$$MQ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix},$$

$$QM = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix},$$

so

$$MQ \neq QM.$$

Thus, the group is *not* commutative. □

Problem 4 (Section 1.5, Exercise 1)**.** Let $C(A)$ denote the centralizer of the subset A of a monoid M. That is, let

$$C(A) = \{b \in M \ : \ ab = ba \text{ for all } a \in A\}.$$

Note that

$$A \subset C(C(A)), \tag{1}$$

and if $A \subset B$, then

$$C(B) \subset C(A). \tag{2}$$

Show that these imply that

$$C(C(C(A))) = C(A).$$

Without using the explicit form of the elements of $\langle A \rangle$, show that $C(A) = C(\langle A \rangle)$.
Use this to show that if a monoid is generated by a set of elements A which pair-wise commute, then the monoid is commutative.

Proof. Throughout, we implicitly use the fact that $C(A)$ is a submonoid of M, where $A \subset M$ is a subset. This can be found in **Section 1.4, pg. 41** of Jacobson.

To see (1), take $a \in A$ and notice that, for all $b \in C(A)$, we have $ab = ba$ by definition of $C(A)$. Hence, $a \in C(C(A))$. Since the choice of a was arbitrary, we get $A \subset C(C(A))$; that is, (1) holds.

To see (2), take $a \in C(B)$. Then we have for all $b \in B$, $ab = ba$. But, since $A \subset B$, we get that for all $b \in A$ we have $ab = ba$. Hence, $a \in C(A)$. Since the choice of a was arbitrary, we get $C(B) \subset C(A)$.

Notice that (1) and (2) tells us that

$$C(C(C(A))) \subset C(A).$$

Replacing A in (1) by $C(A)$, we have that

$$C(A) \subset C(C(C(A))),$$

and so we have

$$C(C(C(A))) = C(A). \tag{3}$$

Let $c \in C(A)$. Then $A \subset C(c)$ by construction, since $ca = ac$ for all $a \in A$. Thus, $\langle A \rangle \subset C(c)$, since $\langle A \rangle$ is the smallest submonoid which contains A. Since this works for all $c \in C(A)$, we have

$$\langle A \rangle \subset \bigcap_{c \in C(A)} C(c) = C(C(A)),$$

which, using (2) and (3), tells us that

$$C(A) = C(C(C(A))) \subset C(\langle A \rangle).$$

By definition, we have

$$A \subset \langle A \rangle,$$

so (2) tells us that

$$C(\langle A \rangle) \subset C(A).$$

Coupling these facts together, we get

$$C(\langle A \rangle) = C(A).$$

Let $M = \langle A \rangle$. The statement says that $A \subset C(A)$, since given $a \in A$, $b \in A$, we have $ab = ba$, and since the choice of b is arbitrary we get $a \in C(A)$. Therefore we have

$$C(A) = C(\langle A \rangle) = C(M),$$

and so $A \subset C(M)$. Hence, $\langle A \rangle \subset C(M)$ by minimality again, and since $\langle A \rangle = M$, this then tells us that $M \subset C(M)$. Therefore, M must be commutative, since given any $a \in M$, $b \in M$, we have that $a \in C(M)$, and so $ab = ba$. □

Problem 5 (Section 1.5, Exercise 4)**.** Show that if g is an element of a group and $o(g) = n$ then g^k, $k \neq 0$, has order $[n, k]/k = n/(n, k)$. Show that the number of generators of $\langle g \rangle$ is the number of positive integers less than n which are relatively prime to n. This number is denoted by $\varphi(n)$ and φ is called the *Euler φ-function.*

Remark. Throughout, we implicitly use the fact that, for cyclic groups, the order of the group is the exponent of the group. This statement is proven in **Theorem 1.4** in Jacobson. We also implicitly use power rules, which are both in Jacobson and Lang, as well as explained in the lecture notes

Proof. Note that $[m, n]$ is the *least common multiple* (lcm) of m and n and (m, n) is the *greatest common divisor* (gcd) of m and n. From earlier in Jacobson, we note that

$$kn = [k, n](k, n). \tag{4}$$

Notice as well that

$$(g^k)^{n/(k,n)} = (g^n)^{k/(k,n)} = e^{k/(k,n)} = e,$$

so we must have that

$$o(g^k) \leq \frac{n}{(k, n)},$$

since $\langle g^k \rangle$ is a cyclic subgroup and so it's order is it's exponent, which is the smallest positive integer power which kills g^k.

Now, suppose that we have an m such that

$$(g^k)^m = g^{km} = e.$$

Then since n is the order of $\langle g \rangle$, and hence the exponent, the division algorithm gives us that

$$n \mid km.$$

That is, since n is the exponent, we have that n is the smallest integer such that $g^n = e$, and so $n \leq km$. Using the division algorithm, we have $km = qn + r$, q a positive integer and $0 \leq r < n$ an integer. If $r \neq 0$, we have that power rules give us

$$g^{km} = g^{qn} g^r = e g^r = g^r = e,$$

so r is a smaller integer than n which kills g, contradicting the minimality of n. Hence, $n \mid km$.

Dividing both sides by (k,n), we have

$$\frac{n}{(k,n)} \mid \frac{k}{(k,n)}m.$$

Notice that $\gcd(n/(k,n), k/(k,n)) = 1$. If we consider the case where $\gcd(n/(k,n), k/(k,n)) = d > 1$, we have that $d(k,n) \mid n$, $d(k,n) \mid k$, and $d(k,n) > (k,n)$, a contradiction of the maximality of (k,n). So, we must have that

$$\frac{n}{(k,n)} \mid m \leftrightarrow \frac{n}{(k,n)} \leq m.$$

Therefore, since this worked for all m which satisfies $(g^k)^m = e$, we can take $m = o(g^k)$ to get

$$\frac{n}{(k,n)} \leq o(g^k) \implies \frac{n}{(k,n)} = o(g^k).$$

From (4), we see that

$$o(g^k) = \frac{n}{(k,n)} = \frac{[k,n]}{k}.$$

Now, if $\langle g^k \rangle$ is a generator for $\langle g \rangle$, we must have that $o(g^k) = o(g) = n$. By what we've just shown, this can only happen if $(k,n) = 1$. So the number of generators of $\langle g \rangle$ is the number of positive integers less than n which are relatively prime to n. $\square$

Problem 6 (Section 1.6, Exercise 4)**.** Show that if α is any permutation, then

$$\alpha(i_1, \ldots, i_r)\alpha^{-1} = (\alpha(i_1), \ldots, \alpha(i_r)).$$

Proof. Let J be the underlying set where these elements are being shifted around. Let $x \in J$. We consider some cases.

- Let $x \in \{i_1, \ldots, i_r\}$ and assume α fixes x (that is, $\alpha^{-1}(x) \in \{i_1, \ldots, i_r\}$). If α fixes x, then we have that $(i_1, \ldots, i_r)\alpha^{-1}(x) = i_k$ for some $1 \leq k \leq r$. So $\alpha(i_1, \ldots, i_r)\alpha^{-1}(x) = \alpha(i_k)$.
- If α does not fix x, consider the case where $\alpha^{-1}(x) \notin \{i_1, \ldots, i_r\}$. Then we have that $(i_1, \ldots, i_r)\alpha^{-1}(x) = \alpha^{-1}(x)$, and so applying α to the left gives x. So we see that $\alpha(i_1, \ldots, i_r)\alpha^{-1}$ fixes x.
- If α does not fix x, consider the case where $\alpha^{-1}(x) = i_{k-1} \in \{i_1, \ldots, i_r\}$, $2 \leq k \leq r+1$. Then we have that $(i_1, \ldots, i_r)\alpha^{-1}(x) = i_k$, and so $\alpha(i_1, \ldots, i_r)\alpha^{-1}(x) = \alpha(i_k)$.
- Finally, if $x \notin \{i_1, \ldots, i_r\}$ and α fixes x, it's clear that $\alpha(i_1, \ldots, i_r)\alpha^{-1}(x) = x$.

Using these properties, we can do the cycle decomposition of $\sigma = \alpha(i_1, \ldots, i_r)\alpha^{-1}$. It is all dependent on whether $\alpha^{-1}(x) \in \{i_1, \ldots, i_r\}$, and for this to happen we need $x = \alpha(i_k)$. We see then that $\sigma(\alpha(i_1)) = \alpha(i_2)$, $\sigma^2(\alpha(i_1)) = \alpha(i_3)$, and so on until we get to $\alpha(i_r)$, in which we see that $\sigma(\alpha(i_r)) = \alpha(i_1)$. Hence, it is a cycle, and it can be written as

$$\alpha(i_1, \ldots, i_r)\alpha^{-1} = \sigma = (\alpha(i_1), \ldots, \alpha(i_r)).$$

□

Problem 7 (Section 1.7, Exercise 4)**.** Let G be a finitely generated group, H a subgroup of finite index. Show that H is finitely generated.

Proof. Let $G = \langle S \rangle$, $S = \{x_1, \ldots, x_r\}$. Then

$$G = \bigsqcup_{i=1}^{n} y_i H,$$

where the y_i are taken to be representatives of the cosets. Take $y_1 = 1$ without loss of generality. Since the $x_i \in G$ by assumption, we get that $x_i y_j \in y_{k_{i,j}} H$ for all i, j, and hence there is an $h_{i,j}$ so that

$$x_i y_j = y_{k_{i,j}} h_{i,j}.$$

Now, take $h \in H$. We have that

$$h = x_{l_1} \cdots x_{l_v}.$$

Notice that

$$x_{l_v} = y_{k_{1,l_v}} h_{l_v,1}.$$

So we can rewrite this as

$$h = x_{l_1} \cdots x_{l_{v-1}} y_{k_{1,l_v}} h_{l_v,1}.$$

We now examine

$$x_{l_{v-1}} y_{k_{1,l_v}} = y_{k_{l_{v-1},k_{1,l_v}}} h_{l_{v-1},k_{1,l_v}}.$$

We can continue replacing these generators, and after relabeling we get

$$h = y \cdot h_{l_1} \cdots h_{l_v}.$$

Since $h \in H$, we get that $y = 1$, and so we have

$$h = h_{l_1} \cdots h_{l_v}.$$

So taking the set

$$S' = \{h_{1,1}, \ldots, h_{r,n}\},$$

we see that

$$\langle S' \rangle = H.$$

Hence, H is finitely generated. □

Problem 8 (Section 1.7, Exercise 6)**.** Let H be a subgroup of the finite group G. Show that there exists a subset $\{z_1, \ldots, z_r\}$ of G which is simultaneously a set of representatives of the left and of the right cosets of H in G, that is, G is a disjoint union of the z_iH and also of the Hz_i, $1 \leq i \leq r$.

Proof. We proceed via the hint. Take $g \in G$. We can write

$$HgH = \bigsqcup_1^s x_j gH,$$

where $x_j \in H$ and $x_j gH \cap x_r gH = \varnothing$ if $j \neq r$. To see this, notice that

$$HgH = \bigcup_{h \in H} hgH.$$

Furthermore, take $x_j, x_r \in H$, and examine $y \in x_j gH \cap x_r gH$. We have that

$$y = x_j g h_1 = x_r g h_2,$$

and so we can rewrite this as

$$x_j g h_1 h_2^{-1} = x_r g,$$

and letting $h = h_1 h_2^{-1}$, we have

$$x_j g h = x_r g.$$

So

$$x_r gH = (x_j gh)H = (x_j g)(hH) = x_j gH.$$

So if they are not disjoint, they are identical. Thus, we can partition the space in a way similar to cosets.

In a way analogous to cosets, we have the inverse map gives us a bijection between left partitions and right partitions, and so there are s right partitions of HgH; that is, there are $y_k \in H$ so that

$$HgH = \bigsqcup_1^s Hgy_j.$$

Let $z_j = x_j g y_j$. We'd like to establish that

$$HgH = \bigcup z_j H = \bigcup Hz_j.$$

But this follows, since

$$\bigcup z_j H = \bigcup x_j g y_j H = \bigcup x_j gH = HgH,$$

and likewise

$$\bigcup Hz_j = \bigcup Hx_j g y_j = \bigcup Hgy_j = HgH.$$

Furthermore, the disjointness follows from the disjointness of the x_j and y_j, so this is a collection of representatives of the left cosets and right cosets. Do this process for every representative coset gH to get

$$HGH = G = \bigcup z_j H = \bigcup Hz_j,$$

so the collection $\{z_j\}$ is a set of representatives of both left and right cosets. □

Problem 9 (Section 1.8, Exercise 4)**.** Show that a subgroup of index two is normal. Hence, prove that A_n is normal in S_n.

Proof. We can write $G = H \sqcup gH$, where $g \notin H$, since this has index 2. Thus, we have that $gH = G - H$; that is, the set of elements in G which are not in H. Notice as well, though that we can write this in terms of right cosets, so that $G = H \sqcup Hg$. Hence, again, $Hg = G - H$, but this tells us that $gH = Hg$. Multiplying by g^{-1} on the right gives $gHg^{-1} = H$, or that H is a normal subgroup.

From lecture, we have that $|A_n| = |S_n|/2$. So $[S_n : A_n] = |S_n|/|A_n| = 2$, and by prior work it must be normal. □

Problem 10 (Section 1.8, Exercise 11)**.** Let G be a group of order $2k$, where k is odd. Show that G contains a subgroup of index 2.

Proof. The hint says to use a prior exercise.

Claim 2. A group of even order contains an nontrivial element a such that $a^2 = 1$.

Proof. Consider the map $\varphi : G \to G$ such that $\varphi(x) = x^2$. We see that $\varphi(e) = e$ and that this function is well defined, since $x = y$ implies that

$$\varphi(x) = x^2 = y^2 = \varphi(y).$$

Examine $\ker(\varphi) = \{y \in G \ : \ \varphi(y) = e\}$. We have that $|\ker(\varphi)| \geq 1$. If $|\ker(\varphi)| = 1$, then this says that every element other than the identity has a unique inverse. However, notice that this implies that the order of the group will be odd, since this says that for all $g \in G$ we have $g \neq g^{-1}$, and so we can write $|G| = 2k + 1$, where k is the number of non-identity elements. This is a contradiction to the fact that $|G|$ is even, and so therefore we must have $|\ker(\varphi)| > 1$; that is, there is some $y \in G$ so that $y^2 = e$, or $y = y^{-1}$. □

Claim 3. Let $\varphi : G \to K$ be a homomorphism of groups. Then

$$\ker(\varphi) = \{g \in G \ : \ \varphi(e) = e_K\}$$

is a subgroup of G.

Proof. We see $e \in \ker(\varphi)$, since $\varphi(e) = e_K$. Next, take $x, y \in \ker(\varphi)$, then we have $xy^{-1} \in \ker(\varphi)$, since

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e_K e_K^{-1} = e_k.$$

Hence, $\ker(\varphi)$ is a subgroup. □

Claim 4. A composition of homomorphisms $\varphi : G \to H$ and $\kappa : H \to K$ is a homomorphism from G to K.

Proof. Let $\gamma : G \to K$ be defined by $\gamma = \kappa \circ \varphi$. Then, for all $x, y \in G$, we have

$$\gamma(xy) = \kappa(\varphi(xy)) = \kappa(\varphi(x)\varphi(y)) = \kappa(\varphi(x))\kappa(\varphi(y)) = \gamma(x)\gamma(y).$$

So γ is indeed a homomorphism. □

Let $G_L = \{\varphi_g \in M(G) \ : \ \varphi_g(x) = gx \ \forall x \in G\}$. This is the **transformation group of left translations**, as defined on pg. 52 of Jacobson.

Claim 5. We have that $G_L \leq S_G$; that is, it is a subgroup of the space of all bijections from G to itself.

Proof. We have $\mathrm{Id} = \varphi_e \in G_L$. Take $\varphi_x \in G_L$. Then we see that $\varphi_x^{-1} = \varphi_{x^{-1}}$, since

$$\varphi_x \circ \varphi_{x^{-1}}(y) = xx^{-1}y = y = \mathrm{Id}(y) = x^{-1}xy = \varphi_{x^{-1}} \circ \varphi_x(y).$$

Furthermore, we have $\varphi_x \circ \varphi_y = \varphi_{xy}$, since

$$\varphi_x \circ \varphi_y(g) = xyg = \varphi_{xy}(g),$$

and so G_L is closed under multiplication, inverses, and has an identity. Therefore, it is a subgroup. □

Define $\kappa : G \to G_L$ via $\kappa(g) = \varphi_g$. We see that κ is an isomorphism. Clearly κ is well defined, since $x = y$ implies that

$$\kappa(x) = \varphi_x = \varphi_y = \kappa(y).$$

It is also clearly surjective, since for all $\varphi_g \in G_L$ we have $\kappa(g) = \varphi_g$. We also see injectivity by noticing that

$$\kappa(x) = \kappa(y) \leftrightarrow \varphi_x = \varphi_y \leftrightarrow xg = yg \text{ for all } g \in G \leftrightarrow x = y.$$

Finally, it is a homomorphism, since

$$\kappa(xy) = \varphi_{xy} = \varphi_x \circ \varphi_y = \kappa(x) \circ \kappa(y).$$

So we have $G \cong G_L \leq S_G$. Recall that $\psi : S_G \to \{-1, 1\}$, where we equip $\{-1, 1\}$ with multiplication and $\psi(\sigma) = 1$ if σ is even and $\psi(\sigma) = -1$ is σ is odd, is a homomorphism (this is by the lecture notes). So we have a homomorphism $\gamma = \psi \circ \kappa : G \to \{-1, 1\}$ by **Claim 3**, and $H = \ker(\gamma) \leq G$ a subgroup by **Claim 2**. By **Claim 1**, we have a non-trivial element $g \in G$ with order 2. We would like to establish that $\gamma(g) = -1$. To do so, we need to see that $\kappa(g) = \varphi_g$ is a product of an odd number of transpositions. Take $x, y \in G$ such that $\varphi_g(x) = gx = y$. Then we have $\varphi_g(y) = x$, since

$$gy = g(gx) = g^2x = x.$$

Notice that φ_g is a bijection as well, and so we can write it as a product of $|G|/2 = k$ transpositions. Since we assumed k was odd, we get that $\gamma(g) = -1$, and so $\gamma : G \to \{-1, 1\}$ is a surjection.

Claim 6. Let $\varphi : G \to K$ be a homomorphism. Then $\ker(\varphi)$ is a normal subgroup.

Proof. **Claim 2** establishes that it is a subgroup. To see that it is normal, we need to show that

$$g \ker(\varphi) g^{-1} \subseteq \ker(\varphi).$$

Notice that for all $g \in G$, $k \in \ker(\varphi)$, we have

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e_K.$$

So $gkg^{-1} \in \ker(\varphi)$, establishing that this is normal. □

Claim 7. A homomorphism $\varphi : G \to K$ is injective if and only if it's kernel is trivial.

Proof. ($\implies$) Assume φ is injective. Then

$$\ker(\varphi) = \{g \in G \ : \ \varphi(g) = e\}.$$

But we see that $\varphi(g) = e = \varphi(e)$ implies $g = e$, and so $\ker(\varphi) = \{e\}$.
($\impliedby$) Assume $\ker(\varphi)$ is trivial. Take $\varphi(g) = \varphi(h)$. Then we have

$$\varphi(g)\varphi(h)^{-1} = \varphi(gh^{-1}) = e \leftrightarrow gh^{-1} = e \leftrightarrow g = h,$$

and so φ is injective. □

Claim 8 (First Isomorphism Theorem)**.** If $\gamma : G \to K$ is a surjective homomorphism, then we have that $G/\ker(\gamma) \cong K$.

Proof. **Claim 5** establishes that $G/\ker(\gamma)$ is indeed a group (see quotient group pg. 56 in Jacobson). Let $f : G/\ker(\gamma) \to K$ via $f(g\ker(\gamma)) = \gamma(g)$. This map is well defined, since if $g\ker(\gamma) = g'\ker(\gamma)$, we have that $g'k = g$ for some $k \in \ker(\gamma)$, and so

$$f(g\ker(\gamma)) = \gamma(g) = \gamma(g'k) = \gamma(g') = f(g'\ker(\gamma)).$$

We see it is a homomorphism, since

$$f(g\ker(\gamma)h\ker(\gamma)) = f(gh\ker(\gamma)),$$

since $\ker(\gamma)$ is normal, and

$$f(gh\ker(\gamma)) = \gamma(gh) = \gamma(g)\gamma(h) = f(g\ker(\gamma))f(h\ker(\gamma)).$$

We see that f is clearly injective, since it's kernel must be trivial. That is, if $f(g\ker(\gamma)) = e$, then we have $\gamma(g) = e$, but this implies that $g \in \ker(\gamma)$ and so $g\ker(\gamma) = \ker(\gamma)$. Finally, the map is surjective, since for all $k \in K$ we have a $g \in G$ so that $\gamma(g) = k$, which is hit by $f(g\ker(\gamma))$. □

Using **Claim 7**, we get that $G/\ker(\gamma) \cong \{-1, 1\}$, or in other words that $[G : \ker(\gamma)] = 2$. Thus, we have found a group of order 2.

□

Problem 11 (Section 1.9, Exercise 3)**.** Show that $a \mapsto a^{-1}$ is an automorphism of a group G if and only if G is abelian, and if G is abelian, then $a \mapsto a^k$ is an endomorphism for every $k \in \mathbb{Z}$.

Proof. ($\implies$) Assume that $f(a) = a^{-1}$ is an automorphism on G. Then we would like to show that for all $a, b \in G$, we have $ab = ba$. Notice that for all $a, b \in G$, we have that the automorphism property gives us

$$ab = f(a^{-1})f(b^{-1}) = f(a^{-1}b^{-1}) = (a^{-1}b^{-1})^{-1} = ba$$

for all $a, b \in G$. Hence, the group G is abelian.
($\impliedby$) Assume that G is abelian. Then we would like to show that $f : G \to G$ defined by $f(a) = a^{-1}$ is an automorphism. To do so, we show that f is well-defined, injective, surjective, and a homomorphism. First, let's see well-defined; take $a = b$, then we see that

$$a^{-1}b = a^{-1}a = e = b^{-1}b,$$

so $a^{-1} = b^{-1}$, and hence $f(a) = f(b)$. To see injective, if $f(a) = f(b)$, we have $a^{-1} = b^{-1}$. Notice that

$$aa^{-1} = e = ba^{-1},$$

and so we see $a = b$. Hence, the function is injective. For surjectivity, since G is closed under inverses, we have that for all $g \in G$, $g^{-1} \in G$, and so we see $f(g^{-1}) = g$. Finally, we need to see that the function is a homomorphism. That is, for all $a, b \in G$, we need to see that $f(ab) = f(a)f(b)$. Notice that, since G is abelian, we have $ab = ba$, or in other words $a^{-1}b^{-1} = b^{-1}a^{-1} = (ab)^{-1}$, and so we have

$$f(a)f(b) = a^{-1}b^{-1} = (ab)^{-1} = f(ab),$$

and hence this is an automorphism.

Finally, assume that G is abelian. We want to establish that $g : G \to G$ defined by $g(a) = a^k$ is an endomorphism for every $k \in \mathbb{Z}$. To do so, we need to show it's well-defined, surjective, and a homomorphism. For well-defined, if $a = b$, then $a^k = b^k$ clearly, and so we have $g(a) = g(b)$. For surjective, we take $h \in G$, and we notice that $h^{-k+1} \in G$ such that $g(h^{-k+1}) = h^{-k+k+1} = h$. Hence, the function is surjective. Finally, we need to show that for all $a, b \in G$, we have $f(ab) = f(a)f(b)$. To do so, we establish a claim.

Claim 9. If G is an abelian group, then $(ab)^k = a^k b^k$ for every $k \in \mathbb{Z}$.

Proof. To establish this, let's first take $k \in \mathbb{Z}_{\geq 0}$. The case $k = 1, 0$ is trivial (for $k = 0$, we have $(ab)^0 = e = a^0 b^0$, and for $k = 1$ we have $(ab)^1 = ab = a^1 b^1$). For $k \geq 2$, we proceed by induction. We first show the base case for $k = 2$; that is,

$$(ab)^2 = a^2 b^2.$$

To see this, notice that

$$(ab)^2 = abab.$$

Now, since G is abelian, we have $ba = ab$, and so we can rewrite this as

$$(ab)^2 = a(ba)b = a(ab)b = a^2 b^2,$$

and so we are done. Now, assume it holds for $k - 1$. That is, we have

$$(ab)^{k-1} = a^{k-1} b^{k-1}.$$

We want to show it holds for k. We can write this as

$$(ab)^k = (ab)^{k-1}ab = a^{k-1}b^{k-1}ab.$$

Again, using the relation that $ba = ab$, we can write this as

$$a^{k-1}b^{k-2}bab = a^{k-1}b^{k-2}ab^2.$$

We repeat this process $k-1$ times to get

$$a^{k-1}ab^{k-1}b = a^kb^k.$$

Thus, we have

$$(ab)^k = a^kb^k,$$

and so the induction hypothesis holds.

We now consider the case where $k \in \mathbb{Z}_{<0}$. Then we can write $k = -c$, where $c \in \mathbb{Z}_{>0}$. Thus, we have

$$(ab)^k = (ab)^{-c} = ((ab)^{-1})^c = (b^{-1}a^{-1})^c = (a^{-1}b^{-1})^c = (a^{-1})^b(b^{-1})^c = a^{-c}b^{-c}$$

using the fact that G is abelian, properties of powers, and the claim shown prior. Hence, we have it holds for $k \in \mathbb{Z}$. □

Using this claim, we see that, since G is an abelian group, we have

$$g(a)g(b) = a^kb^k = (ab)^k = g(ab),$$

and so this is a homomorphism for $k \in \mathbb{Z}$. It is therefore an endomorphism. □

Problem 12 (Section 1.9, Exercise 6)**.** Let $a \in G$ be a group, and define the inner automorphism I_a to be the map $x \mapsto axa^{-1}$ in G. Verify that I_a is an automorphism. Show that $a \mapsto I_a$ is a homomorphism of G into $\mathrm{Aut}(G)$ with kernel the center C of G. Hence, conclude that $\mathrm{Inn}(G) = \{I_a \ : \ a \in G\}$ is a subgroup of $\mathrm{Aut}(G)$ with $\mathrm{Inn}(G) \cong G/C$. Verify that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. We have that $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the group of outer automorphisms.

Proof. There are a lot of steps to this problem, so let's break it up.
Step 1: We first establish that I_a is indeed an automorphism. To do so, we need to check that it's well-defined, injective, surjective, and a homomorphism. Let $x = y \in G$. Then

$$I_a(x) = axa^{-1} = aya^{-1} = I_a(y)$$

by multiplying a^{-1} to the left and a to the right, so the function is well-defined. Next, we check it's injective. Let $I_a(x) = I_a(y)$. Then we have

$$axa^{-1} = aya^{-1} \leftrightarrow x = y$$

after multiplying a^{-1} to the left and a to the right. Hence, it's injective. To see surjectivity, take $g \in G$. We see that $a^{-1}ga \in G$, and furthermore

$$I_a(a^{-1}ga) = aa^{-1}gaa^{-1} = g.$$

Since the choice of g was arbitrary, we get it's surjective. Finally, we need to check it's a homomorphism. Notice that, for $x, y \in G$, we have

$$I_a(xy) = axya^{-1} = ax(a^{-1}a)ya^{-1} = axa^{-1}aya^{-1} = I_a(x)I_a(y),$$

and so it's indeed a homomorphism. Thus, I_a is an automorphism.
Step 2: We presumably need to establish that $\mathrm{Inn}(G)$ is, in fact, a subgroup of G. First, we see that $I_e = \mathrm{Id}$, since $I_e(x) = exe^{-1} = x$ for all $x \in G$. Next, if $I_a \in \mathrm{Inn}(G)$, we need to establish that it's inverse is also in $\mathrm{Inn}(G)$. But notice that $I_{a^{-1}} \circ I_a(x) = a^{-1}axa^{-1}a = x$ for all $x \in G$, and so they are inverses. Hence, $I_a^{-1} = I_{a^{-1}} \in \mathrm{Inn}(G)$. Finally, we need to establish that it's closed under products. But this follows from the fact that $I_a \circ I_b(x) = abxb^{-1}a^{-1} = abx(ab)^{-1} = I_{ab}(x)$ for all $x \in G$, and so $I_a \circ I_b = I_{ab} \in \mathrm{Inn}(G)$. Thus, it is a subgroup.
Step 3: Now, we need to establish that $a \mapsto I_a$ is a homomorphism of G into $\mathrm{Aut}(G)$. That is, if we define this function to be ϕ, we wish to show that ϕ is well-defined and satisfies the homomorphism

property. To see well-definedness, if $a = b$, then we see that $I_a(x) = axa^{-1} = bxb^{-1} = I_b(x)$ for all $x \in G$, and so $I_a = I_b$. Hence, $\phi(a) = \phi(b)$. To see the homomorphism property, we need to show that $\phi(ab) = \phi(a)\phi(b)$. Notice that for all $x \in G$ we have

$$I_{ab}(x) = abxb^{-1}a^{-1} = I_a(bxb^{-1}) = I_a \circ I_b(x),$$

and so

$$I_{ab} = I_a \circ I_b;$$

in other words, $\phi(ab) = \phi(a)\phi(b)$. So it is a homomorphism.
Step 4: We now want to establish that

$$\ker(\phi) = C = \{g \in G \ : \ ga = ag \text{ for all } a \in G\}.$$

Notice that $\ker(\phi) = \{g \in G \ : \ \phi(g) = I_e\}$, but $\phi(g) = I_e$ implies that, for all $x \in G$, we have

$$I_g(x) = gxg^{-1} = x \leftrightarrow gx = xg.$$

Since this applies for all x, we get that $g \in C$. So $\ker(\phi) \subset C$, and for the other direction if $g \in C$ we have $gx = xg$ for all $x \in G$, so in particular $gxg^{-1} = x$, and therefore $I_g = I_e$. Hence, $g \in \ker(\phi)$, and so $C \subset \ker(\phi)$. Thus, $C = \ker(\phi)$.
Step 5: We have a homomorphism $\phi : G \to \text{Inn}(G)$ which is surjective, and so the First Isomorphism Theorem tells us that $G/\ker(\phi) \cong \text{Inn}(G)$. We established in **Step 4** that $\ker(\phi) = C$, and so we get that $G/C \cong \text{Inn}(G) \leq \text{Aut}(G)$.
Step 6: Finally, we need to verify it is a normal subgroup. Take $\kappa \in \text{Aut}(G)$. Then we see that

$$\kappa I_a \kappa^{-1}(x) = \kappa(a\kappa^{-1}(x)a^{-1}) = \kappa(a)\kappa(\kappa^{-1}(x))\kappa(a^{-1}) = \kappa(a)x\kappa(a)^{-1}.$$

Since κ is an automorphism, we have that $\kappa(a) = b \in G$, and so we can write this as

$$\kappa(a)x\kappa(a)^{-1} = bxb^{-1} = I_b \in \text{Inn}(G).$$

Since the choice of I_a, κ were arbitrary, we get that this is a normal subgroup. □

Problem 13 (Section 1.10, Exercise 2)**.** Let $\{H_\alpha\}$ be a collection of subgroups containing the normal subgroup K. Show that

$$\bigcap (H_\alpha/K) = \left(\bigcap H_\alpha\right)/K.$$

Proof. We wish to establish that these sets are equal. Take $xK \in \bigcap(H_\alpha/K)$. Then, for every α, $xK \in H_\alpha/K$, which tells us that $xK = h_\alpha K$ for each α, where $h_\alpha \in H_\alpha$. In other words $xh_\alpha^{-1} \in K \subset H_\alpha$. Thus, we get $xh_\alpha^{-1} = h'_\alpha$, or $x = h'_\alpha h_\alpha$. Hence, $x \in H_\alpha$ for each α, and so $x \in \bigcap H_\alpha \subset G$. Taking it's image in the quotient, we see that $xK \in (\bigcap H_\alpha)/K$, and so we get

$$\bigcap (H_\alpha/K) \subset \left(\bigcap H_\alpha\right)/K.$$

For the other direction, Notice that $\bigcap H_\alpha \subset H_\alpha$ for each α, and so we have

$$\left(\bigcap H_\alpha\right)/K \subset \bigcap (H_\alpha/K).$$

Hence, we have equality. □

Problem 14 (Section 1.12, Exercise 5)**.** Let p be the smallest prime dividing the order of a finite group. Show that any subgroup H of G of index p is normal.

Proof. We use the prior problem to solve this one.

Claim 10 (Section 1.12, Exercise 4)**.** Show that if a finite group G has a subgroup H of index n, then H contains a normal subgroup of G of index a divisor of $n!$.

Proof. We proceed via the hint. Let G act on the coset space G/H via left translation. Then we have a homomorphism $\phi : G \to \mathrm{Sym}(G/H)$, where $\phi(g)(xH) = (gx)H \in G/H$. Notice that

$$\ker(\phi) = \{g \in G \ : \ \phi(g)(xH) = xH \text{ for all } xH \in G/H\}.$$

That is, the collection of $g \in G$ so that

$$gxH = xH \leftrightarrow x^{-1}gx \in H \leftrightarrow g \in x^{-1}Hx$$

for all $x \in G$, and so in particular we have $g \in H$. Hence, $\ker(\phi) \leq H$ a subgroup which is normal in G. We wish to then figure out $[G : \ker(\phi)]$; that is, we would like to know $|G/\ker(\phi)| \mid n!$. But the inner-outer automorphism theorem (**Problem 2**) tells us that $G/\ker(\phi) \cong K \leq \mathrm{Sym}(G/H)$. Lagrange's theorem tells us that $|K| = |G/\ker(\phi)| \mid |\mathrm{Sym}(G/H)| = n!$. Thus, we have the result. □

Now, using this, let G act on G/H via left translation. Then we have that there is a normal subgroup $K \leq H$ such that $[G : K] \mid [G : H]! = p!$. Since $K \leq H$, we have

$$p = [G : H] \mid [G : K] \mid p!.$$

We see that if $[G : K] \neq p$, then $[G : K] = pk$, where $k \geq p$. But this contradicts the fact that $[G : K] \mid p! = p(p-1)\cdots 1$. So we must have $[G : K] = p$, which forces $K = H$. Hence, H is normal. □

Problem 15 (Section 1.2, Exercise 7)**.** Let H be a proper subgroup of a finite group G. Show that

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

Proof. We break this up into cases.
Case 1: If H is normal, then $gHg^{-1} = H$ for all $g \in G$, and so we have

$$\bigcup_{g \in G} gHg^{-1} \subsetneq G,$$

as desired.
Case 2: Assume that H is not normal. Let $K = \{gHg^{-1} \ : \ g \in G\}$. Then $|K| \geq 2$ by assumption. Furthermore, G acts transitively on this set by conjugation, since for any $gHg^{-1}, xHx^{-1} \in K$ we have

$$(gx^{-1}) \cdot (xHx^{-1}) = gx^{-1}xHx^{-1}xg^{-1} = gHg^{-1}.$$

The Cauchy-Frobeinus theorem (or Burnside's Lemma) states that

$$1 = \frac{1}{|G|} \sum_{g \in G} \chi(g)$$

since we have a transitive action, where $\chi(g) = |\{xHx^{-1} \in K \ : \ g(xHx^{-1})g^{-1} = xHx^{-1}\}|$. So,

$$|G| = \sum_{g \in G} \chi(g).$$

Since $|K| \geq 2$, we have $\chi(e) \geq 2$, and so this forces there to be some $g \in G$ such that $\chi(g) = 0$. Assume now for contradiction that

$$G = \bigcup_{g \in G} gHg^{-1},$$

then this implies that for all $g \in G$ there is an $x \in G$ so that $g = xhx^{-1}$, $h \in H$. Notice, however, that this implies that $xHx^{-1} \in K^g = \{k \in K \ : \ g \cdot k = k\}$, since

$$g(xHx^{-1})g^{-1} = xhx^{-1}(xHx^{-1})xh^{-1}x^{-1} = xHx^{-1}.$$

So, we get that $\chi(g) \geq 1$ for all $g \in G$, which is a contradiction. $\square$

Problem 16 (Section 1.12, Exercise 9)**.** A group H is said to act on a group K by automorphisms if we have an action of H on K and for every $h \in H$ the map $k \mapsto hk$ of K is an automorphism. Suppose this is the case and let G be the product set $K \times H$. Define a binary composition in $K \times H$ by

$$(k_1, h_1)(k_2, h_2) = (k_1(h_1k_2), h_1h_2)$$

and define $1 = (1, 1)$ – the units of K and H respectively. Verify that this defines a group such that $h \mapsto (1, h)$ is a monomorphism of H into $K \times H$ and $k \mapsto (k, 1)$ is a monomorphism of K into $K \times H$ whose image is a normal subgroup. G is called a semi-direct product of K and H. Note that if H and K are finite, then $|K \times H| = |K||H|$.

Proof. **Step 1:** We check that $K \times H$ with this law of composition is a group. To do so, we need to check three things. Since h_1 is an automorphism of K, we get that $h_1k_2 = k' \in K$, so $k_1(h_1k_2) = k_1k' \in K$, and $h_1h_2 \in H$ clearly, so the composition is closed. Next, we need to check that this is associative. That is, if we have $k_1, k_2, k_3 \in K$, $h_1, h_2, h_3 \in H$, then

$$(k_1, h_1)((k_2, h_2)(k_3, h_3)) = ((k_1, h_1)(k_2, h_2))(k_3, h_3).$$

Notice that

$$(k_2, h_2)(k_3, h_3) = (k_2(h_2k_3), h_2h_3),$$

so

$$(k_1, h_1)((k_2, h_2)(k_3, h_3)) = (k_1, h_1)(k_2(h_2k_3), h_2h_3) = (k_1(h_1k_2(h_2k_3)), h_1(h_2h_3)).$$

Since H is a group, we can write the second component as

$$(k_1(h_1k_2(h_2k_3)), h_1(h_2h_3)) = (k_1(h_1k_2(h_2k_3)), h_1h_2h_3).$$

Notice now that

$$(k_1, h_1)(k_2, h_2) = (k_1(h_1k_2), h_1h_2),$$

so

$$((k_1, h_1)(k_2, h_2))(k_3, h_3) = (k_1(h_1k_2), h_1h_2)(k_3, h_3) = (k_1(h_1k_2)(h_1h_2k_3), h_1h_2h_3).$$

Since h_1 is an automorphism, we can rewrite this as

$$(k_1(h_1k_2)(h_1h_2k_3), h_1h_2h_3) = (k_1(h_1k_2(h_2k_3)), h_1h_2h_3).$$

Hence,

$$(k_1, h_1)((k_2, h_2)(k_3, h_3)) = ((k_1, h_1)(k_2, h_2))(k_3, h_3),$$

as desired, so we have it's associative.

Next, we see that $(1, 1)$ is an identity. Since H acts on K, we get that $1k_1 = k_1$ for all $k_1 \in K$, and since $h \in H$ is an automorphism we get $h1 = 1$ for all $h \in H$, and so

$$(1, 1)(k, h) = (1(1k), 1h) = (k, h),$$

$$(k, h)(1, 1) = (k(h1), h1) = (k, h),$$

so we have an identity $(1, 1)$.

Finally, we need to check that there are inverses. Take $(k_1, h_1) \in K \times H$, then we want to find (k, h) such that

$$(k_1, h_1)(k, h) = (1, 1).$$

Notice that the left hand side is

$$(k_1, h_1)(k, h) = (k_1(h_1k), h_1h).$$

So, this forces $h = h_1^{-1}$. Hence, we can rewrite this as

$$(k_1(h_1k), h_1h) = (k_1(h_1k), 1).$$

Next, notice that h_1 is an automorphism of K. Hence, we can choose k such that $h_1k = k_1^{-1}$ via setting $k = h_1^{-1}k_1^{-1}$. Thus, we have

$$(k_1, h_1)(h_1^{-1}k_1^{-1}, h_1^{-1}) = (1, 1).$$

Notice as well that

$$(h_1^{-1}k_1^{-1}, h_1^{-1})(k_1, h_1) = (h_1^{-1}k_1^{-1}(h_1^{-1}k_1), h_1^{-1}h_1) = (h_1^{-1}(k_1^{-1}k_1), h_1^{-1}h_1) = (h_1^{-1}(1), 1) = (1, 1).$$

So this is a left and right inverse, and so it is an inverse.

Thus, we have that this is a group.

Step 2: We check now that the mapping $h \mapsto (1, h)$ is a monomorphism of H into $K \times H$. To see that it is a monomorphism, we show it is well-defined, injective, and a homomorphism. For well-defined, if $h_1 = h_2$, then it's clear that $(1, h_1) = (1, h_2)$. Injectivity also clearly follows; $(1, h_1) = (1, h_2)$ forces $h_1 = h_2$. To see that it is a homomorphism, we need to show that $h_1h_2 \mapsto (1, h_1h_2) = (1, h_1)(1, h_2)$. But this follows from the definition of the law of composition. So we have an injective homomorphism of H into $K \times H$, and so it is a monomorphism.

Step 3: We need to check now that the mapping $k \mapsto (k, 1)$ is a monomorphism of K into $K \times H$. Again, to see it is a monomorphism, we check that it is well-defined, injective, and a homomorphism. Again, we see that $k_1 = k_2$ implies $(k_1, 1) = (k_2, 1)$, and so it is well-defined. Injectivity also clearly follows; $(k_1, 1) = (k_2, 1)$ forces $k_1 = k_2$. Finally, to see that its a homomorphism, we need to check that $k_1k_2 \mapsto (k_1k_2, 1) = (k_1, 1)(k_2, 1)$. But this follows from noting that

$$(k_1, 1)(k_2, 1) = (k_1(1k_2), 1) = (k_1k_2, 1).$$

So it is indeed a monomorphism. To see that it's a normal subgroup, take any $(h, k) \in H \times K$, $(k', 1)$ in the image. Then we have

$$(k, h)(k', 1)(h^{-1}k^{-1}, h^{-1}) = (k, h)(k'(h^{-1}k^{-1}), h^{-1} = (k(hk')k^{-1}, 1).$$

Since $hk' \in K$, we get that $k(hk')k^{-1} \in K$, so the image is indeed a normal subgroup (alternatively, we could have used the proof from the class notes, but this seems faster).

Step 4: It clearly follows that $|K \times H| = |K||H|$ if all are finite from basic set theory, since we did not alter the set $K \times H$ itself, only the law of composition on it. □

Problem 17 (Section 1.13, Exercise 3)**.** Show that there are no simple groups of order pq, where p and q are primes.

Proof. Throughout, let $\mathrm{Syl}_p(G)$ denote the Sylow p-subgroups of G. Recall that a group is simple if there are no normal subgroups other than itself or the trivial group. So, it suffices to show that G has a non-trivial normal subgroup if $|G| = pq$.

Remark. This gives us the result for Section 1.12, Exercise 6.

Case 1: If $p = q$, then we have $|G| = p^2$, where p is a prime. Since this is a p-subgroup, we have that $|Z(G)| > 1$. We then have the following claims.

Claim 11. If $G/Z(G)$ is cyclic, then G is abelian.

Proof. Since $G/Z(G)$ is cyclic, we can write it as $G/Z(G) = \langle a \rangle Z(G)$. So, for all $g, h \in G$, we can write $g = a^jx$, $h = a^ky$, where $x, y \in Z(G)$. Thus,

$$gh = a^jxa^ky = a^ja^kxy = a^{j+k}yx = a^{k+j}yx = a^ka^jyx = a^kya^jx = hg.$$

Hence, G is abelian. □

Claim 12. A group of order p must be cyclic.

Proof. Since this is a p-group, we have that $|Z(G)| \neq 1$. Lagrange tells us that $|Z(G)| \mid p$, which tells us that $|Z(G)| = p$. Hence, $Z(G) = G$, and so the group is abelian.

Cauchy's theorem tells us that if $p \mid |G|$, G abelian, then there is an element of order p. Since we have an element a such that $o(a) = |G|$, we get that G must be cyclic. Hence, a group of order p must be cyclic. □

Since the center is non-trivial, we have $|G/Z(G)| = \{1, p\}$. If $|G/Z(G)| = p$, notice that $G/Z(G)$ must be cyclic, and so the claim tells us that G is abelian; hence, $Z(G) = G$, a contradiction to the fact that we took $Z(G) \lneq G$. Thus, we must have $|G/Z(G)| = 1$, or $Z(G) = G$. Since G is abelian, we have that every subgroup is normal, and so using Cauchy's theorem we can find an element a of order p in G, and we have $\langle a \rangle$ is normal in G. Thus, G cannot be simple in the case where $p = q$.
Case 2: Without loss of generality, take $p > q$. Notice that $|\mathrm{Syl}_p(G)| = \{1, q\}$, since $|\mathrm{Syl}_p(G)| \mid |G|$. If $|\mathrm{Syl}_p(G)| = 1$, we are done, since this implies that $P \in \mathrm{Syl}_p(G)$ is normal and non-trivial. Since we require that $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$, and $q < p$, we have that this forces $|\mathrm{Syl}_p(G)| = 1$.

Coupling **Case 1** and **Case 2**, we get that G is not simple for all primes p, q. Therefore, if $|G| = pq$, we have it is not simple. □

Problem 18 (Section 1.13, Exercise 4)**.** Show that every non-abelian group of order 6 is isomorphic to S_3.

Proof. To do this, we classify all groups of order 6. Notice that $|G| = 6 = 2 \cdot 3$, and so $|G| = pq$ where $p = 2$, $q = 3$. We see from the argument above that this forces $|\mathrm{Syl}_3(G)| = 1$; that is, we have that $K \leq G$, where $|K| = 3$ is the unique normal Sylow 3-subgroup of G. Let $H \leq G$ be such that $H \in \mathrm{Syl}_2(G)$. We want to examine

$$\phi : H \to \mathrm{Aut}(K).$$

Since $|K| = 3$, this implies that $K \cong \mathbb{Z}_3$ from prior claims. Notice, then, that $\mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$; this follows since an automorphism $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ is completely determined by where it sends generators. That is, the homomorphism is completely determined by where $f(1)$ is sent. Since it's an automorphism, we need to send 1 to another generator, and the only possibility is 2. Thus, we can rewrite the above as

$$\phi : H \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2.$$

Since K is cyclic, and so abelian, there are two automorphisms already accounted for. We have the identity automorphism, where everything is mapped to itself, and the inverse automorphism. That is, we have

$$\phi : H \to \{\mathrm{Id}, \mathrm{Inv}\}.$$

Since H is a subgroup of order 2, we get that $H \cong \mathbb{Z}_2$. So our options for a homomorphism $\phi : H \to \{\mathrm{Id}, \mathrm{Inv}\}$ is that everything is mapped to the identity map, or the non-trivial element in H is mapped to the inverse map. Denote these by ϕ_1 for everything being sent to the identity map, and ϕ_2 being the one where the non-trivial element is mapped to the inverse map.

So we have that $G \cong K \rtimes_{\phi_1} H$ or $G \cong K \rtimes_{\phi_2} H$ are our only two options. Since ϕ_1 is the trivial homomorphism, we have that $K \rtimes_{\phi_1} H \cong K \times H$. Since $K \cong \mathbb{Z}_3$, $H \cong \mathbb{Z}_2$, we get that $G \cong \mathbb{Z}_3 \times \mathbb{Z}_2$. This is clearly abelian, since it's abelian in each component, and since we know S_3 is not abelian we have that $S_3 \ncong \mathbb{Z}_3 \times \mathbb{Z}_2$.

In the other case, we note that $K \rtimes_{\phi_2} H$ is not abelian (it must not be, since we must have $S_3 \cong K \rtimes_{\phi_2} H$, but we show this explicitly). Let $a \in H - \{e\}$, $k \in K - \{e\}$, where $o(k) \neq 2$, then we have

$$(k, a) \cdot (k, e) = (k(a \cdot k), a) = (e, a),$$
$$(k, e) \cdot (k, a) = (k(e \cdot k), a) = (k^2, a),$$

and we see that $k^2 \neq e$ since k does not have order 2.

Since all groups of order 6 must be isomorphic to one of these, we have that $S_3 \cong K \rtimes_{\phi_2} H$, and since isomorphism is an equivalence relation, we get that any non-abelian group of order 6 is isomorphic to S_3. □

Problem 19 (Section 4.6, Exercise 6)**.** Define G^i by $G^1 = G$, $G^i = (G^{i-1}, G)$. The sequence of normal subgroups

$$\cdots \subset G^3 \subset G^2 \subset G^1$$

is called the lower central series for G. G is called nilpotent if there exists an integer k such that $G^k = 1$. Show that if G is nilpotent, then it is solvable. Give an example where the converse does not hold.

Proof. This will follow if $G^{(i)} \leq G^i = (G^{i-1}, G)$. To show this, we proceed by induction on i. In the case that $i = 1$, we clearly have $G^{(1)} = G' \leq G^1 = G$. Assume that it holds up to $k-1$. Then we need to show that $G^{(k)} \subset G^k$. But this follows, since

$$G^{(k)} = (G^{(k-1)}, G^{(k-1)}) \leq (G^{k-1}, G) = G^k.$$

Hence, induction tells us that this holds, and so since $G^k = 1$ for some k, we have $G^{(k)} \leq G^k = 1$, and so the group is solvable.

Examine S_3. Then we have it is solvable, since $1 \trianglelefteq A_3 \trianglelefteq S_3$, and $S_3/A_3 \cong \mathbb{Z}_2$, so it is abelian, and $A_3 \cong \mathbb{Z}_3$, so $A_3/1$ is also abelian. To see that it is not nilpotent, notice that $S_3^2 = (S_3, S_3) = A_3$, and $S_3^3 = (A_3, S_3) = A_3$ again, since for $\sigma \in S_3$, $\kappa \in A_3$, we have $\sigma\kappa\sigma^{-1}\kappa^{-1}$ gives us a product of three cycles or trivial elements, and so is in A_3. Hence, we see that $S_3^k \neq 1$ for any k, so it is not nilpotent. □

Problem 20 (Section 4.6, Exercise 10)**.** If G is a group, define the upper central series $1 \subset C_1 \subset \cdots$ by $C_1 = C(G)$, the center of G, and C_i, the normal subgroup such that C_i/C_{i-1} is the center of G/C_{i-1}. Show that a finite group G is nilpotent if and only if the upper central series ends in a finite number of steps with G.

Proof.

Remark. We follow a proof given in Isaacs (**Theorem 8.17**).

($\implies$) Assume that G is nilpotent. Then this tells us that G is solvable by the prior problem. So we can construct a sequence

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \cdots \trianglelefteq N_s = G,$$

where $N_i = G^{(s-i)}$. Since G is solvable, we get $G^{(s)} = 1$. Notice that $N_{i+1}/N_i \leq Z(G/N_i)$, since N_{i+1}/N_i is abelian. If we show that $N_i \subset C_i$ for all i, then we get that the upper central series ends in a finite number of steps with G, since this implies that $N_s = G \subset C_s \subset G$. We prove a few claims first.

Claim 13. Let $X \leq G$. Then $X \subset Z(G)$ if and only if $(X, G) = 1$.

Proof. ($\implies$) We have that elements from X commutes with elements from G, so examining generators from (X, G) we have $x^{-1}g^{-1}xg = x^{-1}xg^{-1}g = 1$. Hence, $(X, G) = 1$.

($\impliedby$) If $(X, G) = 1$, then this tells us that all elements of the form $x^{-1}g^{-1}xg = 1$. That is, $xg = gx$, and so $x \in Z(G)$. Since this applies for all $x \in X$, we have $X \subset Z(G)$. □

Claim 14. Let $\phi : G \to H$, $X, Y \leq G$ subgroups. Then $\phi((X, Y)) = (\phi(X), \phi(Y))$.

Proof. Elements in (X, Y) are generated by elements of the form $x^{-1}y^{-1}xy$. Then we see that $\phi(x^{-1}y^{-1}xy) = \phi(x)^{-1}\phi(y)^{-1}\phi(x)\phi(y)$, which is in $(\phi(X), \phi(Y))$. For the other direction, if $\phi(x)^{-1}\phi(y)^{-1}\phi(x)\phi(y) = \phi(x^{-1}y^{-1}xy)$, which is in $\phi((X, Y))$. Hence, the sets are equal. □

Claim 15. Let $Y \trianglelefteq G$, $X \leq G$. Then $(X, G) \subset Y$ if and only if $XY/Y \subset Z(G/Y)$.

Proof. ($\implies$) Assume $(X, G) \subset Y$. Let $\phi : G \to G/Y$ be the canonical map. Notice that $\phi(X, G) = (\phi(X), \phi(G)) = 1$, so we have that $(X, G) \subset \ker(\phi)$, which tells us that $\phi(X) \subset Z(\phi(G))$. Hence, we have $XY/Y \subset Z(G/Y)$.

($\impliedby$) Assume $XY/Y = \phi(X) \subset Z(G/Y) = Z(\phi(G))$. Then this tells us that $(\phi(X), \phi(G)) = \phi((X, G)) = 1$, which implies that $(X, G) \subset \ker(\phi) = Y$. □

Now, we proceed by induction. Clearly $N_0 \subset C_0$, so assume it holds for $k-1$. Then we want to show $N_k \subset C_k$. Notice that we have $(N_k, G) \subset N_{k-1} \subset C_{k-1}$, so $N_k C_{k-1}/C_{k-1} \subset Z(G/C_{k-1}) = C_k/C_{k-1}$, and so by the correspondence theorem we have $N_k C_{k-1} \subset C_k$. Since $N_k \subset N_k C_{k-1}$, we get $N_k \subset C_k$, as desired.

($\impliedby$) Assume that the upper central series ends in a finite number of steps with G. Using the trick outlined in the implication, we have that G is solvable. We then need to deduce that G is nilpotent. Let $G^1 = G$, $G^i = (G^{i-1}, G)$. We want to show that $G^s = 1$ for some s. Assume that our upper central series is of the form

$$1 = C_0 \subset C_1 \subset \cdots \subset C_s = G.$$

Notice that $(C_{k+1}, G) \subset C_k$, since $C_{k+1}/C_k \subset Z(G/C_k)$. Notice as well that $G^1 \subset C_s$. Assume it holds for $k-1$, and we want to show by induction that $G^k \subset C_{s-k+1}$. Since $G^{k-1} \subset C_{s-k+2}$, we have $G^k = (G^{k-1}, G) \subset (C_{s-k+2}, G) \subset C_{s-k+1}$, and so it holds. Therefore, we have that $G^{s+1} = 1$, and so it is nilpotent. □

Problem 21 (Section 2.2, Exercise 1)**.** Show that any finite domain is a division ring.

Proof. Recall that a ring is called a domain if $R^\times$ is a submonoid of $(R, \cdot, 1)$. We have the equivalent characterization that a ring is a domain if and only if $R \neq 0$ and the cancellation laws hold; $ab = ac$, $a \neq 0$ implies $b = c$, and likewise for $ba = ca$, $a \neq 0$. To get that it is a division ring, we need to establish that $R^\times$ is, in fact, a group. That is, for all $a \in R^\times$, there exists an $a^{-1} \in R^\times$such that $aa^{-1} = a^{-1}a = 1$. Let $\varphi_a : R^\times \to R^\times$ be defined by $\varphi_a(x) = ax$. Notice that φ_a is injective; that is, we have $\varphi_a(x) = \varphi_a(y)$ or $ax = ay$ if and only if $x = y$ by our characterization of domains (that is, the cancellation rules). Since $\varphi_a : R^\times \to R^\times$ is injective and $R^\times$ is finite, we have that it is a bijection, and so we have that there is some y such that $\varphi_a(y) = ay = 1$. Notice that we have

$$a = 1 \cdot a = (ay)a = a(ya),$$

and so the cancellation law gives us

$$1 = ya.$$

Since

$$ay = ya = 1,$$

we have that y is an inverse for a. Since the choice of $a \in R^\times$ was arbitrary, we get $R^\times$ is a subgroup, and so R must be a division ring. □

Problem 22 (Section 2.3, Exercise 12)**.** Show that if R is a field, $A \in M_n(R)$ is a zero divisor in this ring if and only if A is not invertible. Does this hold for arbitrary commutative R? Explain.

We need a claim for the following proof.

Claim 16. Let V, W be finite dimensional vector spaces over a field F such that $\mathrm{Dim}(V) = \mathrm{Dim}(W)$, $L : V \to W$ be an injective linear homomorphism. Then L is an isomorphism.

Proof. It suffices to show that L is surjective. Take $w \in W$, then we need to show that there is a $v \in V$ such that $L(v) = w$. Since $\ker(L) = \{0\} = 0$, we have

$$L(v) = L\left(\sum_{i=1}^{n} a_i v_i\right) = \sum_{i=1}^{n} a_i L(v_i),$$

assuming $\{v_i\}$ is a basis for V and $a_i \in F$. Injectivity says

$$L(v) = 0 \leftrightarrow \sum_{i=1}^{n} a_i v_i = 0,$$

and since this is a basis this implies that $a_i = 0$ for all i. Hence, we have that $L(v_i)$ is a linearly independent set of vectors. Since $\mathrm{Dim}(W) = n$, we have that this is a basis for W. So, we have that

$$w = \sum_{i=1}^{n} b_i L(v_i) = L\left(\sum_{i=1}^{n} b_i v_i\right) = L(v),$$

and so there is a $v \in V$ such that $L(v) = w$. Hence, the mapping is surjective. □

Proof. We show that for R a field, $A \in M_n(R)$ is a zero divisor if and only if A is not invertible. ($\implies$) We proceed by contradiction. Assume that A is a zero divisor and A is invertible. Then we have that there is a $B \neq 0$ such that

$$BA = 1$$

and a $C \neq 0$ such that

$$AC = 0.$$

So we have

$$AC = 0 \leftrightarrow B(AC) = (BA)C = C = B(0) = 0.$$

This is a contradiction, since we assumed $C \neq 0$. Thus, we must have that A is not invertible.
($\Longleftarrow$) (Assuming some linear algebra) We want to show that if A is not a zero divisor, then A is invertible (i.e., the contrapositive). Let $L_A : M_n(R) \to M_n(R)$ be defined by $L_A(B) = AB$. Then this is a linear homomorphism; for $A, B \in M_n(R)$, $x, y \in R$, we have $L_A(xB+yC) = A(xB+yC) = xAB+yAC = xL_A(B)+yL_A(C)$. Notice as well that $\ker(L_A) = \{B \in M_n(R) \ : \ AB = 0\}$. However, by assumption, every non-zero element does not multiply into 0, and so we have $\ker(L_A) = 0$. Hence, L_A is an injective linear homomorphism. Since $M_n(R)$ is a finite dimensional vector space, we get that L_A is an isomorphism. Hence, we have that there is some $B \in M_n(R)$ such that $L_A(B) = AB = 1$. Thus, A is invertible.

Examine $F = \mathbb{Z}$, $M_1(F)$. Then any element $a \in M_1(F)$ is not invertible, however no non-zero element is a zero divisor. □

Problem 23 (Section 2.4, Exercise 10)**.** Let D be a division ring, C its center and let S be a division subring of D which is stabilized by every map $x \mapsto dxd^{-1}$, $d \neq 0$ in D. Show that either $S = D$ or $S \subset C$.

Proof. Clearly if S is a division subring of D, we have $S \subset D$ or $S = D$. Thus, it suffices to show that if $S \subset D$, we have $S \subset C$.

Let $\alpha_x : D \to D$ via $\alpha_x(d) = xdx^{-1}$, where $x \in D^\times$. We can rewrite this as

$$\alpha_x(d) = (x, d)d,$$

assuming that $d \neq 0$. Our goal is to show that, assuming $S \subset D$ properly, we get $(x, d) = 1$ for all $x \in S^\times$, $d \in D^\times$ (it's clear that S will commute with zero). Take $x \in S^\times$, $d \in D - S$. First, we notice that

$$\alpha_x(d+1) = x(d+1)x^{-1} = xdx^{-1} + 1 = \alpha_x(d) + 1.$$

Using our alternative notation, this gives

$$\alpha_x(d+1) = (x, d+1)(d+1) = (x, d)d + 1.$$

Expanding and rewriting, we have

$$((x, d+1) - (x, d))d = 1 - (x, d+1).$$

If $(x, d+1) \neq (x, d)$, we have $(x, d), (x, d+1) \in S^\times$, since $S^\times$ is a normal subgroup (since we have it's stabilized under conjugation). We therefore have $(x, d+1) - (x, d) \neq 0 \in S^\times$, and so we have it's invertible. On the right hand side, we have $1 - (x, d+1) \in S^\times$ as well, so therefore we must have $d \in S^\times$, but this contradicts our choice of d, which we assumed was outside of S. Hence, we must have $(x, d+1) = (x, d)$, but this then forces $(x, d+1) = 1 = (x, d)$. Thus, $x \in C(d)$ for all $d \in D - S$.

To see that $x \in C(d)$ for all $d \in S^\times$, take $h \in D - S$. Then we claim $h + s \in D - S$; clearly $h + s \in D$, and if $h + d \in S$, we have $h + d = s'$, and so $h = s' - d \implies h \in S$, a contradiction. This then gives $(x, d+h) = 1$. Writing this out, we have

$$(x, d+h) = x(d+h)x^{-1}(d+h)^{-1} = (xdx^{-1} + xhx^{-1})(d+h)^{-1},$$

and so

$$xdx^{-1} + xhx^{-1} = d + h.$$

From our prior result, $xhx^{-1} = h$, so we get

$$xdx^{-1} + h = d + h \leftrightarrow xdx^{-1} = d,$$

as desired. So, if $S \subset D$ strictly, we must have $S \subset C$, the center of D, as desired. $\square$

Problem 24 (Section 2.5, Exercise 7)**.** Let I be an ideal in R, U the group of units of R. Let U_1 be the subset of elements $a \in U$ such that $a \equiv 1 \pmod{I}$. Show that U_1 is a normal subgroup of U.

Proof. Let $y \in U$, $a \in U_1$. Then we need to show that $yay^{-1} \in U_1$. To see this, notice that

$$yay^{-1} \equiv y(1)y^{-1} \pmod{I} \implies yay^{-1} \equiv 1 \pmod{I},$$

since $yay^{-1} - 1 = yay^{-1} - yy^{-1} = y(a-1)y^{-1}$, and since I is an ideal, $a - 1 \in I$, we get $y(a-1)y^{-1} \in I$.

Hence, $yay^{-1} \in U_1$, and so U_1 is a normal subgroup. $\square$

Problem 25 (Section 2.6, Exercise 4)**.** Let $A \in GL_2(\mathbb{Z}/(p))$. Show that $A^q = 1$ if $q = (p^2-1)(p^2-p)$. Show also that $A^{q+2} = A^2$ for every $A \in M_2(\mathbb{Z}/(p))$.

Proof. We first show a claim on the order of $GL_n(\mathbb{Z}/(p))$.

Claim 17. The order of $GL_n(\mathbb{Z}/(p))$ is $(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1})$.

Proof. We proceed by a combinatorial argument. Notice that the first row of $GL_n(\mathbb{Z}/(p))$ can be anything except the 0 row, so we have $p^n - 1$ options. For the next row, we have it can be anything but what we chose as our first row. We then need our next row to be linearly independent from our first row, and so we only have $p^n - p$ options for it. Continuing, we get the desired result. $\square$

Thus, we have that the order of $GL_2(\mathbb{Z}/(p))$ is $(p^2-1)(p^2-p)$. Hence, if $A \in GL_2(\mathbb{Z}/(p))$, we have $A^q = 1$ if $q = |GL_2(\mathbb{Z}/(p))| = (p^2-1)(p^2-p)$.

Next, we need to show that $A^{q+2} = A^2$ for every $A \in M_2(\mathbb{Z}/(p))$. If $A \in GL_2(\mathbb{Z}/(p))$, we are done, since $A^{q+2} = A^q A^2 = A^2$. If $A \notin GL_2(\mathbb{Z}/(p))$, we have the following identity.

Claim 18. For

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $\det(A) = 0 = ad - bc$, we have

$$A^n = \begin{pmatrix} a(a+d)^{n-1} & b(a+d)^{n-1} \\ c(a+d)^{n-1} & d(a+d)^{n-1} \end{pmatrix}.$$

Proof. We proceed by induction. The case of $n = 1$ is trivial. Assume it holds for $n-1$; that is, we have

$$A^{n-1} = \begin{pmatrix} a(a+d)^{n-2} & b(a+d)^{n-2} \\ c(a+d)^{n-2} & d(a+d)^{n-2} \end{pmatrix}.$$

Then we see that

$$A^n = A^{n-1}A = \begin{pmatrix} a(a+d)^{n-2} & b(a+d)^{n-2} \\ c(a+d)^{n-2} & d(a+d)^{n-2} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Calculating it, we have

$$A^n = \begin{pmatrix} a^2(a+d)^{n-2} + (bc)(a+d)^{n-2} & (ab)(a+d)^{n-2} + (bd)(a+d)^{n-2} \\ (ac)(a+d)^{n-2} + (dc)(a+d)^{n-2} & (bc)(a+d)^{n-2} + d^2(a+d)^{n-2} \end{pmatrix}.$$

We have $ad = bc$, and so rewriting this we get

$$A^n = \begin{pmatrix} a^2(a+d)^{n-2} + (ad)(a+d)^{n-2} & (ab)(a+d)^{n-2} + (bd)(a+d)^{n-2} \\ (ac)(a+d)^{n-2} + (dc)(a+d)^{n-2} & (ad)(a+d)^{n-2} + d^2(a+d)^{n-2} \end{pmatrix}.$$

Factoring gives

$$A^n = \begin{pmatrix} a\left(a(a+d)^{n-2} + d(a+d)^{n-2}\right) & b\left(a(a+d)^{n-2} + d(a+d)^{n-2}\right) \\ c\left(a(a+d)^{n-2} + d(a+d)^{n-2}\right) & d\left(a(a+d)^{n-2} + d(a+d)^{n-2}\right) \end{pmatrix},$$

so

$$A^n = \begin{pmatrix} a(a+d)^{n-1} & b(a+d)^{n-1} \\ c(a+d)^{n-1} & d(a+d)^{n-1} \end{pmatrix}.$$

□

If the trace is 0, then $A^2 = 0$ using the identity, and so

$$A^{q+2} = A^q A^2 = 0 = A^2.$$

If the trace is non-zero, then we notice that for $q = (p^2-1)(p^2-p)$, we have for $x \in \mathbb{Z}/(p\mathbb{Z})$ non-zero,

$$x^q = \left(x^{p-1}\right)^{(p+1)(p^2-p)} \equiv 1 \pmod{p},$$

using Fermat's little theorem, and so

$$x^{q+1} \equiv x \pmod{p}.$$

Hence, the identity gives

$$A^{q+2} = \begin{pmatrix} a(a+d)^{q+1} & b(a+d)^{q+1} \\ c(a+d)^{q+1} & d(a+d)^{q+1} \end{pmatrix} = \begin{pmatrix} a(a+d) & b(a+d) \\ c(a+d) & d(a+d) \end{pmatrix} = A^2.$$

So for all matrices, we get

$$A^{q+2} = A^2.$$

□

Problem 26 (Section 2.7, Exercise 9)**.** If $R_1, \ldots, R_n$ are rings, we define the direct sum $R_1 \oplus \cdots \oplus R_n$ as for monoids and groups. The underlying set is $R = R_1 \times \cdots \times R_n$. Addition, multiplication, 0, and 1 are defined in the obvious way.

(a) Verify that $R = R_1 \oplus \cdots \oplus R_n$ is a ring.

(b) Show that the units of R are the elements $(u_1, \ldots, u_n)$, u_i is a unit of R_i. Hence, show that if $U = U(R)$ and $U_i = U(R_i)$, then $U = U_1 \times \cdots \times U_n$, and that $|U| = \prod |U_i|$ if they are finite.

Proof. (a) We need to check that $(R, +, 0)$ is an abelian group, $(R, \cdot, 1)$ is a monoid, and that we have the distributive property. Throughout, let $(a_1, \ldots, a_n), (b_1, \ldots, b_n)$, and $(c_1, \ldots, c_n)$ are arbitrary elements. First, notice that

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$

so the operation is closed. Next, notice that

$$\begin{aligned}(a_1, \ldots, a_n) + ((b_1, \ldots, b_n) + (c_1, \ldots, c_n)) &= (a_1, \ldots, a_n) + (b_1 + c_1, \ldots, b_n + c_n) \\ = (a_1 + (b_1 + c_1), \ldots, a_n + (b_n + c_n)) &= ((a_1 + b_1) + c_1, \ldots, (a_n + b_n) + c_n) \\ = ((a_1, \ldots, a_n) + (b_1, \ldots, b_n)) &+ (c_1, \ldots, c_n),\end{aligned}$$

using the properties of the underlying ring. So we have associativity. Next, we see that

$$(a_1, \ldots, a_n) + (0, \ldots, 0) = (a_1, \ldots, a_n) = (0, \ldots, 0) + (a_1, \ldots, a_n),$$

again by the underlying ring structure in each component, and so we have that 0 is the identity. Next, we have that

$$(a_1, \ldots, a_n) + (-a_1, \ldots, -a_n) = (0, \ldots, 0) = (-a_1, \ldots, -a_n) + (a_1, \ldots, a_n),$$

again by the underlying ring structure, and so we have inverses. Finally, we check that

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n) = (b_1 + a_1, \ldots, b_n + a_n) = (b_1, \ldots, b_n) + (a_1, \ldots, a_n),$$

so it's abelian.

Next, we check that $(R, \cdot, 1)$ is a monoid. Notice that it's closed, since

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n) \in R.$$

Next, we have identity, since

$$(a_1, \ldots, a_n) \cdot (1, \ldots, 1) = (a_1 \cdot 1, \ldots, a_n \cdot 1) = (a_1, \ldots, a_n) = (1 \cdot a_1, \ldots, 1 \cdot a_n) = (1, \ldots, 1) \cdot (a_1, \ldots, a_n),$$

Finally we have associativity, since

$$\begin{aligned}(a_1, \ldots, a_n)((b_1, \ldots, b_n)(c_1, \ldots, c_n)) &= (a_1, \ldots, a_n)(b_1 c_1, \ldots, b_n c_n) = (a_1(b_1 c_1), \ldots, a_n(b_n c_n)) \\ = ((a_1 b_1)c_1, \ldots, (a_n b_n)c_n) &= (a_1 b_1, \ldots, a_n b_n)(c_1, \ldots, c_n) = ((a_1, \ldots, a_n)(b_1, \ldots, b_n))(c_1, \ldots, c_n).\end{aligned}$$

Finally, we check the distributive property.

$$(a_1, \ldots, a_n) \cdot ((b_1, \ldots, b_n) + (c_1, \ldots, c_n)) = (a_1, \ldots, a_n) \cdot (b_1 + c_1, \ldots, b_n + c_n) = (a_1 b_1 + a_1 c_1, \ldots, a_n b_n + a_n c_n)$$

$$= (a_1 b_1, \ldots, a_n b_n) + (a_1 c_1, \ldots, a_n c_n) = (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) + (a_1, \ldots, a_n) \cdot (c_1, \ldots, _n),$$

using the distributive property inherent to the underlying rings. We also have that

$$((a_1, \ldots, a_n) + (b_1, \ldots, b_n)) \cdot (c_1, \ldots, c_n) = (a_1, \ldots, a_n) \cdot (c_1, \ldots, c_n) + (b_1, \ldots, b_n) \cdot (c_1, \ldots, c_n)$$

by the same kind of argument. Thus, R is a ring.

(b) The units of R are those elements $(u_1, \ldots, u_n)$ such that there is an element $(a_1, \ldots, a_n)$ where $(a_1, \ldots, a_n)(u_1, \ldots, u_n) = 1 = (u_1, \ldots, u_n)(a_1, \ldots, a_n)$. Using our definition, we have that $u_i a_i = a_i u_i = 1$ for each i. Hence, for each i, we must have that $u_i \in U(R_i)$. Thus, we have that $U \subset U_1 \times \cdots \times U_n$, and it's clear that $U_1 \times \cdots \times U_n \subset U$, so $U = U_1 \times \cdots \times U_n$. Basic set theory tells us that if each of the U_i are finite, we get

$$|U| = \prod_{i=1}^{n} |U_i|.$$

□

Problem 27 (Section 2.7, Exercise 10)**.** Let I_1 and I_2 be ideals of a ring R which are relatively prime in the sense that $I_1 + I_2 = R$. Show that if $a_1, a_2 \in R$ then there exists an $a \in R$ such that $a \equiv a_i \pmod{I_i}$. Generalize this result to show that if $I_1, \ldots, I_m$ are ideals where

$$I_j + \bigcap_{k \neq j} I_k = R$$

for $1 \leq j \leq m$, then for any $(a_1, \ldots, a_m)$, $a_i \in R$, there exists an $a \in R$ such that $a \equiv a_k \pmod{I_k}$ for all k.

Proof. We start with the 2 case. Since $I_1 + I_2 = R$, choose $x, y \in I_1, I_2$ respectively such that $x + y = 1$. Let $a = a_1 y + a_2 x$. Then we have that

$$a - a_1 = (a_1 y + a_2 x) - a_1 = a_1(y - 1) + a_2 x.$$

Since $x + y = 1$, we have $x = 1 - y$, so using the fact that I_1 is an ideal, we get $a - a_1 \in I_1$. In other words, $a \equiv a_1 \pmod{I_1}$. An analogous argument applies to a, a_2.

We use induction to generalize. Assume that this holds for m ideals. Then we examine the case of $m + 1$ ideals. Notice that we have

$$I_{m+1} + \bigcap_{i=1}^{m} I_i = R.$$

Notice as well that the intersection of finitely many ideals is an ideal; the intersection of finitely many abelian groups is an abelian group, and if $a \in R$, we have

$$a \bigcap_{i=1}^{m} I_i \subset I_j \ \forall\ 1 \leq j \leq m \implies a \bigcap_{i=1}^{m} I_i \subset \bigcap_{i=1}^{m} I_i.$$

We then repeat the trick from the case $n = 2$. Take $x \in I_{m+1}$, $y \in \bigcap_{i=1}^{m} I_i$ such that $x + y = 1$. Since the induction hypothesis holds, let a' be chosen such that $a' \equiv a_i \pmod{I_i}$ for $1 \leq i \leq m$. Then setting $a = a_{m+1} y + (a')x$, we have that

$$a - a_{m+1} = a_{m+1}(y - 1) + a' x \in I_{m+1} \implies a \equiv a_{m+1} \pmod{I_{m+1}},$$

and similarly for each $1 \leq i \leq m$, we have

$$a - a' = a_{m+1} y + a'(x - 1) \in I_i \implies a \equiv a' \pmod{I_i} \implies a \equiv a_i \pmod{I_i}.$$

Thus, we win. □

Problem 28 (Section 2.7, Exercise 11)**.** Use the Chinese remainder theorem and the fundamental theorem of homomorphisms to show that if I_1, I_2 are relatively prime ideals and $I = I_1 \cap I_2$, then

$$R/I \cong R/I_1 \oplus R/I_2.$$

Proof. We construct a map $\phi : R \to R/I_1 \oplus R/I_2$ via $\phi(a) = (a \pmod{I_1}, a \pmod{I_2})$. We see first that this is well-defined, since this is just the canonical mapping onto each component. Likewise, this a homomorphism by the first problem, since it's a homomorphism in each component. Finally, it's surjective by the Chinese remainder theorem. Notice as well that

$$\ker(\phi) = \{a \in R \ : \ \phi(a) = (0,0)\} = \{a \in R \ : \ a \in I_1 \cap I_2\},$$

so we have by the fundamental theorem of homomorphisms that

$$R/(I_1 \cap I_2) \cong R/I_1 \oplus R/I_2.$$

□

Problem 29 (Section 2.9, Exercise 5)**.** Let R be a commutative ring, and S a submonoid of the multiplicative monoid of R. In $R \times S$, define $(a, s) \sim (b, t)$ if there exists a $u \in S$ such that $u(at - bs) = 0$.

(a) Show that this is an equivalence relation in $R \times S$.
(b) Denote the equivalence class of (a, s) as a/s and the quotient set consisting of these classes as RS^{-1}. Show that RS^{-1} becomes a ring relative to

$$a/s + b/t = (at + bs)/st$$
$$(a/s)(b/t) = ab/st$$
$$0 = 0/1$$
$$1 = 1/1.$$

(c) Show that $a \to a/1$ is a homomorphism of R into RS^{-1}.
(d) Show that the homomorphism given above is a monomorphism if and only if no element of S is a zero divisor in R.
(e) Show that the elements $s/1$, $s \in S$, are units in RS^{-1}.

Proof. (a) To show it's an equivalence class, we need to establish three things.
(1) (Reflexive) Notice that we have $(a, s) \sim (a, s)$, since $(as - as) = 0$, so we have $1 \in S$ satisfies the property that $1(as - as) = 0$.
(2) (Symmetric) If $(a, s) \sim (b, t)$, we have $u(at - bs) = 0$. Notice that $-u(bs - at) = u(at - bs) = 0$. Multiplying by -1 to both sides gives $u(bs - at) = (-1) \cdot 0 = 0$, so we have $(b, t) \sim (a, s)$.
(3) (Transitive) If $(a, s) \sim (b, t)$, and $(b, t) \sim (c, k)$, we wish to establish that $(a, s) \sim (c, k)$. Notice that we have $u, v \in S$ so that

$$u(at - bs) = 0, \quad v(bk - ct) = 0.$$

Hence, we have

$$uvk(at - bs) + uvs(bk - ct) = 0 \leftrightarrow uvt(ak - cs) + uvksb - uvksb = uvt(ak - cs) = 0.$$

Since S is a monoid, we have $uvt \in S$, and so $(a, s) \sim (c, k)$.

(b) We need to show that it is an abelian group with respect to addition, a monoid with respect to multiplication, and it satisfies the distributive properties. Throughout, $(a, s), (b, t)$ and (c, k) are arbitrary elements. To see that it is a group with respect to addition, we first check closure; notice that

$$(a, s) + (b, t) = (at + bs, st) \in RS^{-1}.$$

Next, we check associativity

$$(a, s) + ((b, t) + (c, k)) = (a, s) + (bk + ct, tk) = (atk + bks + cts, tks)$$
$$= (at + bs, st) + (c, k) = ((a, s) + (b, t)) + (c, k).$$

We see that 0 is the identity, since

$$(a,s)+(0,1)=(a,s)=(0,1)+(a,s).$$

We have inverses, since

$$(a,s)+(-a,s)=(as-as,s^2)=(0,s^2),$$

and we see

$$(0,s^2)\sim(0,1)\leftrightarrow 1(0-0)=0.$$

So $(a,s)+(-a,s)=(0,1)$. Finally, we see it's abelian, since

$$(a,s)+(b,t)=(at+bs,st)=(bs+at,ts)=(b,t)+(a,s).$$

To see that it's a monoid under multiplication, we first check closure; we have

$$(a,s)(b,t)=(ab,st)\in RS^{-1}.$$

Next, we check associativity;

$$(a,s)((b,t)(c,k))=(a,s)(bc,tk)=(abc,stk)=(ab,ts)(c,k)=((a,t)(b,s))(c,k).$$

Finally, we check that $1=1/1$ is the identity;

$$(a,s)(1,1)=(a,s)=(1,1)(a,s).$$

Hence, it's a monoid under multiplication. To finish, we need to check the distributive properties. That is,

$$(a,s)\cdot((b,t)+(c,k))=(a,s)\cdot(b,t)+(a,s)\cdot(c,k)$$

and

$$((a,s)+(b,t))\cdot(c,k)=(a,s)\cdot(c,k)+(b,t)\cdot(c,k).$$

The first follows, since

$$(a,s)\cdot((b,t)+(c,k))=(a,s)\cdot(bk+ct,tk)=(abk+act,tks),$$

$$(a,s)(b,t)+(a,s)(c,k)=(ab,st)+(ac,sk)=(absk+acst,s^2tk)=(s,s)(abk+act,stk)=(abk+act,stk),$$

by noticing that, as before, $(s,s)=(1,1)$. Likewise, the second follows, since

$$((a,s)+(b,t))(c,k)=(at+bs,st)(c,k)=(atc+bcs,stk),$$

$$(a,s)(c,k)+(b,t)(c,k)=(ac,sk)+(bc,tk)=(actk+bcsk,stk^k)=(k,k)(act+bcs,stk)=(act+bcs,stk).$$

So we have that RS^{-1} is a ring.

(c) To see that it is a homomorphism, we need to check four things. First, notice that $\phi(1)=(1,1)=1$ and $\phi(0)=(0,1)=0$, so it since the respective identities to identities. Next, notice that $\phi(a+b)=(a+b,1)=(a,1)+(b,1)=\phi(a)+\phi(b)$. Finally, we have $\phi(ab)=(ab,1)=(a,1)(b,1)$. So it's a homomorphism.

(d) ($\implies$) Assume that it is a monomorphism. Then $\ker(\phi)=0$, so $\phi(a)=0$ if and only if $a=0$. If there were an element of S that were a zero divisor, say t, we have that $ta=0$ for some $a\in S\subset R$ non-zero. Taking this a, we see that

$$\phi(a)=0\leftrightarrow(a,1)=(0,1)\leftrightarrow t(a)=0,$$

which contradicts our kernel being trivial. Hence, there cannot be an element of S that is a zero divisor.

($\impliedby$) Assume that no element of S is a zero divisor. Then we have that, for all $s\in S$,

$$sa=0\iff a=0.$$

Notice that this implies that

$$\phi(a)=(0,1)\iff(a,1)=(0,1)\iff s(a)=0\iff a=0.$$

So $\ker(\phi) = 0$, and thus ϕ is injective. Hence, it's a monomorphism.

(e) We need to show that there is an inverse for $(s, 1)$ in RS^{-1}. That is, some element (a, t) so that

$$(a, s)(s, 1) = (as, s) = (1, 1).$$

Recall that

$$(as, s) = (1, 1) \iff \exists t \in S \text{ such that } t(as - s) = 0 \iff ts(a - 1) = 0.$$

If we choose $a = 1$, $t = 1$, we get that

$$(1, s)(s, 1) = (s, s) = (1, 1)$$

as desired. So the elements $(s, 1)$ are invertible.

□

Problem 30 (Section 2.11, Exercise 7)**.** (a) Use the Chinese remainder theorem to show that if F is a field and $f(x) \in F[x]$ is monic and factors as $f(x) = g(x)h(x)$, $(g(x), h(x)) = 1$, then $F[x]/(f(x)) \cong F[x]/(g(x)) \oplus F[x]/(h(x))$.

(b) Show that if $f(x) = \prod_1^n (x - a_i)$ in $F[x]$ where the a_i are distinct, then $F[x]/(f(x)) = F \oplus \cdots \oplus F$ n times.

Proof. (a) Notice that, since $(g(x), h(x)) = 1$, we have that $(g(x)) + (h(x)) = 1$; that is, the ideals generated by them are relatively prime. To see this, we follow the proof of Bezout's identity for integers. Let $S = \{r(x)g(x) + s(x)h(x) \ : \ r(x), s(x) \in F[x]\}$. The well-ordering on degree gives us that there is a smallest element non-zero element, call it $w(x)$. The division algorithm then gives us that $g(x) = q(x)w(x) + t(x)$, where $\deg t < \deg w$. Furthermore, $t(x) = g(x) - q(x)w(x)$, so $t(x) \in S$. However, $\deg t <$ deg implies that t must be zero, and so we get that w divides g. Likewise, we get that w divides h. Any common divisor between g and h divides all the elements in S, and so in particular divides w. But this means that w is the greatest common divisor, which we have is 1, and so we get that there are polynomials so that

$$r(x)g(x) + s(x)h(x) = 1.$$

Next, we'd like to show that $(f(x)) = (g(x)) \cap (h(x))$. Notice that $f(x) = g(x)h(x)$ implies that $(f(x)) \subset (g(x)) \cap (h(x))$. For the other direction, take $p(x) \in (g(x)) \cap (h(x))$. Then we have that $p(x) = g(x)t(x)$, $p(x) = h(x)s(x)$. By the above, we have that there are polynomials $a(x), b(x)$ such that $a(x)g(x) + b(x)h(x) = 1$. Thus, we have that $p(x)a(x)g(x) + p(x)b(x)h(x) = p(x)$, and furthermore using the identities from prior we have that $h(x)s(x)a(x)g(x) + g(x)t(x)b(x)h(x) = p(x)$, or $f(x)(s(x)a(x) + t(x)b(x)) = p(x)$, and so $p(x) \in (f(x))$. So we get that the ideals are equal. Hence, the Chinese Remainder theorem tells us that

$$F[x]/((g(x)) \cap (h(x))) = F[x]/(f(x)) \cong F[x]/(g(x)) \oplus F[x]/(h(x)).$$

(b) Consider the case $n = 2$. Since a_1, a_2 are distinct, we get $(x - a_1, x - a_2) = 1$. Hence, by (a), we have that

$$F[x]/(f(x)) \cong F[x]/(x - a_1) \oplus F[x]/(x - a_2).$$

Notice that we have a map $\phi : F[x] \to F$ via evaluating a polynomial $f(x)$ at the point a_1. This is surjective, clearly, and we see that $\ker(\phi) = \{f(x) \in F[x] \ : \ f(a_1) = 0\}$. This must mean that $x - a_1 \mid f(x)$, and so $\ker(\phi) \subset (x - a_1)$, and clearly $(x - a_1) \subset \ker(\phi)$. Hence, $\ker(\phi) = (x - a_1)$. By the fundamental theorem of homomorphisms, we get that

$$F[x]/(x - a_1) \cong F.$$

Since the choice of a_1 was arbitrary, this also applies for a_2. Hence, we have

$$F[x]/(f(x)) \cong F \oplus F.$$

Now, assume by induction this holds for the case of $n-1$ linear factors. We wish to then show it holds for n linear factors. We can write this as $g(x) = \prod_1^{n-1}(x - a_i)$ and $h(x) = (x - a_n)$. Then we have $f(x) = g(x)h(x)$, and $(g(x), h(x)) = 1$, since the a_i are all distinct. By (a), this gives us

$$F[x]/(f(x)) \cong F[x]/(g(x)) \oplus F[x]/(x - a_n) \cong F[x]/(g(x)) \oplus F.$$

By the induction hypothesis, we have

$$F[x]/(g(x)) \cong F \oplus \cdots \oplus F$$

$n-1$ times, and so we get

$$F[x]/(f(x)) \cong F \oplus \cdots \oplus F$$

n times. Thus, by induction, the result holds.

□

Problem 31 (Section 2.12, Exercise 4)**.** Show that if f_0 and g_0 are two polynomials of degree less than q, and f_0 and g_0 define the same function, then $f_0 = g_0$.

Proof. Let $\zeta = \zeta_s : F[x] \to F[s]$ be defined by $\zeta(x) = s$ and $\zeta(r) = r$ for all $r \in F$, where $s = \mathrm{Id}$ is the identity function. Since f_0, g_0 define the same function, we have that $\zeta(f_0) = \zeta(g_0)$, or $\zeta(f_0 - g_0) = 0$, so that $f_0 - g_0$ are in the kernel. Notice that the isomorphism given on page 137 tells us that $f_0 - g_0 \in (x^q - x)$. That is, there is a $p \in F[x]$ such that $p(x^q - x) = f_0 - g_0$. The degree function tells us that $\deg(f_0 - g_0) = \deg(p) + q$. However, since $\deg(f_0 - g_0) < q$, this forces $\deg(p) = -\infty$; that is, we must have that $\deg(f_0 - g_0) = -\infty$, which tells us that $f_0 - g_0 = 0$. So, $f_0 = g_0$ in $F[x]$.

Not assuming that $r = 1$, we have that the degrees of f_0 and g_0 are less than q for every x_i. Furthermore, we have our substitution function is $\zeta = \zeta_{s_1,\dots,s_r} : F[x_1, \dots, x_r] \to F[s_1, \dots, s_r]$, where here the s_i are projection functions onto the ith coordinate. Again, we get that $\zeta(f_0) = \zeta(g_0)$, hence the difference is in the kernel, and so there are polynomials $p_1, \dots, p_r$ such that

$$f_0 - g_0 = p_1(x_1^q - x_1) + \cdots + p_r(x_r^q - x_r).$$

Restricting to each coordinate (e.g. view $f_0 - g_0 \in F[x_1, \dots, x_{r-1}][x_r]$), we see that the above argument tells us that the degree must be $-\infty$ with regards to each coordinate, and so we have that it is 0 in every coordinate. Hence, we have that $f_0 - g_0 = 0$, or $f_0 = g_0$ in the polynomial ring $F[x_1, \dots, x_r]$. □

Problem 32 (Section 2.12, Exercise 7)**.** Let $f(x_1, \dots, x_r)$ be a polynomial of degree $n < r$, the number of indeterminates. Assume $f(0, \dots, 0) = 0$. Prove that there exists $(a_1, \dots, a_r) \neq (0, \dots, 0)$ such that $f(a_1, \dots, a_r) = (0, \dots, 0)$.

Proof. We do this by doing the previous two problems.

Problem 33 (Section 2.12, Exercise 5)**.** Let $f(x_1, \dots, x_r)$ satisfy $f(0, \dots, 0) = 0$ and $f(a_1, \dots, a_r) \neq 0$ for every $(a_1, \dots, a_r) \neq (0, \dots, 0)$. Prove that if $g(x_1, \dots, x_r) = 1 - f(x_1, \dots, x_r)^{q-1}$, then

$$g(a_1, \dots, a_r) = \begin{cases} 1 \text{ if } (a_1, \dots, a_r) = (0, \dots, 0) \\ 0 \text{ otherwise.} \end{cases}$$

Proof. Since $f(a_1, \dots, a_r) \neq 0$ for every $(a_1, \dots, a_r)$, we have that Fermat's little theorem gives that $f(a_1, \dots, a_r)^{q-1} = 1$. Hence, we have that $1 - f(a_1, \dots, a_r)^{q-1}$ is non-zero if and only if $f(a_1, \dots, a_r)^{q-1} = 0$, which forces $f(a_1, \dots, a_r) = 0$, which only happens if $(a_1, \dots, a_r) = (0, \dots, 0)$. In this case, we get that it evaluates to 1. Thus, we have the resulting g. □

Problem 34 (Section 2.12, Exercise 6)**.** Show that the g of the prior exercise determines the same polynomial function as

$$f_0(x_1, \dots, x_r) = (1 - x_1^{q-1}) \cdots (1 - x_r^{q-1}).$$

Hence, prove that $\deg(g) \geq r(q-1)$.

Proof. Notice that we have $g = f_0$ as functions, since we have

$$f_0(a_1, \dots, a_r) = \begin{cases} 1 \text{ if } (a_1, \dots, a_r) = (0, \dots, 0) \\ 0 \text{ otherwise.} \end{cases}$$

If g has degree less than q in every x_i, then by **Problem 1** we get that these polynomials are equal, and so $\deg(g) = r(q-1)$. Otherwise, we have that g has degree greater than q in at least one x_i. We wish to show that $\deg(g) \geq r(q-1)$. Let h be the polynomial defined by taking the degrees of

the monomials of g modulo $q-1$; notice we have that $\deg(h) < \deg(g)$. We also notice that h has degree less than q in each variable, and so if we can show that $h = f_0$ as functions, we are done. But this is clear, since $F[x_1, \ldots, x_r]/(x_1^q - x_1, \ldots, x_r^q - x_r) \cong F[s_1, \ldots, s_r]$, and we have that $g = h$ as functions in $F[s_1, \ldots, s_r]$, since taking the degree modulo $q-1$ is the same as taking the image of g under this isomorphism, so $h = f_0$ as functions. So by the first problem, we get that $h = f_0$ as polynomials, and so $\deg(h) = r(q-1)$. Hence, for all possible g, we get that $\deg(g) \geq r(q-1)$ as desired. □

Assume $\deg(f) = n < r$, which is the number of indeterminates, and assume that for all $(a_1, \ldots, a_r) \neq (0, \ldots, 0)$ we have $f(a_1, \ldots, a_r) \neq (0, \ldots, 0)$. Then by **Problem 3**, we have that there is a $g(x_1, \ldots, x_r) = 1 - f(x_1, \ldots, x_r)^{q-1}$ which satisfies the criteria. By **Problem 4**, we see $\deg(g) \geq r(q-1)$. Finally, by the additive property of degree, we see that $\deg(1 - f(x_1, \ldots, x_r)^{q-1}) = n(q-1)$. However, we have a contradiction, since this implies that $n(q-1) \geq r(q-1) \implies n \geq r$. Thus, we must have at least one $(a_1, \ldots, a_r) \neq (0, \ldots, 0)$ such that $f(a_1, \ldots, a_r) = (0, \ldots, 0)$. □

Problem 35 (Section 2.13, Exercise 2)**.** Let $\Delta = \prod_{i<j}(x_i - x_j)$. Show that Δ^2 is symmetric, and express Δ^2 for $r = 3$ in terms of elementary symmetric polynomials.

Proof. We first show that Δ^2 is symmetric. Let $\pi \in \mathrm{Sym}(r)$. In the case where $r = 2$, we have that $\Delta = x_1 - x_2$. Notice that our options are $\pi = (12)$ or π is trivial. If $\pi = (12)$, we get that $x_{\pi(1)} - x_{\pi(2)} = -\Delta$, and so the automorphism applied to Δ^2 gives back Δ^2. Hence, it holds for $r = 2$.

Notice as well that if it holds for a transposition (ij) and another transposition (kl), then it holds for the product $(ij)(kl)$. This holds since, viewing $\pi = (ij)(kl)$, we have

$$\zeta(\pi)(\Delta) = \zeta(\pi)\left(\prod_{i<j}(x_i - x_j)\right) = \prod_{i<j}(x_{\pi(i)} - x_{\pi(j)}) = \zeta((ij))\left(\zeta((kl))\left(\prod_{i<j}(x_i - x_j)\right)\right).$$

That is, the flipping can be done in any order, and so it suffices to check it on transpositions.

Assume for induction Δ^2 is symmetric for $1 \leq k \leq r-1$. We wish to then establish it holds for r. It suffices to show it holds for any transposition of the form $\pi = (kr)$, $1 \leq k \leq r-1$ by the observations above. We wish to show that

$$\zeta(\pi)(\Delta) = (-1)^C \Delta,$$

for some constant C (one can determine this constant, however for our purposes it just matters that it's -1 to some power). This, however, is clear, since we're just permuting around variables; hence, we have that either the variables are flipped, in which case we multiply by (-1), or they are not flipped, in which case we multiply by 1. Regardless, we have at most a negative sign on the outside, and so once we square it we see that this goes away. That is, we see we have

$$\zeta(\pi)(\Delta^2) = \Delta^2.$$

So for any such transposition, we have that $\zeta(\pi)(\Delta^2) = \Delta^2$, and since $\mathrm{Sym}(r)$ is generated by products of transpositions, by the above remark, we have that for any $\pi \in \mathrm{Sym}(r)$,

$$\zeta(\pi)(\Delta^2) = \Delta^2.$$

Hence, we have that Δ^2 is a symmetric polynomial.

Notice that, for $r = 3$, $\Delta^2 = (x_1 - x_3)(x_2 - x_3)(x_1 - x_2)$. Writing this out, we have

$$f = x_1^2 x_2 - x_1^2 x_3 - x_1 x_2^2 + x_1 x_3^2 + x_2^2 x_3 - x_2 x_3^2.$$

We follow the procedure from the proof given in the class notes. That is, going by lexicographic ordering, the highest monomial is $x_1^2 x_2^1 x_3^0$, so we have $k_1 = 2$, $k_2 = 1$, $k_3 = 0$, and so going through

and doing this for each polynomial, we get

$$\Delta^2 - s_1^2 s_2^2 = f_1,$$
$$f_1 = -4x_1^4x_2x_2 - 4x_1^3x_2^3 - 6x_1^3x_2^2x_3 - 6x_1^3x_2x_3^2 - 4x_1^3x_3^3 - 6x_1^2x_2^3x_3 - 21x_1^2x_2^2x_3^2$$
$$-6x_1^2x_2x_3^3 - 4x_1x_2^4x_3 - 6x_1x_2^3x_3^2 - 6x_1x_2^2x_3^3 - 4x_1x_2x_3^4 - 2x_2^3x_3^3,$$
$$f_1 + 4s_1^3s_3 = f_2,$$
$$f_2 = -4x_1^3x_2^3+6x_1^3x_2^2x_3+6x_1^3x_2x_3^2-4x_1^3x_3^3+6x_1^2x_2^3x_3+3x_1^2x_2^2x_3^2+6x_1^2x_2x_3^3+6x_1x_2^3x_3^2+6x_1x_2^2x_3^3-4x_2^3x_3^3,$$
$$f_2 + 4s_2^3 = f_3,$$
$$f_3 = 18x_1^3x_2^2x_3 + 18x_1^3x_2x_3^2 + 18x_1^2x_2^3x_3 + 27x_1^2x_2^2x_3^2 + 18x_1^2x_2x_3^3 + 18x_1x_2^3x_3^2 + 18x_1x_2^2x_3^3,$$
$$f_3 - 18s_1s_2s_3 = f_4,$$
$$f_4 = -27x_1^2x_2^2x_3^2,$$
$$f_5 = f4 + 27s_3^2,$$
$$f_5 = 0,$$

and so going through all of the calculations we get

$$\Delta^2 = (s_1)^2(s_2)^2 - 4(s_1)^3s_3 - 4(s_2)^3 + 18(s_1)(s_2)(s_3) - 27s_3^2,$$

where

$$s_1 = x_1 + x_2 + x_3,$$
$$s_2 = x_1x_2 + x_1x_3 + x_2x_3,$$
$$s_3 = x_1x_2x_3.$$

□

Problem 36 (Section 2.14, Exercise 6)**.** Show that any prime is irreducible.

Proof. Let p be a prime. We wish to show that p is irreducible. Let b be a proper factor of p. Then we have that there is an a such that $ab = p$. If p did not divide a, we have that p does not divide ab, which is a contradiction, and so we must have that p divides a. Hence, there is an r so that $pr = a$. Substituting this in, we get $(pr)b = p$, or $p(br - 1) = 0$. Since $p \neq 0$, this forces $br = 1$, which means that b is a unit. Hence, any proper factor of p is a unit, and so p is irreducible. □

Problem 37 (Section 2.14, Exercise 7)**.** Let $\mathbb{Z}[\sqrt{10}]$ be the set of real numbers of the form $a+b\sqrt{10}$, where $a, b \in \mathbb{Z}$. Show that $\mathbb{Z}[\sqrt{10}]$ is not factorial.

Proof. Notice that we have

$$10 = 2 \cdot 5 = (\sqrt{10}) \cdot (\sqrt{10}).$$

Define the norm by

$$N(r) = a^2 - 10b^2,\ r = a + b\sqrt{10}.$$

Then it's a quick calculation to see that $N(rs) = N(r)N(s)$. We wish to show that there are no common irreducible elements to 2 and $\sqrt{10}$, and likewise $\sqrt{10}$ and 5. Hence, even if these were not irreducible elements, they would not share the same factorization, and so we have two different factorizations. Notice that $N(2) = 4$, $N(\sqrt{10}) = -10$. So if x irreducible is such that $x \mid 2$, $x \mid \sqrt{10}$, then we have that $N(x) \mid 4$ and $N(x) \mid -10$. Since $4 \nmid -10$, it suffices to show that there is no x so that $N(x) = \pm 2$.

Assume $N(x) = 2$. Then we have

$$a^2 - 10b^2 = 2.$$

Taking this mod 2, we see that

$$a^2 \equiv 0 \pmod 2 \implies a \equiv 0 \pmod 2.$$

Hence, a is even. Taking this mod 4 gives

$$-10b^2 \equiv 2 \pmod 4,$$

and checking this by hand shows that b is odd. Hence, we have that $a = 2k$, $b = 2d + 1$, and so we write this as

$$4k^2 - 10(2d+1)^2 = 2 \leftrightarrow 4k^2 - 40d^2 - 40d - 10 = 2.$$

Taking this modulo 10 gives us

$$4k^2 = 2 \pmod{10},$$

which has no solutions, and so there is no such x.

Likewise, assume $N(x) = -2$. Then we have

$$a^2 - 10b^2 = -2.$$

Taking mod 2 again gives a even, and taking mod 4 gives that b is odd. So following the same procedure and taking it mod 10, we have

$$4k^2 = 8 \pmod{10},$$

which also has no solutions, and so there is no such x.

Hence, we have that there is no common irreducible element to 2 and $\sqrt{10}$. Likewise, we see $N(5) = 25$, and so we need to show that there is no x such that $N(x) = \pm 5$. Again, assume $N(x) = 5$. Then we have

$$a^2 - 10b^2 = 5.$$

Taking this mod 5 gives $a^2 \equiv 0 \pmod 5$, so $a = 5k$. Taking it mod 25 gives $-10b^2 \equiv 5 \pmod{25}$. However, there is no solution, and so no such x exists.

Assuming $N(x) = -5$, we again get that $a = 5k$, and so taking mod 25 gives $-10b^2 \equiv -5 \pmod{25}$, which again has no solutions. So no such x exists. Hence, we have that 5 and $\sqrt{10}$ cannot share any irreducible elements. We have 10 has two different factorizations, and so the ring cannot be factorial. $\square$

Problem 38 (Section 2.15, Exercise 4)**.** Let D be a PID, E a domain containing D as a subring. Show that if d is a gcd of a and b in D, then d is also a gcd of a and b in E.

Proof. If $\gcd(a,b) = d$, then we have that $(a,b) = (d)$, since we are in a PID. That is, there are $e, f \in D$ such that $ae + bf = d$. We need to show that d is the gcd in E; that is, if $l \mid a$, $l \mid b$, then $l \mid d$. Notice that if $l \mid a$, we have that there is a $g \in E$ such that $gl = a$, and likewise we have a $t \in E$ such that $lt = b$. Hence, using the fact that $ae + bf = d$, we have

$$ae + bf = (gl)e + (lt)b = l(ge + tb) = d,$$

so that $l \mid d$. Hence, we get that d is the gcd of a and b in E. □

Problem 39 (Section 2.15, Exercise 11)**.** Let a_1, a_2 be non-zero elements of a Euclidean domain. Define a_i and q_i recursively by $a_1 = q_1 a_2 + a_3$, $a_i = q_i a_{i+1} a_{i+2}$ where $\delta(a_{i+2}) < \delta(a_{i+1})$. Show that there exists an n such that $a_n \neq 0$ but $a_{n+1} = 0$ and that $d = a_n = (a_1, a_2)$. Also use the equations to obtain an expression for d in the form $xa_1 + ya_2$.

Proof. By the definition of a Euclidean domain, since $a_1, a_2 \neq 0$, we have that there are q_1, a_3 such that

$$a_1 = q_1 a_2 + a_3,$$

where $\delta(a_3) < \delta(a_2)$. We can then define a_i and q_i recursively in this form; that is, now with a_2, a_3, we have

$$a_2 = q_2 a_3 + a_4,$$

where $\delta(a_4) < \delta(a_3)$. Since this is a strictly decreasing sequence, and $\delta(a_1) < \infty$, we have that eventually there is an a_n such that $\delta(a_n) = 0$ by the well-ordering principle. Notice that if $a_n \neq 0$, we have that a_{n+1} must be zero, since $\delta(a_{n+1}) < \delta(a_n)$, but $\delta(a_n)$ is the smallest such degree by assumption. If a_n is 0, then $\delta(a_n)$ is strictly the smallest value in the chain, and so $a_{n-1} \neq 0$. Hence, it is fine after relabeling to let n be the value such that $a_n \neq 0$, $a_{n+1} = 0$.

Next, we show that a_n divides a_i for all i. Notice that it holds for a_{n-1}, since

$$a_{n-1} = q_{n-1} a_n.$$

Assume by induction it holds for $n - 1 \geq i > 1$. We wish to show it holds for a_{i-1}. But we see this follows, since

$$a_{i-1} = q_{i-1} a_i + a_{i+1},$$

and since $a_n \mid a_i$, $a_n \mid a_{i+1}$ by assumption, we have that there are d, f so that $da_n = a_i$, $fa_n = a_{i+1}$, and so

$$a_{i-1} = a_n \left(q_{i-1} d + f \right).$$

Hence, $a_n \mid a_{i-1}$, and so we get that it holds for all such i. So $a_n \mid a_2$, $a_n \mid a_1$.

Next, we need to show it is the greatest such divisor. Notice that we have

$$a_1 = q_1 a_2 + a_3,$$

and we can rewrite this as

$$a_3 = a_1 - q_1 a_2.$$

So a_3 is a linear combination of a_1, a_2. Assume that we can describe a_i as a linear combination of a_1, a_2 for $3 \leq i < n$, we wish to show it holds for $i + 1$. The hypothesis gives us that

$$a_{i-1} = q_{t-1} a_i + a_{i+1},$$

and so we can write

$$a_{i+1} = q_{t-1} a_i + a_{i-1}.$$

Since we have a_i, a_{i-1} can be described in linear combinations, we have u_1, u_2, v_1, v_2 such that

$$a_{i-1} = u_1 a_1 + u_2 a_2,$$
$$a_i = v_1 a_1 + v_2 a_2,$$

and so

$$a_{i+1} = q_{t-1}(v_1 a_1 + v_2 a_2) + (u_1 a_1 + u_2 a_2),$$

and so after grouping terms we get

$$a_{i+1} = a_1(q_{t-1} v_1 + u_1) + a_2(q_{t-1} v_2 + u_2),$$

and hence a_{i+1} can be described as a linear combination of a_1, a_2. So we have that it holds for all $1 \leq i \leq n$, and hence we can write

$$a_n = x a_1 + y a_2,$$

where x, y are values in our Euclidean domain. Assume now that $l \mid a_1$, $l \mid a_2$. Then we have that there are u, v such that

$$ul = a_1,$$
$$vl = a_2,$$

and hence

$$a_n = x(ul) + y(vl) = l(xu + yv).$$

Hence, $l \mid a_n$, and so a_n is the greatest common divisor. That is, $(a_1, a_2) = a_n$. □

Problem 40 (Section 2.16, Exercise 2)**.** Prove the following irreducibility criterion due to Eisenstein. If $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$, and there exists a prime p such that $p \mid a_i$, $0 \leq i \leq n-1$, $p \nmid a_n$, and $p^2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. Assume for contradiction that $f(x)$ factors into polynomials over $\mathbb{Q}[x]$; say, $f(x) = g(x)h(x)$, $g(x)$, $h(x) \in \mathbb{Q}[x]$. That is, we have

$$h(x) = b_0 + b_1 x + \cdots + b_r x^r,$$
$$g(x) = c_0 + c_1 x + \cdots + c_s x^s,$$

where $n = r + s$, and $b_i, c_i \in \mathbb{Q}$. Since we must have $b_0 c_0 = a_0$, and we have $p \mid a_0$, we get that $p \mid b_0 c_0$. Notice that we cannot have $p \mid b_0$ and $p \mid c_0$, as this implies that $p^2 \mid a_0$. So without loss of generality, assume $p \mid b_0$, $p \nmid c_0$. Since $b_r c_s = a_n$, and $p \nmid a_n$, we have $p \nmid b_r$, $p \nmid c_s$. Now, notice that we can write

$$a_k = \sum_{i+j=k} c_i b_j = c_0 b_k + c_1 b_{k-1} + \cdots + c_k b_0,$$

where if $c_i b_j$ are not within the bounds of their respective indices we rewrite them as 0. Hence, we have

$$a_r = c_r b_0 + \cdots + b_r c_0.$$

Notice that we have that $p \mid b_0$. We show that $p \mid b_i$ for $0 \leq i \leq r-1$. Once established, this implies that, since a_r is divisible by p, we must have that $p \mid b_r c_0$, which results in a contradiction since $p \nmid b_r$, $p \nmid c_0$.

We have

$$a_1 = c_0 b_1 + b_1 c_0.$$

Since $p \nmid c_0$, this forces $p \mid b_1$. Assume by induction it holds for $0 \leq t < r-1$, we wish to show it holds for $t+1$. We expand

$$a_{t+1} = c_0 b_{t+1} + c_1 b_t + \cdots + c_{t+1} b_0.$$

Again, since $p \nmid c_0$, $p \mid a_{t+1}$, we have that $p \mid b_{t+1}$. Hence, it holds by induction. □

Problem 41 (Section 2.16, Exercise 6)**.** Let F be a field and $f(x)$ an irreducible polynomial in $F[x]$. Show that $f(x)$ is irreducible in $F(t)[x]$, t an indeterminate.

Proof. Assume for contradiction that $f(x)$ is reducible in $F(t)[x]$. Then by the contrapositive of Lemma 3 (Gauss Lemma 2), we have that $f(x)$ is reducible in $F[t][x] = F[x][t]$ or it does not have positive degree. Not having positive degree implies that it is either 0 or a constant in F; since $f(x)$ is irreducible in $F[x]$, we have that it is neither of these, and so $f(x)$ must be reducible in $F[x][t]$. Let $D = F[x]$, then we have that $f(x)$ is reducible in $D[t]$. That is, $f(x) = g(t)h(t)$, where $g(t), h(t) \in D[t]$ are non-units with coefficients as polynomials in $F[x]$. Notice that this means we can write

$$g(t) = a_0 + a_1 t + \cdots + a_r t^r,$$
$$h(t) = b_0 + b_1 t + \cdots + b_s t^s,$$

where $a_i, b_i \in D$. Since $\deg(f) = 0$ with respect to t, we have that $g(t) = a_0$, $h(t) = b_0$. In other words, we have that $f(x) = a_0 b_0$, $a_0, b_0 \in D = F[x]$. Since $f(x)$ is irreducible with respect to $F[x]$, we must have that a_0 or b_0 is a unit in F; thus, we have a contradiction. □

Problem 42 (Section 3.1, Exercise 4)**.** Determine $\mathrm{End}(\mathbb{Q}, +, 0)$.

Proof. We want to determine the collection of maps ζ such that $\zeta(x+y) = \zeta(x)+\zeta(y)$. Let $p/q \in \mathbb{Q}$. Notice that if $q = 1$, we have that $p \in \mathbb{Z}$, and so we have that

$$\zeta(p) = \zeta(1 + \cdots + 1) = \zeta(1) + \cdots + \zeta(1) = p\zeta(1).$$

Next, if $q \neq 1$, we have that

$$\zeta(p) = \zeta\left(\frac{p}{q} + \cdots + \frac{p}{q}\right) = \zeta\left(\frac{p}{q}\right) + \cdots + \zeta\left(\frac{p}{q}\right) = q\zeta\left(\frac{p}{q}\right).$$

Hence, notice that

$$\zeta\left(\frac{p}{q}\right) = \frac{p}{q}\zeta(1);$$

that is, these endomorphisms are completely determined by where they send 1. We claim that this gives us a bijection from $\mathrm{End}(\mathbb{Q}, +, 0)$ into $\mathbb{Q}$ via $\varphi(\zeta) = \zeta(1)$. To see that it's well-defined, notice that if $\zeta = \gamma$, then $\zeta(1) = \gamma(1)$ clearly, so $\varphi(\zeta) = \varphi(\gamma)$. To see it's injective, notice that if $\varphi(\zeta) = \zeta(1) = \gamma(1) = \varphi(\gamma)$, then for any $t \in \mathbb{Q}$, we have that $\zeta(t) = t\zeta(1) = t\gamma(1) = \gamma(t)$, and so $\zeta = \gamma$. Finally, for surjectivity, notice that for any $t \in \mathbb{Q}$ we can define the map ζ by $\zeta(1) = t$. This is an endomorphism, since $\zeta(0) = 0, \zeta(1) = t$ and $\zeta(x + y) = t(x + y) = tx + ty = \zeta(x) + \zeta(y)$. So we have a bijection.

Since $\mathrm{End}(\mathbb{Q}, +, 0)$ is a ring, we would also like to check that whether this is a ring isomorphism. Notice that $0 \in \mathrm{End}(\mathbb{Q}, +, 0)$ is the map which sends everything to 0; hence, $\varphi(0) = 0$. Notice as well that $\varphi(1) = 1$, where $1 \in \mathrm{End}(\mathbb{Q}, +, 0)$ is the identity map. Finally, for ζ, γ, we have

$$\varphi(\gamma + \zeta) = (\gamma + \zeta)(1) = \gamma(1) + \zeta(1) = \varphi(\gamma) + \varphi(\zeta),$$
$$\varphi(\gamma \circ \zeta) = (\gamma(\zeta(1))) = \gamma(1)\zeta(1) = \varphi(\gamma)\varphi(\zeta).$$

So φ is a bijective ring homomorphism, or a ring isomorphism. Hence, we have $\mathrm{End}(\mathbb{Q}, +, 0) \cong \mathbb{Q}$. □

Problem 43 (Section 3.5, Exercise 5)**.** Let M and N be R modules, $f : M \to N$, $g : N \to M$ R module homomorphisms such that $(f \circ g)(y) = y$ for all $y \in N$. Show that $M = \ker(f) \oplus \mathrm{Im}(g)$.

Proof. First, we note that $\mathrm{Im}(g)$, $\ker(f)$ are submodules of M. Let $a, b \in \ker(f)$, then $a-b \in \ker(f)$, since $f(a-b) = f(a) - f(b) = 0 - 0 = 0$, and if $r \in R$, we have that $f(ra) = rf(a) = r0 = 0$, so $ra \in \ker(f)$. Hence, it's a subgroup under addition, and it's closed under the R action.

Likewise, we show that $\mathrm{Im}(g)$ is a submodule. Let $a, b \in \mathrm{Im}(g)$. Then we have $x, y \in N$ such that $g(x) = a$, $g(y) = b$. So we get that $a - b \in \mathrm{Im}(g)$, since $g(x-y) = g(x) - g(y) = a - b$. Hence, it's a subgroup under addition. Let $r \in R$, then we have that $ra = rg(x) = g(rx)$, so $ra \in N$. Hence, it's closed under the R action. Thus, it's a submodule.

Next, take $m \in M$. Notice that we can write m as

$$m = g(f(m)) - (g(f(m)) - m).$$

It's clear that $g(f(m)) \in \mathrm{Im}(g)$, so it suffices to show that $g(f(m)) - m \in \ker(f)$. To see this, we notice that

$$f\left(g(f(m)) - m\right) = f(g(f(m))) - f(m)$$

using module homomorphism properties. Next, we have that $f(g(x)) = x$, and so $f(g(f(m))) = f(m)$. Hence,

$$f(g(f(m))) - f(m) = f(m) - f(m) = 0,$$

so $g(f(m)) - m \in \ker(f)$. Hence, $M = \ker(f) + \mathrm{Im}(g)$.

Next, we need to show that $\ker(f) \cap \mathrm{Im}(g) = 0$. Let $a \in \ker(f) \cap \mathrm{Im}(g)$. Since $a \in \mathrm{Im}(g)$, we have that there is an $x \in N$ such that $g(x) = a$. Since $a \in \ker(f)$, we have that $f(a) = (f \circ g)(x) = 0$. Since $(f \circ g)(y) = y$ for all $y \in N$, this forces $x = 0$, which then forces $a = 0$. Thus, we must have $\ker(f) \cap \mathrm{Im}(g) = 0$.

By **Theorem 3.5**, we see that $M = \ker(f) \oplus \mathrm{Im}(g)$. □

Problem 44 (Section 3.6, Exercise 2)**.** Find a basis for the submodule of $\mathbb{Q}[\lambda]^{(3)}$ generated by $f_1 = (2\lambda - 1, \lambda, \lambda^2 + 3)$, $f_2 = (\lambda, \lambda, \lambda^2)$, $f_3 = (\lambda + 1, 2\lambda, 2\lambda^2 - 3)$.

Proof. Create a 3×3 matrices with our generators as rows; that is, we have

$$\begin{pmatrix} 2\lambda - 1 & \lambda & \lambda^2 + 3 \\ \lambda & \lambda & \lambda^2 \\ \lambda + 1 & 2\lambda & 2\lambda^2 - 3 \end{pmatrix}.$$

We do Gaussian elimination to find the generators. Notice that this will preserve the span of the elements.

We want to first shift it so we have the smallest element is in the top left, so we have

$$\begin{pmatrix} \lambda & \lambda & \lambda^2 \\ \lambda + 1 & 2\lambda & 2\lambda^2 - 3 \\ -2\lambda + 1 & -\lambda & -\lambda^2 - 3 \end{pmatrix}.$$

Subtracting the first row from the second gives

$$\begin{pmatrix} \lambda & \lambda & \lambda^2 \\ 1 & \lambda & \lambda^2 - 3 \\ 2\lambda - 1 & \lambda & \lambda^2 + 3 \end{pmatrix}.$$

Subtracting the first row from the third gives

$$\begin{pmatrix} \lambda & \lambda & \lambda^2 \\ 1 & \lambda & \lambda^2 - 3 \\ \lambda - 1 & 0 & 3 \end{pmatrix}.$$

Subtracting the first row from the third again gives

$$\begin{pmatrix} \lambda & \lambda & \lambda^2 \\ 1 & \lambda & \lambda^2 - 3 \\ -1 & -\lambda & 3 - \lambda^2 \end{pmatrix}.$$

Adding the second to the third gives

$$\begin{pmatrix} \lambda & \lambda & \lambda^2 \\ 1 & \lambda & \lambda^2 - 3 \\ 0 & 0 & 0 \end{pmatrix}.$$

We then show that these elements are linearly independent. Let $a \in \mathbb{Q}[x]$, $b \in \mathbb{Q}[x]$, then

$$a(\lambda, \lambda, \lambda^2) + b(1, \lambda, \lambda^2 - 3) = (0, 0, 0).$$

Hence, we need to find a, b such that

$$a\lambda + b = 0,$$
$$(a + b)\lambda = 0,$$
$$(a + b)\lambda^2 - 3b = 0.$$

Notice that the second equation tells us that $a = -b$. So substituting this in to the

$$a\lambda - a = 0,$$
$$3a = 0.$$

Thus, the third condition tells us that $a = 0$, and so we have $a = b = 0$ are the only $a, b \in \mathbb{Q}[x]$ such that they satisfy the conditions. Hence, we have that $(\lambda, \lambda, \lambda^2)$ and $(1, \lambda, \lambda^2 - 3)$ form a basis for the submodule. □

Problem 45 (Section 3.7, Exercise 9)**.** Show that if $A \in M_{m,n}(D)$, D a pid, then A and A^t have the same invariant factors.

Proof. We have that

$$QAP = \operatorname{diag}(d_1, \ldots, d_r, 0, \ldots, 0),$$

where Q and P are appropriate matrices formed by products of elementary matrices of type I, II, and III. Taking the transpose of both sides gives

$$(QAP)^t = (\operatorname{diag}(d_1, \ldots, d_r, 0, \ldots, 0))^t = \operatorname{diag}(d_1, \ldots, d_r, 0, \ldots, 0).$$

Transpose is an anti-homomorphism, since $(AB)^t = B^t A^t$, so using this we have that

$$(QAP)^t = P^t A^t Q^t = \operatorname{diag}(d_1, \ldots, d_r, 0, \ldots, 0).$$

We need to show that if $P \in \mathrm{GL}_n(D)$, then $P^t \in \mathrm{GL}_n(D)$. This, however, is clear by using the antihomomorphism property of transpose; since. $P \in \mathrm{GL}_n(D)$, we have that there is a P^{-1} such that $PP^{-1} = P^{-1}P = I$, and taking the transpose gives $(PP^{-1})^t = (P^{-1})^t P^t = I^t = I = P^t(P^{-1})^t = (P^{-1}P)^t$. So A^t is equivalent to $\operatorname{diag}(d_1, \ldots, d_r, 0, \ldots, 0)$, and we see that $d_i \mid d_j$ if $i \leq j$ still. Hence, A and A^t share the same invariant factors. □

Problem 46 (Section 3.8, Exercise 3)**.** Let M be the ideal in $\mathbb{Z}[x]$ generated by 2 and x. Show that M is not a direct sum of cyclic $\mathbb{Z}[x]$-modules.

Proof. We have that $M = (2, x)$. We wish to show that $M \neq \mathbb{Z}[x]a_1 \oplus \cdots \oplus \mathbb{Z}[x]a_n$. Assume it was the case, then we have that M is expressible in terms of principal ideals. That is, we have principal ideals (a_i) such that $M = \sum(a_i)$. Part of being a direct sum means that the (a_i) need to be disjoint. But this is not the case for principal ideals over $\mathbb{Z}[x]$; if $a \in (a_i)$, $b \in (a_j)$, then we have that $ab \in (a_i) \cap (a_j)$, so the intersection for $n > 1$ will be non-trivial. Hence, this must mean that $M = (a)$ for some $a \in \mathbb{Z}[x]$. So we must have that $(a) \subset (2, x)$ and $(2, x) \subset (a)$. But if $(2, x) \subset (a)$, this means that $(2) \subset (a)$ and $(x) \subset (a)$. If $(2) \subset (a)$, this means that $a \mid 2$. Since 2 is irreducible in $\mathbb{Z}[x]$, this must mean that either a is a unit or a is 2. Next, $(x) \subset (a)$ implies that $a \mid x$, and so since x is irreducible we have that a is a unit or $a = x$. Since we need both conditions, this forces a to be a unit, which means that $(2, x) = \mathbb{Z}[x]$. However, this is a contradiction, since $(2, x)$ is clearly not the whole ring (for example, $5 \notin (2, x)$), and so we cannot have that $(2, x)$ is principally generated. Hence, $(2, x)$ cannot be decomposed into a direct sum of cyclic $\mathbb{Z}[x]$ modules. □

Problem 47 (Section 3.9, Exercise 2)**.** Show that a torsion module M over a pid D is irreducible if and only if $M = Dz$ and $\text{ann}(z) = (p)$, p a prime. Show that if M is finitely generated then M is indecomposable in the sense that M is not a direct sum of two non-zero submodules if and only if $M = Dz$, where $\text{ann}(z) = 0$ or $\text{ann}(z) = (p^e)$, p a prime.

Proof. Recall that a module is said to be *irreducible* if $M \neq 0$ and 0 and M are the only submodules of M. We first show the following:

Problem 48 (Section 3.3, Exericse 7)**.** A module M is irreducible if and only $M \neq 0$ and M is cyclic with every non-zero element as a generator.

Proof. ($\implies$) If M is irreducible, then it's clear that $M \neq 0$ by definition. Furthermore, taking $0 \neq x \in M$, we have that $0 \subsetneq Dx \subset M$, and so $Dx = M$. Hence, M is cyclic, and every nonzero element is a generator.
($\impliedby$) Let M be cyclic; that is, $M = Dx$ for some x. If $0 \subset N \subset M$, take $y \in N$, we have that $Dy \subset N \subset M$, but since $y \in N \subset M$, this implies $Dy = M$, and so we have $M \subset N \subset M$, or $M = N$. So there are no non-trivial proper submodules. □

We now establish the first part.
($\implies$) Assume that M is torsion and irreducible. Let $0 \neq z \in M$. By above, we have that $M \neq 0$ and $M = Dz$. Since M is torsion, we must have $\text{ann}(z) \neq (0)$. By the lemma and the remark right after (**page 190**), we see that if $\text{ann}(z) \neq (p^e)$, $e \geq 1$ and p a prime, we get a contradiction, since there must be non-zero proper submodules of M or, in the case that $\text{ann}(z) = D$, we have that M is the 0 module, which contradicts irreducibility as well. Notice as well by the remark in the invariance theorem, we have that if $e \neq 1$, we can find a non-trivial proper submodule of the form $p^{e-1}M \subset M$. Hence, we must have that $e = 1$, and so $M = Dz$, where $\text{ann}(z) = (p)$.
($\impliedby$) We first show the following claim.

Claim 19. A module M is irreducible if and only if M is isomorphic to R/I for a maximal ideal I.

Proof. ($\implies$) Assume M is irreducible. Then by prior, $0 \neq M = Dz$ for some $z \in M$. Take the map $f : D \to Dz$ via $f(r) = rz$. Then this is a module homomorphism, since $f(r+s) = (r+s)z = rz + sz = f(r) + f(s)$, $f(rs) = (rs)z = r(sz) = rf(s)$. Notice that for all $m \in M$, we have $m = rz$, and so $f(r) = m$. Hence, f is surjective. By the fundamental homomorphism theorem, we get $M \cong R/\ker(f)$. So it suffices to show that the kernel is an ideal, and it is maximal.

To see it's an ideal, notice that for all $a, b \in \ker(f)$, $a-b \in \ker(f)$, since $f(a-b) = f(a)-f(b) = 0$, and $0 \in \ker(f)$, so it's subgroup under addition. Let $r \in R$, $a \in \ker(f)$, then we have that $ra \in \ker(f)$, since $f(ra) = rf(a) = r0 = 0$, and likewise for ar. So the kernel is indeed an ideal.

To see it is maximal, let $\ker(f) \subset J \subset R$ be some ideal. The correspondence theorem tells us that $J/\ker(f) \subset R/\ker(f) \cong M$ is an ideal, and moreover a submodule. Since M is irreducible, we must have that $J/\ker(f) = R/\ker(f)$ or $J/\ker(f) = 0$; that is, $J = \ker(f)$ or $J = R$. Hence, we get that $\ker(f)$ is a maximal ideal.
($\Longleftarrow$) Let $M \cong R/I$, I a maximal ideal (notice implicitly this says that $M \neq 0$). Take $N \subset M \cong R/I$ a submodule. Since it's a submodule, it must be closed under the action and it must be an additive subgroup; in other words, it must be an ideal in R/I. Since I is maximal, R/I is a field, so the only ideals are (0) (which corresponds to $N = 0$) or (1) (which corresponds to $M = N$). Hence, we have that M is irreducible. □

So we have $M = Dz$ by assumption, $M \cong R/\text{ann}(z)$, and since $\text{ann}(z) = (p)$, we have that (p) is a maximal ideal (since the principal ideal generated by an irreducible element in a PID gives a maximal ideal), so M is irreducible.

Next, we need to show that if M is finitely generated, then M is *indecomposable* in the sense that M is not a direct sum of two non-zero submodules if and only if $M = Dz$, where $\text{ann}(z) = 0$ or $\text{ann}(z) = (p^e)$, where p a prime.

($\Longrightarrow$) Assume that M is indecomposable. Since M is finitely generated, we can write it as $M = \text{tor}(M) \oplus N$, where N is a free submodule of M. Since M is indecomposable, we must have either M is torsion or M is free. If M is torsion, the classification theorem (**Theorem 3.12**) tells us that $M = Dz$, and we have that $\text{ann}(z) \neq 0$. Notice that this forces $\text{ann}(z) = (p^e)$ for some $e \geq 1$, where p is a prime, since otherwise we would be able to write it as a direct sum of two non-zero submodules by the lemma and its remark (**page 190**).

If M is free, then we have that M has a basis $\{x_1, \ldots, x_n\}$, and $M = Dx_1 \oplus \cdots \oplus Dx_n$. Since M is indecomposable, we must have that M is generated by one element, say z. So we have $M = Dz$. Since M has no torsion, we must have that $\text{ann}(z) = 0$. So we have the desired result.
($\Longleftarrow$) Assume that $M = Dz$, where $\text{ann}(z) = 0$ or $\text{ann}(z) = (p^e)$, p a prime. In the first case, we have that M has no torsion, and so is a free module – in particular, this means that M is indecomposable, since it has a basis consisting of one element. In the latter case, since $\text{ann}(z) = (p^e)$ and M is torsion, we have that the invariance theorem tells us that we cannot write it as a direct sum of two submodules. In either case, we have that M is indecomposable. □

Problem 49 (Section 3.10, Exercise 2)**.** Let $\mathbb{Z}^{(n)}$ be the free $\mathbb{Z}$-module with base $(e_1, \dots, e_n)$, K the submodule generated by the elements $f_i = \sum_1^n a_{ij}e_j$ where $a_{ij} \in \mathbb{Z}$ and $d = \det(a_{ij}) \neq 0$. Show that

$$|\mathbb{Z}^{(n)}/K| = |d|.$$

Proof. Let M be the module such that $M \cong \mathbb{Z}^{(n)}/K$. Then M is a finitely generated abelian group. Using the fundamental structure theorem for finitely generated modules over a pid, we have that we can diagonalize $A = (a_{ij})$ to get $PAQ = \text{diag}\{d_1, \dots, d_r, 0, \dots, 0\}$. Now, since $\det(A) = d \neq 0$, we have that the diagonal row is full; that is, $PAQ = \text{diag}\{d_1, \dots, d_n\}$. This is due to the fact that determinant is multiplicative, and sends the elements to the underlying ring, so $\det(PAQ) = \det(P)\det(A)\det(Q) = \prod_{i=1}^r d_r \cdot \prod_{r+1}^n 0$, and since $\det(P), \det(A), \det(Q) \neq 0$, we cannot have any 0's along the diagonal. Thus, we get

$$M = \bigoplus_{i=1}^n \mathbb{Z}y_i,$$

where y_i is such that $\text{ann}(y_i) = (d_i)$. Recall that

$$\mathbb{Z}y_i \cong \mathbb{Z}/(d_i),$$

so

$$M = \bigoplus_{i=1}^n \mathbb{Z}/(d_i).$$

Now, we have that

$$|\mathbb{Z}/(d_i)| = d_i,$$

taking the d_i to be positive without loss of generality and

$$|\mathbb{Z}/(d_i) \oplus \mathbb{Z}/(d_k)| = d_i \cdot d_k$$

via properties of groups, so inducting gives

$$|M| = \prod_{i=1}^n d_i.$$

Finally, it remains to show that $\prod_{i=1}^n d_i = |d|$. Recall by **Theorem 3.9** we have the following formula for the d_i (the theorem says up to units, but the only units in $\mathbb{Z}$ are ± 1, so just taking the absolute value of the determinant gives us this);

$$d_1 = \Delta_1, \ d_r = \Delta_r \Delta_{r-1}^{-1},$$

where Δ_j is the gcd of the i-rowed minors of A. In this case, we get

$$\prod_{i=1}^n d_i = \Delta_1 \cdot (\Delta_2 \cdot \Delta_1^{-1}) \cdot \dots \cdot (\Delta_n \cdot \Delta_{n-1}^{-1}) = \Delta_n = |d|,$$

since we take the d_i to be positive. □

Problem 50 (Section 3.10, Exercise 8)**.** Prove that any nilpotent matrix in $M_n(F)$ is similar to a matrix of the form

$$\begin{pmatrix} N_1 & & & 0 \\ & N_2 & & \\ & & \ddots & \\ 0 & & & N_3 \end{pmatrix},$$

where N_i has the form

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Proof. Let $M \in M_n(F)$ be a nilpotent matrix. That is, there exists an r such that $M^r = 0$. We find the characteristic polynomial of this matrix; that is, we have

$$f(\lambda) = \det(\lambda I - M) = \lambda^n - a_1\lambda^{n-1} + \cdots + (-1)^n a_n.$$

In a geometric series sort of fashion, notice that we have

$$(\lambda I - M)(\lambda^{r-1}I + \lambda^{r-2}IM + \cdots + M^{r-1}) = \lambda^r I + \lambda^{r-1}IM + \cdots + \lambda IM - \lambda^{r-1}IM - \lambda^{r-2}IM^2 - \cdots - M^r = \lambda^r I.$$

So we have $f(\lambda) \mid \lambda^{rn}$ after taking determinants of both sides. Hence, this forces $f(\lambda) = \lambda^n$. Thus, we must have that any invariant factors are of the form λ^k for $0 \leq k \leq n$.

Since the invariant factors are linear, with root zero, the Jordan canonical form tells us that our matrix is similar to a matrix of the form

$$\begin{pmatrix} N_1 & & & 0 \\ & N_2 & & \\ & & \ddots & \\ & 0 & & N_3 \end{pmatrix},$$

where N_i has the form

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

□

Problem 51 (Section 3.10, Exercise 9)**.** Show that a matrix $A \in M_n(\mathbb{C})$ is similar to a diagonal matrix $\operatorname{diag}\{r_1, \ldots, r_n\}$, $r_i \in \mathbb{C}$, if and only if the minimum polynomial $m(\lambda)$ has distinct roots.

Proof. ($\implies$) Assume A is similar to diagonal matrix $\operatorname{diag}\{r_1, \ldots, r_n\}$, $r_i \in \mathbb{C}$. Recall two matrics are similar if there exists an invertible matrix $P \in \mathrm{GL}_n(\mathbb{C})$ such that $PAP^{-1} = \operatorname{diag}\{r_1, \ldots, r_n\}$. Notice that this gives

$$\lambda I - PAP^{-1} = P(\lambda I - A)P^{-1} = \operatorname{diag}\{\lambda - r_1, \ldots, \lambda - r_n\}.$$

Taking the determinant gives

$$\det(\lambda I - PAP^{-1}) = \prod_{i=1}^{n}(\lambda - r_i).$$

Notice, that by our equivalence above, we have

$$\det(\lambda I - PAP^{-1}) = \det(P(\lambda I - A)P^{-1}) = \det(P)\det(\lambda I - A)\det(P)^{-1} = \det(\lambda I - A).$$

Thus the characteristic polynomial is of the form

$$f(\lambda) = \prod_{i=1}^{n}(\lambda - r_i).$$

Hence, since the minimal polynomial $m(\lambda) \mid f(\lambda)$, we get that

$$m(\lambda) = \prod_{j=1}^{k} (\lambda - r_{i_j})$$

for some $k \leq n$, and some subset of the r_i. In fact, since the minimal polynomial and the characteristic polynomial share the same linear (prime) factors (**Theorem 3.14**), we must have that $m(\lambda) = f(\lambda)$ by this. Regardless, though, the minimal polynomial has distinct roots.
($\Longleftarrow$) Since the minimum polynomial has all distinct roots, and we're working over $\mathbb{C}$, we see that the invariant factors must be linear of the form $\prod_{j=1}^{k}(\lambda - r_j)$, where r_j are the roots (this follows since all invariant factors divide the minimum polynomial). In other words, the Jordan form will be given by

$$\begin{pmatrix} C_1 & & \\ & \ddots & \\ & & C_n \end{pmatrix},$$

where the C_i are simply r_i (since they all have multiplicity 1). Hence, the Jordan form is

$$\begin{pmatrix} r_1 & & \\ & \ddots & \\ & & r_n \end{pmatrix},$$

and so we have that A is similar to the matrix $\text{diag}\{r_1, \ldots, r_n\}$.

□

Problem 52 (Section 6.1, Exercise 3)**.** Let B be a non-degenerate bilinear form on V. Show that if C is a bilinear form on V, then there exists a unique linear transformation L_C of V into V such that $C(x, y) = B(L_c(x), y)$ for all $x, y \in V$. Show that C is non-degenerate if and only if L_C is bijective. Show that there exists a unique bijective linear transformation P of V into V such that $B(y, x) = B(P(x), y)$ for all $x, y \in V$.

Proof. We have that every linear function on V is of the form $x_L : V \to F$ such that $x_L(y) = B(x, y)$ since B is non-degenerate. Notice that the function $x'_L : V \to F$ is such that $x'_L(y) = C(x, y)$ is a linear function. For some $z \in X$, then, we have $z_L : V \to F$ is such that $z_L(y) = C(x, y) = B(z, y)$. Let $L_C : V \to V$ be the linear function defined by $L_C(x) = z$, where $z_L : V \to F$ is defined to be such that $z_L(y) = B(z, y) = B(L_C(x), y) = C(x, y) = x_L(y)$. Notice this is well-defined by assumption (that is, if $x = y$, then $x_L(g) = y_L(g)$ for all g, and so they map to the same function z_L). We first check that this is indeed a linear function. Let $a, b \in V$. Then we have $L_C(a) = f$, $L_C(b) = g$, and we notice that $f_L(y) + g_L(y) = B(f, y) + B(g, y) = B(f + g, y) = (f + g)_L(y)$, $B(f + g, y) = B(f, y) + B(g, y) = C(a, y) + C(b, y) = C(a + b, y)$, so we have $L_C(a + b) = f + g = L_C(a) + L_C(b)$.

Next, if $a \in V$, $r \in F$, we want to see that $L_C(ra) = rL_C(a)$. Letting $f = L_C(a)$, we have that $rf_L(y) = rB(f, y) = B(rf, y)$, $B(f, y) = C(a, y)$, $rC(a, y) = C(ra, y)$, so we see that $rL_C(a) = rf = L_C(ra)$. Hence, the function is linear.

Next, we wish to check that the function is unique. Let $T : V \to V$ be such that $B(T(x), y) = C(x, y)$. Then we see that $B(T(x), y) = B(L_C(x), y)$ for all $x \in V$, and so $B(T(x), y) - B(L_C(x), y) = 0$ for all $x \in V$. Using linearity in the first component, we see that $B(T(x) - L_C(x), y) = 0$ for all y. This implies that $T(x) - L_C(x) \in V^{\perp L}$, but this is trivial by assumption, so $T(x) - L_C(x) = 0$, or $T(x) = L_C(x)$ for all $x \in V$, and so $T = L_C$. Hence, it is unique.

We now show that C is non-degenerate if and only if L_C is bijective.
($\Longrightarrow$) Since C is non-degenerate, there exists a linear function $L_B : V \to V$ such that $C(L_B(x), y) =$

$B(x,y)$ by the previous part. Hence, we have $C(L_B(L_C(x)),y) = B(L_C(x),y) = C(x,y)$. Since the function is unique, this tells us that $L_B \circ L_C = \mathrm{Id}$. Going the other direction, we have that $B(L_C(L_B(x)),y) = C(L_B(x),y) = B(x,y)$, so $L_C \circ L_B = \mathrm{Id}$ again by uniqueness. This tells us that L_C is bijective, since it admits a left and right inverse.
($\Longleftarrow$) Examine $U = \{x \in V \ : \ C(x,y) = 0 \text{ for all } y \in V\}$. Notice that this is the same as $\{x \in V \ : \ B(L_C(x),y) = 0 \text{ for all } y \in V\}$ by assumption. Since L_C is bijective and B non-degenerate, we have that $U = 0$; if it weren't, we have $0 \neq z \in U$ such that $B(z,y) = 0$ for all $y \in V$ (since $\ker(L_C) = 0$), but this is a contradiction since $V^{\perp L}$ relative to B is trivial. Notice that this implies that $V^{\perp L}$ relative to C is trivial, and by the equivalence in **Theorem 6.1**, we see that C is non-degenerate.

We check that the map $C : (x,y) \mapsto B(y,x)$ gives is a bilinear form. By the first part of the problem, we can deduce a unique linear transformation P exists, and by **Theorem 6.1** we see that $B(y,x)$ will still be non-degenerate, and so we have a unique bijective linear transformation by the second part of the problem.

To see that this still gives us a bilinear form. That is, we need to check it is linear in each component (it's clear that the map is still into F). Notice that for $a,b,c \in V$, $r \in F$ we have

$$\begin{aligned} C(a+b,c) = B(c,a+b) = B(c,a) + B(c,b) = C(a,c) + C(a,b), \\ C(ra,b) = B(b,ra) = rB(b,a) = rC(a,b), \\ C(a,b+c) = B(b+c,a) = B(b,a) + B(c,a) = C(a,b) + C(a,c), \\ C(a,rb) = B(rb,a) = rB(b,a) = rC(a,b). \end{aligned}$$

So this is indeed a bilinear form. □

Problem 53 (Section 6.1, Exercise 8)**.** Let B be a bilinear form. Note that if u and v are fixed vectors, then the map $x \mapsto B(x,u)v$ is a linear transformation of V into V. Denote this as $u \otimes v$. Find a formula for the trace $\mathrm{tr}(u \otimes v)$. Show that if B is non-degenerate then every linear transformation has the form $\sum u_i \otimes v_i$.

Proof. Fix a basis $\{e_1, \ldots, e_n\}$ for V. Let $T : V \to V$ be the linear transformation given by $T(x) = B(x,u)v$, where B the bilinear form. We have that u and v are fixed vectors, and so we can write them as

$$\begin{aligned} u = \sum_{i=1}^{n} a_i e_i, \\ v = \sum_{i=1}^{n} b_i e_i. \end{aligned}$$

Furthermore, we see that we have values $d_{ij} = B(e_i, e_j)$. Notice that we can write

$$B(x,u)v = B\left(x, \sum_{i=1}^{n} a_i e_i\right) v = \left(\sum_{i=1}^{n} a_i B(x,e_i)\right) v = \sum_{i=1}^{n} a_i B(x,e_i) v$$

We can then form a matrix A from seeing where we map the basis elements to; we have that

$$\begin{aligned} T(e_1) = \sum_{i=1}^{n} a_i B(e_1,e_i)v = \sum_{i=1}^{n} a_i d_{1i} v, \\ T(e_2) = \sum_{i=1}^{n} a_i B(e_2,e_i)v = \sum_{i=1}^{n} a_i d_{2i} v, \\ \cdots \end{aligned}$$

to get the matrix

$$A = \begin{pmatrix} \sum_{i=1}^n a_i d_{1i} b_1 & \sum_{i=1}^n a_i d_{2i} b_1 & \cdots & \sum_{i=1}^n a_i d_{ni} b_1 \\ \vdots & \vdots & \vdots & \vdots \\ \sum_{i=1}^n a_i d_{1i} b_n & \sum_{i=1}^n a_i d_{2i} b_n & \cdots & \sum_{i=1}^n a_i d_{ni} b_n \end{pmatrix}.$$

Thus, the trace is given by

$$\operatorname{tr}(u \otimes v) = \sum_{i,j=1}^n a_i d_{ji} b_j,$$

relative to the chosen basis. Notice that this corresponds to, after fixing a basis, $v^T B u$, where B is the matrix with coefficients given by $B(e_i, e_j)$.

Remark. This actually aligns with the answer given in class using a basis free method. That is, the trace is $B(v, u)$.

If B is non-degenerate, then every linear transformation on V to F is of the form $x_R : V \to F$ where $x_R(y) = B(x, y)$. Take a given function $T : V \to V$. Fix a basis $\{e_1, \ldots, e_n\}$. Writing a vector $x \in V$ as $x = \sum_{i=1}^n a_i e_i$, we have that projecting onto the ith coordinate gives us a function $T_i : V \to F$ via $T_i(x) = a_i$. Hence, we can write $T : V \to V$ as $T(x) = \sum T_i(x) e_i = (T_1(x), \ldots, T_n(x))$. Since each $T_i : V \to F$ is a linear function (since T is linear in each component), we have that there is a $u_i \in V$ so that $(u_i)_R(x) = B(x, u_i) = T_i(x)$. To get a vector, then, we sum these over the basis e_i; that is, we have $T(x) = \sum_{i=1}^n T_i(x) e_i = \sum_{i=1}^n B(x, u_i) e_i$. By definition, this tells us that $T(x) = \sum_{i=1}^n (u_i \otimes e_i)(x)$. Since this applies for all x, we get $T = \sum (u_i \otimes e_i)$, as desired. Hence, every linear transformation is a sum of these tensors. □

Problem 54 (Section 6.2, Exercise 2)**.** Assume B is an alternate bilinear form and $(u_1, v_1, \ldots, u_k, v_k)$ satisfy $B(u_i, v_i) = 1 = -B(v_i, u_i)$ with all other $B(x, y) = 0$ for $x, y \in (u_1, v_1, \ldots, u_k, v_k)$. Using the notation prior, let

$$E_k = \sum_1^k (u_i \otimes v_i - v_i \otimes u_i).$$

Verify that $E_k^2 = E_k$ and

$$B(E_k x, y) = B(x, E_k y)$$

for all $x, y \in V$.

Proof. Notice that $u_i \otimes v_i = (x \mapsto B(x, u_i)v_i)$ is a map $V \to V$. Hence, we see that $E_k : V \to V$ as well. Since B is alternate, we can find a basis for V of the form $(u_1, v_1, \ldots, u_k, v_k, u_{k+1}, v_{k+1}, \ldots, u_r, v_r, z_1, \ldots, z_{n-2r})$, where n is the dimension of V by **Theorem 6.3**. Then the matrix of B is of the form $\operatorname{diag}(S, \ldots, S, 0, \ldots, 0)$ (here, there are r S's) where

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We then would like to find a matrix form for $u_i \otimes v_i$ relative to this basis. Notice that

$$u_i \otimes v_i(u_j) = B(u_j, u_i)v_i = 0,$$
$$u_i \otimes v_i(v_j) = B(v_j, u_i)v_i = -\delta_{ji}v_i,$$
$$u_i \otimes v_i(z_j) = B(z_j, u_i)v_i = 0.$$

Hence, the corresponding matrix is the matrix with all 0's and a -1 at the $(i+1, i+1)$ location; that is, it is $-e_{(i+1)(i+1)}$. Likewise, we see that, relative to this basis,

$$v_i \otimes u_i(u_j) = B(u_j, v_i)u_i = \delta_{ij}u_i,$$
$$v_i \otimes u_i(v_j) = 0,$$
$$v_i \otimes u_i(z_j) = 0.$$

In other words, this corresponds to the matrix e_{ii}. So we have

$$u_1 \otimes v_1 - v_1 \otimes u_1$$

corresponds to the matrix

$$\begin{pmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

and so on. So the matrix of E_k relative to this basis corresponds to $\operatorname{diag}(J, \ldots, J, 0, \ldots, 0)$, where the J occur k times and are of the form

$$J = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

I believe the book is wrong at this point, or I'm misunderstanding something. We see that E_k corresponds to this matrix with the respective basis, and so we have $E_k^2 \neq E_k$, since one will have 1's along the diagonal and the other has -1 along the diagonal. Checking with others, we seem to have independently all reached the same conclusion.

Let $x, y \in V$. Then we have that

$$x = \sum_{i=1}^{r} a_i u_i + \sum_{j=1}^{r} b_j v_j + \sum_{t=1}^{2n-r} c_t z_t,$$

$$y = \sum_{i=1}^{r} a_i' u_i + \sum_{j=1}^{r} b_j' v_j + \sum_{t=1}^{2n-r} c_t' z_t.$$

Hence,

$$E_k(x) = \sum_{i=1}^{r} a_i E(u_i) + \sum_{j=1}^{r} b_j E(v_j) = \sum_{i=1}^{k} (-a_i) u_i - \sum_{j=1}^{k} (b_j) v_j,$$

$$B(E_k(x), y) = B\left(\sum_{i=1}^{k} (-a_i) u_i - \sum_{j=1}^{k} b_j v_j, y \right)$$

$$= -a_i \sum_{i=1}^{k} B(u_i, y) - \sum_{j=1}^{k} b_j B(v_j, y),$$

and substituting y in we get

$$= -\sum_{i=1}^{k} a_i \left(\sum_{f=1}^{r} a_f' B(u_i, u_f) + \sum_{g=1}^{r} b_g' B(u_i, v_g) + \sum_{h=1}^{2n-r} c_h' B(u_i, z_h) \right)$$

$$-\sum_{j=1}^{k} b_j \left(\sum_{f=1}^{r} a_f' B(v_j, u_f) + \sum_{g=1}^{r} b_g' B(v_j, v_g) + \sum_{h=1}^{2n-r} c_h' B(v_j, z_h) \right)$$

$$= -\sum_{i=1}^{k} a_i b_i' + \sum_{j=1}^{k} b_j a_j'.$$

A similar argument gives

$$E_k(y) = \sum_{i=1}^{k} (-a_i') u_i - \sum_{j=1}^{k} (b_j') v_j,$$

$$B(x, E_k(y)) = B\left(x, \sum_{i=1}^{k} (-a_i') u_i - \sum_{j=1}^{k} (b_j') v_j \right)$$

$$= \sum_{i=1}^{k} (-a_i') B(x, u_i) - \sum_{j=1}^{k} (b_j') B(x, v_j),$$

and substituting in x gives

$$= \sum_{i=1}^{k} (-a_i') \left(\sum_{f=1}^{r} a_f B(u_f, u_i) + \sum_{g=1}^{r} b_g B(v_g, u_i) + \sum_{h=1}^{2n-r} c_h B(z_h, u_i) \right)$$

$$-\sum_{i=1}^{k} (b_i') \left(\sum_{f=1}^{r} a_f B(u_f, v_i) + \sum_{g=1}^{r} b_g B(v_g, v_i) + \sum_{h=1}^{2n-r} c_h B(z_h, v_i) \right)$$

$$= \sum_{i=1}^{k} a_i' b_i - \sum_{i=1}^{k} b_i' a_i,$$

and so we get that $B(E_k(x), y) = B(x, E_k(y))$, as desired. □

Problem 55 (Section 6.2, Exercise 3)**.** Let B be a non-degenerate alternate bilinear form on V, T a linear transformation of V into V. Define the adjoint of T relative to B as the (unique) linear transformation T' such that $B(Tx, y) = B(x, T'y)$ for all $x, y \in V$. Determine the adjoint of $u \otimes v$ relative to B.

Proof. We have $u \otimes v = (x \mapsto B(x, u)v)$. We see then that

$$B((u \otimes v)(x), y) = B(B(x, u)v, y) = B(x, u)B(v, y).$$

We then want to find T' so that

$$B(x, T'y) = B(x, u)B(v, y).$$

If we define $T' = (x \mapsto B(v, x)u)$, we get

$$B(x, T'y) = B(x, B(v, y)u) = B(v, y)B(x, u) = B(x, u)B(v, y).$$

Hence, this is the adjoint. It's unique by the prior problem set. □

Problem 56 (Section 6.2, Exercise 7)**.** Let $s = \mathrm{diag}(S, \ldots, S)$, where

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Call a matrix $a \in M_n(R)$, R a commutative ring, *symplectic symmetric* if $s^{-1}a^t s = a$. Show that this condition is equivalent to the condition that sa is skew.

Show that a is a root of the equation, $\mathrm{Pf}(s\lambda - sa) = 0$.

Proof. ($\implies$) Recall that sa is skew if $(sa)^t = -(sa)$. Assume that $a \in M_n(R)$ is symplectic symmetric. Then we have that $s^{-1}a^t s = a$. Notice that

$$sa + (sa)^t = sa + a^t s^t = sa - a^t s,$$

since $s^t = -s$, and we have that the symplectic symmetric property gives us that $a^t s = sa$, so

$$sa + (sa)^t = sa - a^t s = sa - sa = 0.$$

In other words,

$$(sa)^t = -sa,$$

and so the matrix is skew.
($\impliedby$) Assume the matrix is skew. Then we have

$$-a^t s = a^t s^t = (sa)^t = -sa,$$

or

$$a^t s = sa.$$

Since s is invertible (in fact, $s^4 = 1$), we have that

$$s^{-1}a^t s = a.$$

So the matrix is symplectic symmetric.

Remark. The next portion originally had a very wrong proof. I found this proof in Structure and Representations of Jordan Algebras by Jacobson.

Next, we wish to show that $\mathrm{Pf}(s\lambda - sa) = 0$ has a root at a (assuming a is symplectic symmetric). To do this, we need to do the prior problems. Let $X = (x_{ij})$ a $2n \times 2n$ matrix in $\mathbb{Z}[x_{ij}]$ which is skew symmetric; that is, we have $x_{ii} = 0$ and $x_{ij} = -x_{ji}$. First, notice that $X\mathrm{Adj}(X) = \det(X)I$. This then gives us

$$\sum_{k=1}^{2n} a_{ik}X_{kj} = \delta_{ij}\det(X),$$

where here X_{ij} represents the cofactor. We notice that $X_{ii} = 0$, $X_{ij} = -X_{ji}$. Using this, we get an equation for $2n-1$ elements X_{kj}, $k \neq j$. Taking the determinant of the coefficients of these linear equations gives the $(-1)^{i+j}$ cofactor of x_{ij}. That is, we get

$$x_{ij} = (-1)^{i+j}X_{ji} = (-1)^{i+j+1}X_{ij}.$$

Using Cramer's rule, we get

$$(-1)^{i+j+1}X_{ij}^2 = (\det(X))\Delta_{ij},$$

for some $\Delta_{ij} \in \mathbb{Z}[x_{ij}]$. Now, we have that $\det(X) = \mathrm{Pf}(X)^2$, so replacing this gives

$$(-1)^{i+j+1}X_{ij}^2 = (\det(X))\mathrm{Pf}(X)^2,$$

So for all i, j, we get

$$\mathrm{Pf}(X) \mid X_{ij},$$

since $X_{ii} = 0$. Using this, we have that

$$\mathrm{Pf}(X)Y_{ij} = X_{ij}$$

for some $Y_{ij} \in \mathbb{Z}[x_{ij}]$, so writing $Y = (Y_{ij})$, we get

$$X\mathrm{Adj}(X) = XY\mathrm{Pf}(X) = (\mathrm{Pf}(X))^2 1.$$

This then gives us

$$XY = \mathrm{Pf}(X)1.$$

Using this, write

$$X = s\lambda - sa,$$

then we have

$$(s\lambda - sa)Y = \mathrm{Pf}(s\lambda - sa)1.$$

We now follow the proof of Cayley-Hamilton, which gives us the desired result. Write $p(\lambda) = \mathrm{Pf}(s\lambda - sa)$. Then we have

$$(s\lambda - sa)Y = p(\lambda)1.$$

For simplicity, let $m = 2n$. Y is a matrix of polynomials with respect to λ as well, so we can write

$$Y = \sum_{i=0}^{m-1} \lambda^i Y_i,$$

where Y_i is the matrix of coefficients of λ^i in Y. So using this, we get

$$(s\lambda - sa)\sum_{i=0}^{m-1} \lambda^i Y_i$$

$$= s\left(\sum_{i=1}^{m} \lambda^i Y_{i-1} - \sum_{i=0}^{m-1} \lambda^i a Y_i\right).$$

Expanding then gives

$$s\left(\lambda^m Y_{m-1} + \sum_{i=0}^{m-1} \lambda^i \left(Y_{i-1} - aY_i\right) - aY_0\right).$$

Write

$$p(\lambda)1 = \sum_{i=0}^{m} \lambda^i c_i I_n,$$

where c_i are constant matrices. By the equality, we get

$$c_0 = -aY_0,\ Y_{i-1} - aY_i = c_i,\ c_m = Y_{m-1} = 1,$$

noting here that $p(\lambda)$ is monic. Multiplying the coefficients of λ^i by a^i, we have

$$a^m Y_{m-1} + \sum_{i=1}^{m-1} (a^i Y_{i-1} - a^{i+1} Y_i) - aY_0 = \sum_{i=0}^{m} a^i c_i = p(a)$$

We notice that the left hand side dies completely, so we get $p(a) = 0$. In other words, a is a root of the Pfaffian. □

Problem 57 (Section 6.3, Exercise 3)**.** Show that a symmetric bilinear form B in V over $\mathbb{R}$ is *positive definite* in the sense that $B(u, u) > 0$ for all $u \neq 0$ if and only if it has 1 as one of its matrices. Use the Lagrange reduction (in this case called the Schmidt orthogonalization process) to prove that if s is a matrix of a positive definite symmetric bilinear form, then there exists a triangular matrix p with 0's above the main diagonal such that

$$psp^t = 1$$

or

$$s = qq^t,$$
$$q = p^{-1}.$$

Proof. We first show that a symmetric bilinear form B in V over $\mathbb{R}$ is positive definite if and only if it has 1 as one if its matrices.
($\Longrightarrow$) Assume B is positive definite. Then we get that it's corresponding matrix $\overline{B}$ is symmetric and has only positive values; hence, we have that it is diagonalizable. Since we require that it be positive definite, we must have that its signature is $p = n$, where p here denotes the number of 1's along the diagonal, by **Theorem 6.8**. In other words, it has 1 has one of its matrices.
($\Longleftarrow$) Assume that it has 1 as one of its matrices. Then we have a basis $(v_1, \ldots, v_n)$ for V such that $B(v_i, v_j) = \delta_{ij}$. Taking $x \in V$, we have

$$x = \sum a_i v_i,$$

where $a_i \in F$, and so we get

$$B(x, x) = B\left(\sum a_i v_i, \sum a_i v_i\right) = \sum_{i=1}^{n} B\left(v_i, \sum_{j=1}^{n} a_j v_j\right) = \sum_{i,j=1}^{n} a_i a_j B(v_i, v_j) = \sum_{i=1}^{n} a_i^2.$$

So as long as $x \neq 0$, we have that $a_i \neq 0$ for at least one i, and so $B(x, x) > 0$.

Write $B = (B(e_i, e_j))$ where e_i is the current basis of V. We then do a change of basis using the Schmidt orthogonalization procedure; let $v_1 = e_1$, $u_1 = e_1/\sqrt{B(e_1, e_1)}$, and given the basis up to k, say $(u_1, \ldots, u_k)$, we find u_{k+1} by

$$v_{k+1} = e_{k+1} - \sum_{i=1}^{k} \frac{B(e_{k+1}, e_i)}{B(e_i, e_i)} e_i,$$

$$u_{k+1} = \frac{v_{k+1}}{\sqrt{B(v_{k+1}, v_{k+1})}}$$

Then we have a collection of vectors $(u_1, \ldots, u_n)$, and we check that this is a basis. It suffices to show that its linearly independent. That is, if we have

$$\sum a_i u_i = 0,$$

then this forces $a_i = 0$. But writing this out, we have

$$\sum_{i=1}^{n} a_i u_i = \sum_{i=1}^{n} \frac{a_i}{\sqrt{B(v_i, v_i)}} v_i,$$

so it suffices to check that the v_i are also a basis. Hence, we check

$$\sum_{i=1}^{n} a_i v_i = a_1 e_1 + \sum_{i=2}^{n} a_i \left(e_i - \sum_{j=1}^{i-1} \frac{B(e_i, e_j)}{B(e_j, e_j)} e_j \right).$$

Expanding this out gives

$$\sum_{i=1}^{n} d_i e_i = 0,$$

which forces the $d_i = 0$, where here we have that

$$d_1 = a_1 - \sum_{j=2}^{n} a_j \frac{B(e_j, e_1)}{B(e_1, e_1)},$$

$$d_2 = a_2 - \sum_{j=3}^{n} a_j \frac{B(e_j, e_2)}{B(e_2, e_2)},$$

$$\cdots$$

$$d_{n-1} = a_{n-1} - a_n \frac{B(e_n, e_{n-1})}{B(e_{n-1}, e_{n-1})},$$

$$d_n = a_n.$$

We see that the basis criteria forces $a_n = 0$. This then forces $a_{n-1} = 0$, $a_{n-2} = 0$, etc. Hence, we have that the v_i are linearly independent, and since $\mathrm{Dim}(V) = n$, this forces them to be a basis, and furthermore this then forces the u_i to also be a basis. Under this basis, we see that

$$B(u_1, u_1) = 1,$$

$$B(u_1, u_i) = 0 \text{ for all } i \neq 1,$$

and furthermore by calculation we get

$$B(u_i, u_j) = \delta_{ij}.$$

Hence, the corresponding matrix will be 1.

Notice that to get the matrix $(B(u_i, u_j))$, we have to multiply the matrix $s = B(e_i, e_j)$ by

$$p = \begin{pmatrix} u_1 & u_2 & \cdots & u_n \end{pmatrix}$$

and (p^t) to get

$$p^t s p = (B(u_i, u_j)) = 1.$$

Notice that p here is an upper triangular matrix by this orthonormalization process, so by taking the transpose we get a lower triangular matrix. Letting p be the lower triangular matrix without loss of generality, we get

$$p s p^t = 1.$$

Notice that along the diagonal of p, we have non-zero values (by construction), and so it is invertible. Letting $q = p^{-1}$, we see that

$$q p s p^t q^t = s = q q^t$$

as well. □

Problem 58 (Section 6.3, Exercise 4)**.** Assume we have the same hypothesis as in the prior problem. Call a base $(u_1, \ldots, u_n)$ *Cartesian* if $B(u_i, u_j) = \delta_{ij}$. Show that if $(v_1, \ldots, v_n)$ is a second such base, then the matrix relating the two is orthogonal. Use the result of the prior exercise to show that if m is any invertible matrix in $M_n(\mathbb{R})$, m can be written in the form po, where p is triangular and o is orthogonal (RQ, LQ factorization).

Proof. Recall that being orthogonal means that $oo^t = 1$. Let o be the matrix relating these bases; that is, letting $s = (B(u_i, u_j))$, $v = (B(v_i, v_j))$, we have

$$oso^t = v.$$

However, $s = (B(u_i, u_j)) = (\delta_{ij}) = 1$, and likewise $v = (B(v_i, v_j)) = (\delta_{ij}) = 1$, so

$$oso^t = oo^t = 1.$$

Thus, the matrix is orthogonal.

Let m be an invertible matrix. Let B the bilinear form with associated matrix $s = m^t m$. We see that this has 1 as one of its matrices, since

$$(m^t)^{-1} s (m^{-1}) = 1,$$

so B is a positive definite bilinear form. Hence, we can find a lower triangular matrix p by the last problem with

$$p(m^{-1})^t s (m^{-1}) p^t = p m^{-1} s (p m^{-1})^t = 1.$$

Since this is relating to basis which both give the 1 matrix, by the first part of this problem we have that $p(m^{-1})^t$ is an orthogonal matrix; in other words, we have

$$p(m^t)^{-1} = o.$$

Multiplying (m^t) to the right of both sides and o^t to the left of both sides gives

$$o^t p = m^t.$$

Taking the transpose of both sides gives

$$p^t o = m.$$

Since p was chosen to be lower triangular, we have that the transpose is still a triangular matrix, say q, so we get that

$$qo = m,$$

where q is a triangular matrix, o orthogonal.

□

Problem 59 (Section 6.2, Exercise 4)**.** Show that $\mathrm{Pf}(a)$ is linear in any one of the rows of the alternate matrix a (for fixed values of entries in the submatrix obtained by deleting the chosen row and corresponding column).

Proof. Now, examine the matrix

$$a = \begin{pmatrix} 0 & x_{12} & \cdots & x_{1m} \\ -x_{12} & 0 & \cdots & x_{2m} \\ -x_{13} & -x_{23} & \ddots & x_{3m} \\ \vdots & \vdots & \ddots & \vdots \\ -x_{1m} & -x_{2m} & \cdots & 0 \end{pmatrix}.$$

We want to show that this is linear with regards to a row. Multiply the ith row of a by λ. Since it's alternating, this corresponds to

$$D_i(\lambda) a D_i(\lambda),$$

so we have

$$\mathrm{Pf}(D_i(\lambda) a D_i(\lambda)) = \det(D_i(\lambda))\mathrm{Pf}(a) = \lambda \mathrm{Pf}(a).$$

Using the swapping row and linearity properties, we can use the trick to show that determinants are linear in rows to get that the Pfaffian is linear in rows. □

Problem 60 (Section 6.3, Exercise 5)**.** Prove that the set of polynomial functions on V can be defined as the subring of the ring of maps from V to F generated by the linear functions. Here, addition and multiplication of maps from V to F are the usual ones:

$$(f+g)(x) = f(x) + g(x) \quad \text{(pointwise)}$$

$$(fg)(x) = f(x)g(x) \quad \text{(pointwise)}.$$

This gives an intrinsic definition of polynomial functions.

Proof. Let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$, where n is the dimension of V. We wish to show that f is a linear combination of linear functions. We write

$$f(a_1, \ldots, a_n) = \sum_{(i_1, \ldots, i_r)} b_{i_1} \cdots b_{i_r} a_{i_1}^{p_{i_1}} \cdots a_{i_r}^{p_{i_r}},$$

where $1 \leq r \leq n$, $i_j \in \{1, \ldots, n\}$. It's clear that it's a linear combination of linear functionals via projections. Likewise, any linear combination of these linear functionals is some linear combination of the projections, so we get that it's a polynomial. □

Problem 61 (Section 6.3, Exercise 6)**.** Let Q be a non-degenerate quadratic form on an $n \geq 3$ dimensional vector space over a finite field. Show that Q is isotropic (where isotropic means that there exists a vector $u \neq 0$ such that $B(u, u) = 0$.)

Proof. Associated to Q is the bilinear form

$$B(x, y) = Q(x + y) - Q(x) - Q(y).$$

Assume for contradiction that there is no vector u such that $B(u, u) = 0$. Then we have that

$$B(u, u) = 2Q(u) \neq 0$$

for all $u \neq 0$. Associated to this bilinear form (since it's non-degenerate) is a matrix of the form

$$b := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d \end{pmatrix}$$

Since $n \geq 3$, we have at least 2 1s. We also have that B is universal. Write $v = (x_1, \ldots, x_n)$, then with regards to this base we have

$$\begin{aligned} B(v, v) &= (x_1, \ldots, x_n) b (x_1, \ldots, x_n)^t \\ &= (x_1, \ldots, x_n) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ dx_n \end{pmatrix} = x_1^2 + \cdots + dx_n^2. \end{aligned}$$

The Chevalley-Warning Theorem applies then to find us a non-zero solution. □

Problem 62. Recall that an *isometry* of V onto V relative to the quadratic forms Q_1, Q_2 (equivalently, bilinear forms B_1, B_2) is a bijective linear map $\eta : V \to V$ such that $Q_2(\eta(x)) = Q_1(x)$ for all $x \in V$ (equivalently, $B_2(\eta(x), \eta(y)) = B_1(x, y)$ for all $x, y \in V$).

Recall that an *orthogonal transformation* of V onto V relative to a non-degenerate quadratic form Q is an isometry which has the same quadratic form in the domain and codomain. In other words, we have that $Q(\eta(x)) = Q(x)$ for all $x \in V$.

Prove that a linear transformation $\eta : V \to V$ is orthogonal if and only if for all $1 \leq i, j \leq n$,

$$B(\eta(e_i), \eta(e_j)) = B(e_i, e_j),$$

where here B is the associated bilinear form to Q. Recall that the associated bilinear form is of the form

$$B(x, y) = Q(x + y) - Q(x) - Q(y)$$

Proof. Let $\eta : V \to V$ be a linear transformation.
($\implies$) Assume η is orthogonal, $(e_1, \ldots, e_n)$ a base for V, Q a quadratic form, B the associated bilinear form (that is, $B(x, y) = Q(x + y) - Q(x) - Q(y)$). We have that

$$\begin{aligned} B(\eta(e_i), \eta(e_j)) &= Q(\eta(e_i) + \eta(e_j)) - Q(\eta(e_i)) - Q(\eta(e_j)) = Q(\eta(e_i + e_j)) - Q(\eta(e_i)) - Q(\eta(e_j)) \\ &= Q(e_i + e_j) - Q(e_i) - Q(e_j) = B(e_i, e_j). \end{aligned}$$

($\impliedby$) We need to show that for all $x \in V$, $Q(\eta(x)) = Q(x)$. We have

$$\begin{aligned} 2Q(\eta(x)) = B(\eta(x), \eta(x)) &= B\left(\eta\left(\sum a_i e_i\right), \eta\left(\sum a_j e_j\right)\right) \\ &= \sum a_i a_j B(\eta(e_i), \eta(e_j)) = \sum a_i a_j B(e_i, e_j) \\ &= B\left(\sum a_i e_i, \sum a_j e_j\right) = B(x, x) = 2Q(x). \end{aligned}$$

Hence, $Q(\eta(x)) = Q(x)$. □

From here onwards, unless otherwise stated, let V be a vector space and Q a non-degnerate quadratic form on V.

Problem 63 (Section 6.4, Exercise 1)**.** Show that if η is an orthogonal transformation and

$$V_1 = \{x \ : \ \eta(x) = x\},$$

then $\dim(V) = \dim(V_1) + \dim((1-\eta)V)$. Show also that $V_1 = ((1-\eta)V)^\perp$ and hence $V_1^\perp = (1-\eta)V$.

Problem 64. Recall that a *symmetry* is a map of the form

$$S_u(x) = x - \frac{B(x,u)}{Q(u)}u)$$

(1) Prove that S_u is linear.
(2) Prove that S_u is orthogonal.
(3) Recall that a transformation is called *improper* if the determinant relative to some base is -1 (it turns out this is equivalent to saying the determinant relative to *all* bases is -1). Show that S_u is improper. (Hint: $Fu^\perp$)
(4) Show that $S_u^2 = 1$.

Problem 65. Let B be a non-degenerate biliner form on a vector space V. Recall that the adjoint of a linear map T relative to B is a linear map T' so that

$$B(Tx, y) = B(x, T'y).$$

Prove that the adjoint of an orthogonal transformation is its inverse.

Problem 66 (Section 6.4, Exercise 2)**.** Let η be an orthogonal transformation such that $\dim(V_1) \geq \dim(V) - 1$, where V_1 is as in the prior exercise. Show that either $\eta = 1$ or η is a symmetry.

Problem 67 (Section 6.4, Exercise 3)**.** Recall that a a pair of vectors (u, v) is called a *hyperbolic pair* relative to a quadratic form Q if

$$B(u,u) = 0 = B(v,v), \quad B(u,v) = 1 = -B(v,u),$$

where B is the associated bilinear form to Q.

Let (u, v) be a hyperbolic pair and let $w \in (Fu+Fv)^\perp$ be non-isotropic (that is, either $Q(w) \neq 0$ or $w = 0$). Verify that the linear transformation ρ defined by

$$u \mapsto u$$

$$v \mapsto v - Q(w)u - w,$$

$$x \mapsto x + B(x,w)u, \quad x \in (Fu + Fv)^\perp$$

coincides with $S_w S_{w-Q(w)u)}$. (Note that $Q(w - Q(w)u) \neq 0$.)

Problem 68. Read/prove Witt's Cancellation theorem:
Let Q be a non-degenerate quadratic form on a vector space V over a field F of characteristic $\neq 2$, U_1, U_2 non-degenerate subspaces which are isometric. Then $U_1^\perp$ and $U_2^\perp$ are isometric.

Problem 69. Read/prove Witt's Extension theorem:
If V is equipped with a non-degenerate quadratic form Q, any isometry of a subspace U_1 onto a subspace U_2 can be extended to an orthogonal transformation.

Problem 70. Read/prove Cartan-Dieudonné theorem:
If $\dim(V) = n$, then any orthogonal transformation of V is a product of $\leq n$ symmetries.
Read/prove also the "cheap version:"
Any orthogonal transformation is a product of symmetries.

Problem 71 (Section 6.9, Exercise 1)**.** Recall that a symplectic base for V relative to a non-degnerate alternate bilinear form B is a base $(u_1, v_1, \ldots, u_r, v_r)$ which satisfies the following conditions:

$$B(u_i, u_j) = 0 = B(v_i, v_j), \quad B(u_i, v_j) = \delta_{ij} = -B(v_j, u_i).$$

Let (u_i, v_i) be a symplectic base for V, and let U and U' be the subspaces spanned by the u_i and v_i respectively. Let K be the subset of $\mathrm{Sp}_n(F)$ of η which stabilize U and U'. Show that a linear transformation $\eta \in K$ if and only if its matrix relative to the base

$$(u_1, \ldots, u_r, v_1, \ldots, v_r)$$

has the form

$$\begin{pmatrix} A & 0 \\ 0 & (A^t)^{-1} \end{pmatrix}, \ A \in \mathrm{GL}_r(F).$$

Note that K is actually a subgroup of $\mathrm{Sp}_n(F)$.

Problem 72 (Section 6.7, Exercise 4)**.** A linear transformation T is called a *transvection* if there exists a hyperplane U such that $T|U = 1_U$, and for every x, we have $T(x) - x \in U$. Show that the linear transformations corresponding the matrices $T_{ij}(b)$, $i \neq j$, $b \in F$ are transvections. Show that any transvection τ has the form $x \mapsto x + f(x)u$, where $f(x)$ is a linear function and u is a vector such that $f(u) = 0$. Hence, show that there exists a base $(e_1, \ldots, e_n)$for V such that the matrix of τ is $T_{12}(1)$.

Problem 73 (Section 6.9, Exercise 2)**.** Let the notation be as in Exercise 1 of this section. Let L be the subgroup of $\mathrm{Sp}_n(F)$ of σ's which fix every $v \in U'$. Show that a linear transformation $\sigma \in L$ if and only if the matrix relative to $(u_1, \ldots, u_r, v_1, \ldots, v_r)$ has the form

$$\begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix},$$

where $S^t = S$. Show that the map $\sigma \mapsto S$ is a monomorphism of L into the additive group of $r \times r$ symmetric matrices. Show that if $S = e_{ii}$, $1 \leq i \leq r$, then the corresponding σ is a *transvection* (see above).

Problem 74 (Section 6.9, Exercise 3)**.** Let $\sigma \in L$ and $\eta \in K$ (as in Exercises 1 and 2 in this section). Verify that $\eta\sigma\eta^{-1} \in L$. Verify that if the matrices of η and σ are

$$\begin{pmatrix} A & 0 \\ 0 & (A^t)^{-1} \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix}$$

respectively, then the matrix of the commutator $\eta\sigma\eta^{-1}\sigma^{-1}$ is

$$\begin{pmatrix} 1 & S_1 \\ 0 & 1 \end{pmatrix}$$

where

$$S_1 = ASA^t - S.$$

Problem 75 (Section 1.2, Exercise 9)**.** Let G be a non-vacuous subset of a monoid M. Show that G is a subgroup if and only if every $g \in G$ is invertible in M and $g_1 g_2^{-1} \in G$ for any $g_1, g_2 \in G$.

Proof. ($\implies$) Let G be a subgroup of M. Then we have that every $g \in G$ is invertible, and G is closed under multiplication, so $g_1 g_2^{-1} \in G$ for all $g_1, g_2 \in G$.
($\impliedby$) Let G be a subset satisfying these conditions. We need to show that $1 \in G$, G is closed under multiplication, and G is closed under inverses. To see that $1 \in G$, we take $g \in G$ and notice that $gg^{-1} = 1 \in G$. To get that it is closed under multiplication, let $g_1, g_2 \in G$. Since G is closed under inverses, we get that $g_2^{-1} \in G$. Hence, we have $g_1(g_2^{-1})^{-1} = g_1 g_2 \in G$. Finally, it's closed under inverses by assumption. Thus, we have that G is a subgroup. □

Problem 76 (Section 1.2, Exercise 10)**.** Let G be a semigroup having the following properties:

(a) G contains a right unit 1_r, that is, an element satisfying $a1_r = a$, $a \in G$,
(b) every element $a \in G$ has a right inverse relative to 1_r; that is, every $a \in G$ has an associated $b \in G$ such that $ab = 1_r$.

Show that G is a group.

Proof. We need to show that three conditions:

(1) (Closure) This follows since G is a semigroup.
(2) (Associativity) This follows since G is a semigroup.
(3) (Identity) We need to show that there is a 1_l and $1_r = 1_l$. First, notice that
$$1_r = 1_r \cdot 1_r.$$
Notice as well that for every $a \in G$, we have a $b \in G$ such that $ab = 1_r$. So
$$1_r = 1_r \cdot ab = ab \cdot 1_r = ab.$$
Multiplying throughout by the right inverse of b, denoted c, we get
$$1_r \cdot c = abc = c.$$
Furthermore, we notice that
$$abc = c = a.$$
So we have for all $a \in G$ that
$$1_r \cdot a = (ab)a = a(ba) = a(bc) = a.$$
So 1_r is a left inverse, as desired. Thus, we can denote it by 1.
(4) (Inverses) From (3), we see that a is a right inverse for b. In other words, b is both a left and right inverse for a.

Thus, since it satisfies all of the axioms, we have that G is a group. □

Problem 77 (Section 1.2, Exercise 11)**.** Show that in a group, the equations $ax = b$ and $ya = b$ are solvable for $b \in G$. Conversely, show that any semigroup having this property contains a unit and is a group.

Proof. We start with the forward direction. Notice that we can solve for x in the equation $ax = b$ by multiplying by a^{-1} on the left; that is, we have $x = a^{-1}b$. Likewise, we can solve for y by multiplying on the right by a^{-1}; that is, we get $y = ba^{-1}$.

Now, assume we have a semigroup satisfying that these equations are solvable. Denote this set by S. We again have closure and associativity immediately, and so it suffices to show that we have an identity and inverses. We proceed first by showing that S has a unit. Fix $a \in S$. We have

solving $ax = a$ gives us a right identity for a. We need to then establish that for any other $b \in S$, $bx = b$. Notice that $ab = (ax)b = a(xb) = ab$, and so we get $xb = b$. So x is a left inverse for any element $b \in B$, which gives us that it is also a left identity for a. To get that it is a right identity, notice that $cb = c(xb) = (cx)b$, so we have $cx = c$ and so x is a right identity as well. We can denote it by 1.

To get inverses, we solve $ax = 1$, $ya = 1$. Then we see that $x = (ya)x = y(ax) = y$. So every element also admits an inverse. Hence, it's a group. □

Problem 78 (Section 1.2, Exercise 14)**.** Show that a group G cannot be the union of two proper subgroups.

Proof. Let $G = H \cup K$, $H, K \leq G$. If either $H, K = G$, we are done. Assume $H, K \neq G$. Let $x \in (H - K)$, $y \in (K - H)$; we have $(H - K), (K - H) \neq \varnothing$ since $H \cup K = G$ but $H, K \neq G$. Then we have $xy \in G$, since it is closed under products, and by assumption we must have $xy \in H$ or $xy \in K$. But if $xy \in H$, then there is a $h \in H$ so that

$$xy = h \leftrightarrow y = x^{-1}h,$$

and since $x, h \in H$, this implies $y \in H$, a contradiction. Similarly, if $xy \in K$, we have a $k \in K$ so that

$$xy = k \leftrightarrow x = ky^{-1},$$

and since $k, y \in K$ this implies that $x \in K$, a contradiction. Therefore, we cannot have that $H, K \neq G$ and $H \cup K = G$. □

Problem 79 (Section 1.3, Exercise 3)**.** Let G be a group. Define the right translation a_R for $a \in G$ as the map $x \mapsto xa$ in G. Show that $G_R = \{a_R\}$ is a transformation group of the set G and $a \mapsto a_R^1$ is an isomorphism of G with G_R.

Proof. We first show that it's a transformation group. That is, we need to show that a_R is a bijection $G \to G$, and G_R is a group. To see that a_R is a bijection, we see that

$$a_R(x) = a_R(y) \leftrightarrow xa = ya \leftrightarrow x = y,$$

so it is injective, and to get surjective, we note

$$a_R(ya^{-1}) = y$$

for all $y \in G$. Next, we first see G_R is closed under composition. That is,

$$a_R \circ b_R \in G_R.$$

Notice that

$$a_R \circ b_R(x) = a_R(xb) = xba = (ba)_R(x) \in G_R.$$

So it is indeed closed under composition. Associativity follows from the associativity of composition of functions. We have an identity, via noticing that

$$e_R(x) = xe = x$$

for all $x \in G$, and so $e_R = I \in M(G)$. Finally, given $a_R \in G_R$, we can construct an inverse via taking a_R^{-1}; notice that

$$a_R \circ a_R^{-1}(x) = a_R(xa^{-1}) = xa^{-1}a = x$$

for all $x \in G$, so $a_R \circ a_R^{-1} = I$. Hence, this is a group of transformations on G.

We now need to show that $f : G \to G_R$ via $f(x) = x_R^{-1}$ is an isomorphism. For injectivity, we see

$$f(x) = f(y) \leftrightarrow x_R^{-1}(a) = y_R^{-1}(a)\ \forall a \in G \leftrightarrow ax^{-1} = ay^{-1} \leftrightarrow x = y.$$

For surjectivity, notice that we can get any transformation by just taking the inverse of it's respective element. Finally, to see it's a homomorphism, we have

$$f(xy) = (xy)_R^{-1} = (y^{-1}x^{-1})_R,$$
$$f(x)f(y) = x_R^{-1} \circ y_R^{-1} = (y^{-1}x^{-1})_R,$$

so

$$f(xy) = f(x)f(y)$$

for all $x, y \in G$. Hence, it is an isomorphism. □

Problem 80 (Section 1.3, Problem 5)**.** Is the additive group of rationals isomorphic to the multiplicative group of non-zero rationals?

Proof. No. Assume that it were; for example, we have $f(p/q) = 2$ for some $p/q \in \mathbb{Q}$. But we see that

$$f(p/(2q) + p/(2q)) = f(p/(2q))f(p/(2q)) = 2,$$

but this implies that

$$f(p/(2q)) = \sqrt{2},$$

which is not a rational number. So there cannot be an isomorphism. □

Problem 81 (Section 1.3, Problem 6)**.** In $\mathbb{Z}$, define $a \circ b = a + b - ab$. Show that $(\mathbb{Z}, \circ, 0)$ is a monoid, and that the map $a \mapsto 1 - a$ is an isomorphism of the multiplicative monoid $(\mathbb{Z}, \cdot, 1)$ with $(\mathbb{Z}, \circ, 0)$.

Proof. We break this up into steps.
Step 1: We first show that $(\mathbb{Z}, \circ, 0)$ is a monoid. To do so, we need to show three properties.

(1) (Closure) $\mathbb{Z}$ is closed under multiplication and addition, so clearly $a \circ b = a + b - ab \in \mathbb{Z}$. Hence, it's closed.

(2) (Associative) We have

$$(a \circ b) \circ c = (a + b - ab) \circ c = (a + b - ab) + c - c(a + b - ab) = a + b - ab + c - ca - cb + cab,$$
$$a \circ (b \circ c) = a \circ (b + c - bc) = a + b + c - bc - a(b + c - bc) = a + b + c - bc - ab - ac + abc.$$

Hence, we see that

$$(a \circ b) \circ c = a \circ (b \circ c),$$

so the operation is associative.

(3) (Identity) We need to show 0 is the identity. Notice that for all $a \in \mathbb{Z}$,

$$a \circ 0 = a + 0 - a(0) = a = 0 + a - 0(a) = 0 \circ a,$$

so 0 is indeed an identity.

Hence, $(\mathbb{Z}, \circ, 0)$ is a monoid.
Step 2: We need to show that $f : (\mathbb{Z}, \cdot, 1) \to (\mathbb{Z}, \circ, 0)$ is an isomorphism. That is, it is a bijective homomorphism. First, let's show it is bijective. To see that it is injective, we have

$$f(a) = f(b) \leftrightarrow 1 - a = 1 - b \leftrightarrow a = b.$$

To see it is surjective, notice that for all $a \in \mathbb{Z}$, we have $1 - a \in \mathbb{Z}$, so

$$f(1 - a) = 1 - (1 - a) = a.$$

So it is a bijection.

To see it is a homomorphism, we need to show that $f(ab) = f(a) \circ f(b)$. Notice that

$$f(ab) = 1 - ab,$$
$$f(a) \circ f(b) = (1-a) \circ (1-b) = (1-a) + (1-b) - (1-a)(1-b) = 2 - a - b - (1 - b - a + ab) = 1 - ab.$$

Hence, $f(ab) = f(a) \circ f(b)$, and so it is a homomorphism.

Since it is a bijective homomorphism, it is an isomorphism. □

Problem 82 (Section 1.4, Exercise 1)**.** Let A be a monoid, $M(A)$ the monoid of transformations of A into itself, A_L the set of left translations a_L, and A_R the set of right translations a_R. Show that A_L is the centralizer of A_R in $M(A)$ and vice versa. Show that $A_L \cap A_R = \{c_R = c_L \ : \ c \in C\}$, C the center of A.

Proof. **Step 1:** We need to show that A_L is the centralizer of A_R in $M(A)$. Recall that the centralizer is the set of elements in $M(A)$ such that they commute with all of A_R. We first establish that $A_L \subset C(A_R)$. Take $a_L \in A_L$. Then we have

$$a_L \circ b_R(x) = axb = b_R \circ a_L(x) \ \forall x \in A.$$

Hence, $a_L \in C(A_R)$. Since the choice of a_L was arbitrary, we get $A_L \subset C(A_R)$.

Next, we need to show that $C(A_R) \subset A_L$. Take $c \in C(A_R)$. Then we have

$$c \circ b_R(x) = b_R \circ c(x).$$

Notice that the left hand side gives

$$c \circ b_R(x) = c(xb)$$

and the right hand side gives

$$b_R \circ c(x) = c(x)b.$$

So we have that $c(xb) = c(x)b$ for all $x, b \in A$. Notice that for $x = e$, we find $c(b) = c(e)b$ for all $b \in A$. So we have $c(x) = c(e)x$, and hence $c(x) = c(e)_L \in A_L$. Since this was for arbitrary $c \in C(A_R)$, we have that $C(A_R) \subset A_L$. Hence, they are equal.

A similar argument applies to show $A_R = C(A_L)$.

Step 2: Take $f \in A_L \cap A_R$. Then since $f \in A_L$, we have f commutes with all of A_R, and likewise f commutes with all of A_L. Notice as well that from our prior argument f is determined completely by where it sends 1; that is $f = f(1)_L = f(1)_R$. Denote $f(1) = a$. Furthermore, since $a_L = a_R$, we have

$$a_L(x) = ax = xa = a_R(x),$$

so $a \in C$. □

Problem 83 (Section 1.4, Exercise 2)**.** Show that if $n \geq 3$, $C(S_n) = 1$.

Proof. Assume $n \geq 3$, take $\gamma \in C(S_n)$ non-trivial. Since $\gamma \in C(S_n)$, we have

$$\sigma\gamma\sigma^{-1} = \gamma$$

for all $\sigma \in S_n$. Recall that, rewriting γ in terms of a cycle (WLOG take it to just be $(\gamma_1, \ldots, \gamma_k)$), we have

$$\sigma\gamma\sigma^{-1} = (\sigma(\gamma_1), \ldots, \sigma(\gamma_k)).$$

So we have $\sigma(\gamma_1) = \gamma_1, \ldots, \sigma(\gamma_n) = \gamma_n$. But this cannot hold for all σ; take $\sigma(\gamma_1) = \gamma_2$, $\sigma(\gamma_2) = \gamma_1$ if $k \geq 3$, and if $k = 2$ take $\sigma(\gamma_1) = j$ for $j \neq \gamma_1, \gamma_2$. Then we have $\sigma\gamma\sigma^{-1} \neq \gamma$, which is a contradiction of $\gamma \neq 1$ being in the center. Thus, $\gamma = 1$. □

Problem 84 (Center of Dihedral Group pt. 1)**.** Show that the center of the Dihedral group D_{2n} is trivial for $n > 2$ odd.

Proof. Recall

$$D_{2n} = \langle r, \tau \ : \ r^n = \tau^2 = 1, \tau r \tau = r^{n-1}. \rangle$$

Let $\gamma \in C(D_{2n})$. That is,

$$\sigma\gamma = \gamma\sigma$$

for all $\sigma \in D_{2n}$. Notice that elements in D_{2n} are of the form $r^k\tau^j$, $0 \leq k < n$, $0 \leq j < 2$. So we have

$$\sigma r^k \tau^j = r^k \tau^j \sigma.$$

It suffices to check this on generators. Notice that if $\sigma = \tau$, we have

$$\tau r^k \tau = r^k,$$

but this can only happen if $n - k = k$. That is, $n = 2k$, which is a contradiction. □

Problem 85 (Center of Dihedral Group pt. 2)**.** Show that the center of D_{2n} is non-trivial for n even, $n \geq 2$. Explicitly calculate it.

Proof. Again, it suffices to check it on generators. From before, we had if $\sigma = \tau$, then this forces $k = n/2$. If $\sigma = r$, we have

$$r^{k+1}\tau^j = r^k \tau^j r.$$

Consider the case where $j = 0$. Then these are clearly equal. Consider now the case where $j = 1$. Notice from the presentation that $r\tau r = \tau$, so we have

$$r^{k+1}\tau = r^{k-1},$$

or in other words

$$r^2\tau = 1 \leftrightarrow r^2 = \tau.$$

For $n = 2$, we see that this holds, and so $D_4 = Z(D_4)$ (this checks out with the fact that $D_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$). If $n > 2$, we see that this is false, and so $j \neq 1$. Hence, we have that $Z(D_{2n})$ for $n > 2$ is $\{e, r^{n/2}\}$. □

Problem 86 (Section 1.5, Exercise 2)**.** Let M be a monoid generated by a set S (i.e. $\langle S \rangle = M$) and suppose every element of S is invertible. Show that M is a group.

Proof. Since M is a monoid, to show that M is a group we just need to show that for every $x \in M$, there is an $x^{-1} \in M$ such that $xx^{-1} = x^{-1}x = e$. Using the constructive definition, which is equation (11) on page 43 in the book, we have that every $x \in M$ is such that

$$x = s_1 \cdots s_r, \quad s_i \in S, r \geq 1.$$

Since every s_i has an inverse, denoted by s_i^{-1}, we can write

$$x^{-1} = s_r^{-1} \cdots s_1^{-1}.$$

Then we have

$$x^{-1}x = (s_r^{-1} \cdots s_1^{-1})(s_1 \cdots s_r),$$

and using associativity we get

$$x^{-1}x = s_r^{-1} \cdots (s_1^{-1}s_1) \cdots s_r = s_r^{-1} \cdots s_2^{-1}s_2 \cdots s_r = \cdots = e.$$

Likewise, we have

$$xx^{-1} = s_1 \cdots s_r \cdot s_r^{-1} \cdots s_1^{-1} = \cdots = e.$$

So we get that every element is invertible in M, and so M is a group. □

Problem 87 (Section 1.5, Exercise 3)**.** Let G be an abelian group with a finite set of generators which is periodic in the sense that all of its elements have finite order. Show that G is finite.

Proof. Let $\langle S \rangle = G$, $S = \{a_1, \ldots, a_n\}$, $o(a_i) = l_i < \infty$. Then we have that, for all $g \in G$,

$$g = a_1^{k_1} \cdots a_n^{k_n},$$

where $0 \leq k_i < l_i$. We see that $o(G) = \prod_{i=1}^n l_i < \infty$. □

Problem 88 (Section 1.5, Exercise 5)**.** Show that any finitely generated subgroup of the additive group of rationals $(\mathbb{Q}, +, 0)$ is cyclic. Use this to prove that this group is not isomorphic to the direct product of two copies of it.

Proof. **Step 1:** Let $H \leq \mathbb{Q}$ be a subgroup such that $H = \langle S \rangle$, $S = \{p_1/q_1, \ldots, p_n/q_n\}$. Notice that $S \subset \langle 1/(q_1 \cdots q_n) \rangle$, so $\langle S \rangle = H \leq \langle 1/(q_1 \cdots q_n) \rangle$. Hence, a subgroup of a cyclic group is cyclic, and so H is cyclic.
Step 2: Take $H \leq \mathbb{Q} \times \mathbb{Q}$, where $H = \langle (0,1), (1,0) \rangle$. Then if $\mathbb{Q} \times \mathbb{Q} \cong \mathbb{Q}$, we have that H is cyclic. It suffices then to show that H is not cyclic. If it were cyclic, then $H = \langle (a,b) \rangle$, $a, b \in \mathbb{Q}$. So $(1,0) = n(a,b)$, $(0,1) = m(a,b)$, and therefore $a = b = 0$, a contradiction. Hence, H is not cyclic. □

Problem 89 (Bezout's Lemma)**.** If $(m,n) = d$, show that there are integers $a, b \in \mathbb{Z}$ so that

$$am + bn = d.$$

Proof. Since $d \mid m, n$, let $x = dx_1$, $y = dy_1$. Thus, we have that $(x_1, y_1) = 1$. Therefore, $[x_1, y_1] = x_1 y_1$. So y_1 is the smallest positive number so that

$$x_1 y_1 \equiv 0 \pmod{y}.$$

Now, if for all other integers $0 \leq a, b < y_1$, we have that

$$x_1 a \not\equiv x_1 b \pmod{y_1}$$

implies that there is an a in this range so that

$$x_1 a \equiv 1 \pmod{y_1}$$

by Pidgeonhole principle. If there is an $a \neq b$ so that

$$x_1 a \equiv x_1 b \pmod{y_1},$$

then assuming $b > a$ we have that

$$x_1(b-a) \equiv 0 \pmod{y_1},$$

and this contradicts the minimality of y_1. So we have there is an a so that

$$x_1 a \equiv 1 \pmod{y_1}.$$

Thus, $y_1 \mid x_1 a - 1$, and so there is an integer b so that $x_1 a - 1 = b y_1$, or $x_1 a - b y_1 = 1$. Multiplying by d and letting $c = -b$, we have

$$a(dx_1) + c(dy_1) = ax + cy = d.$$

□

Problem 90 (Section 1.5, Exercise 6)**.** Let a, b be as in Lemma 1. That is, let a and b be elements of an abelian group G such that $o(a) = n$, $o(b) = m$, $m, n < \infty$, and $(m,n) = 1$. Show that $\langle a \rangle \cap \langle b \rangle = 1$ and $\langle a, b \rangle = \langle ab \rangle$.

Proof. Let $x \in \langle a \rangle \cap \langle b \rangle$. We see that $\langle x \rangle \leq \langle a \rangle$; that is, is is a subgroup of the cyclic group. Then we have that $o(x) \mid n$. Likewise, $\langle x \rangle \leq \langle b \rangle$, so $o(x) \mid m$. Since $1 \leq o(x) \leq (m,n) = 1$, we must have that $o(x) = 1$. Thus, $x = 1$.

Next, we want to show that $\langle a, b \rangle = \langle ab \rangle$. Notice first we have

$$\langle a, b \rangle = \{1, s_1 \cdots s_r \ : \ s_i \text{ or } s_i^{-1} \in \{a, b\}\}.$$

It's clear by this construction that

$$\langle ab \rangle \subseteq \langle a, b \rangle.$$

So it suffices to show the other direction. Let $x \in \langle a, b\rangle$. Then

$$x = s_1 \cdots s_r.$$

Since the group G is abelian, we can write this as

$$x = a^k b^j, \quad k + j = r, \quad 0 < j < m, \ 0 < k < n$$

If $k = j$, we are done; $x \in \langle ab\rangle$. Notice that taking $(ab)^n = b^n$, $(ab)^m = a^m$. Since $(m, n) = 1$, Bezout's lemma gives there are integers $a, b \in \mathbb{Z}$ such that

$$am + bn = 1.$$

Now, assume without loss of generality that $k < j$ (the argument works the same the other direction). Then we have

$$x = (ab)^k b^{j-k}.$$

So it suffices to show that $b^{j-k} \in \langle ab\rangle$, since clearly $(ab)^k \in \langle ab\rangle$. Using Bezout's lemma, we have

$$a(j-k)m + b(j-k)n = (j-k).$$

Since $o(b) = m$, we can write this as

$$b(j-k)n = (j-k) - a(j-k)m.$$

So we see that

$$(ab)^{b(j-k)n} = a^{b(j-k)n} b^{(j-k)-a(j-k)m} = b^{j-k},$$

so $b^{j-k} \in \langle ab\rangle$. Hence, $x \in \langle ab\rangle$, and since this works for arbitrary $x \in \langle a, b\rangle$, we have $\langle a, b\rangle = \langle ab\rangle$. □

Problem 91 (Section 1.7, Exercise 2)**.** Show that if G is finite and H and K are subgroups such that $K \subseteq H$, then

$$[G : K] = [G : H][H : K].$$

Proof. Since G is finite, we have that all the indices will be finite as well. Hence, let $[G : H] = n$. Then we have representatives so that

$$G = \bigsqcup_{i=1}^{n} y_i H.$$

If we let $[H : K] = r$, we have

$$H = \bigsqcup_{j=1}^{r} z_j K.$$

Substituting this in, we get

$$G = \bigsqcup_{i=1}^{n} \bigsqcup_{j=1}^{r} y_i z_j K.$$

Since $H \subseteq G$, we get $y_i z_j = g_{i,j}$ for some g. So we get

$$G = \bigsqcup_{i=1}^{n} \bigsqcup_{j=1}^{r} g_{i,j} K.$$

Notice, however, this is the same as just taking

$$G = \bigsqcup_{i=1}^{nr} g_i K.$$

Hence,

$$[G : H] = nr = [G : H][H : K].$$

□

Problem 92 (Section 1.7, Exercise 3)**.** Let H_1, H_2 be subgroups of G. Show that any right coset relative to $H_1 \cap H_2$ is the intersection of a right coset of H_1 with a right coset of H_2. Use this to prove Poincare's Theorem; that if H_1 and H_2 have finite index in G, then so has $H_1 \cap H_2$.

Proof. **Step 1:** Take a right coset relative to $H_1 \cap H_2$; that is, let $(H_1 \cap H_2)x$. Then we have

$$(H_1 \cap H_2)x = \{hx \ : \ h \in H_1 \cap H_2\}.$$

However, we notice that

$$\{hx \ : \ h \in H_1 \cap H_2\} = \{hx \ : \ h \in H_1\} \cap \{hx \ : \ h \in H_2\} = H_1x \cap H_2x.$$

Step 2: If H_1, H_2 have finite index, then we have that there are finite representatives such that

$$G = \bigsqcup_{i=1}^{n} H_1 x_i,$$

$$G = \bigsqcup_{j=1}^{m} H_2 x_j.$$

Then we see that, by **Step 1**, any representative $(H_1 \cap H_2)x_k$ for the right coset of the intersection must be a representative for H_1 and H_2. Hence, the number of representatives is finite, since H_1 and H_2 have finite representatives. □

Problem 93 (Section 1.7, Exercise 4 (Schrier's Lemma))**.** Let G be a finitely generated group, H a subgroup of finite index (that is, $[G : H] = n < \infty$). Show that H is finitely generated.

Proof. Let $G = \langle S \rangle$, $S = \{x_1, \ldots, x_r\}$. Then

$$G = \bigsqcup_{i=1}^{n} y_i H,$$

where the y_i are taken to be representatives of the cosets. Take $y_1 = 1$ without loss of generality. Since the $x_i \in G$ by assumption, we get that $x_i y_j \in y_{k_{i,j}} H$ for all i, j, and hence there is an $h_{i,j}$ so that

$$x_i y_j = y_{k_{i,j}} h_{i,j}.$$

Now, take $h \in H$. We have that

$$h = x_{l_1} \cdots x_{l_v}.$$

Notice that

$$x_{l_v} = y_{k_{1,l_v}} h_{l_v,1}.$$

So we can rewrite this as

$$h = x_{l_1} \cdots x_{l_{v-1}} y_{k_{1,l_v}} h_{l_v,1}.$$

We now examine

$$x_{l_{v-1}} y_{k_{1,l_v}} = y_{k_{l_{v-1},k_{1,l_v}}} h_{l_{v-1},k_{1,l_v}}.$$

We can continue replacing these generators, and after relabeling we get

$$h = y \cdot h_{l_1} \cdots h_{l_v}.$$

Since $h \in H$, we get that $y = 1$, and so we have

$$h = h_{l_1} \cdots h_{l_v}.$$

So taking the set

$$S' = \{h_{1,1}, \ldots, h_{r,n}\},$$

we see that

$$\langle S' \rangle = H.$$

Hence, H is finitely generated. □

Problem 94 (Section 1.7, Exercise 5)**.** Let H and K be two subgroups of a group G. Show that the set of maps $x \to hxk$, $h \in H$, $k \in K$ is a group of transformations of the set G. Show that the orbit of x relative to this group is the set $HxK = \{hxk \ : \ h \in H, k \in K\}$. This is called the double coset of x relative to the pair (H, K). Show that if G is finite, then $|HxK| = |H|[K : x^{-1}Hx \cap K] = |H|[H : xKx^{-1} \cap H]$.

Proof. **Step 1:** We need to show that the set of maps $\{f_{hk} \ : \ f_{hk}(x) = hxk\}$ is a group of transformations of the set G. To do so, we need to show that its closed under composition, the identity is in it, and it is closed under inverses.

To see it's closed under composition, take $f_{hk}, f_{h'k'}$. Then we have

$$(f_{hk} \circ f_{h'k'})(x) = f_{hk}(h'xk') = hh'xk'k = f_{hh'k'k}(x).$$

Since this applies for all $x \in G$, we get that the maps are equal, and so the set is closed. To see that the identity is in it, we notice that $1 \in H \cap K$, and so

$$f_{11}(x) = 1x1 = x = I(x),$$

and so I is in this set as well. Finally, we need to show it's closed under inversion. Notice that the inverse of the map f_{hk} will be $f_{h^{-1}k^{-1}}$, which is in this set as well since H and K are closed under inversions. Hence, this is indeed a group of transformations.

Step 2: We now need to show that the orbit of x relative to this group is the set HxK. Denote the group above by Z. Then we want to show that $Zx = HxK$. We see clearly that $Zx = \{f_{hk}(x) \ : \ f_{hk} \in Z\} \subset HxK$, so it suffices to go the other direction. However, this is also clear; if $hxk \in HxK$, take the function $f_{hk} \in Z$.

Step 3: Let $F = x^{-1}Hx \cap K$, then we want to establish a bijection between the cosets of F in K and the cosets of H in HxK. Let $f(Fk) = Hxk$. We need to show that this is well-defined, injective, and surjective. To see it's well-defined, let $Fk' = Fk$. Then $k'k^{-1} \in F = x^{-1}Hx \cap K$, which tells us that $k'k^{-1} \in x^{-1}Hx$, and so $xk'k^{-1}x^{-1} = (xk')(xk)^{-1} \in H$. Hence, $Hxk = Hxk'$. To see it's injective, we have $Hxk = Hxk' \leftrightarrow (xk)(xk')^{-1} \in H \leftrightarrow kk'^{-1} \in x^{-1}Hx \cap K \leftrightarrow Fk = Fk'$. Finally, we see that surjectivity is clear. Thus,

$$[K : x^{-1}Hx \cap K] = [HxK : H] \leftrightarrow |H|[K : x^{-1}Hx \cap K] = |HxK|.$$

The other equality is proven in the same way. □

Problem 95 (Section 1.8, Exercise 5)**.** Verify that the intersection of any set of normal subgroups of a group is a normal subgroup. Show that if H and K are normal subgroups, then HK is a normal subgroup.

Proof. **Step 1:** We need to verify that $\cap_\alpha H_\alpha$, $H_\alpha \trianglelefteq G$, is normal. Notice that for $h \in \bigcap_\alpha H_\alpha$, we have $xhx^{-1} \in H_\alpha$ for all α, since H_α is normal. Since this applies for all h, we get

$$x\left(\bigcap_\alpha H_\alpha\right)x^{-1} \subset \bigcap_\alpha H_\alpha,$$

and so this, too, is normal.

Step 2: We have that HK is a subgroup, since H is normal. To see that it is normal, we have

$$xHKx^{-1} = xHx^{-1}xKx^{-1} = HK.$$

Hence, it's a normal subgroup. □

Problem 96 (Section 1.8, Exercise 6)**.** Let G_1, G_2 be simple groups. Show that every normal subgroup of $G_1 \times G_2$ is either G, isomorphic to G_1, isomorphic to G_2, or is trivial.

Proof. Let $H_1 \times H_2 \leq G$. Then if this is normal, we have $x(H_1 \times H_2)x^{-1} = H_1 \times H_2$. But this implies that it is normal in each component, so we must have that $H_1 \cong \{G_1, 1\}$, $H_2 \cong \{G_2, 1\}$, and this gives us all possibilities. □

Problem 97 (Section 1.8, Exercise 7)**.** Let $\equiv$ be an equivalence relation on a monoid M. Show that $\equiv$ is a congruence if and only if the subset $M \times M$ defining $\equiv$ is a submonoid of $M \times M$.

Proof. ($\implies$) Let $S \subset M \times M$ be defined by $(a, b) \in S$ if and only if $a \equiv b$. Since this is a congruence $(a, b), (a', b') \in S$ implies $aa' \equiv bb'$ implies $(aa', bb') \in S$. Furthermore, $(1, 1) \in S$. So it's closed, associative, and there's an identity, and so S is a submonoid.
($\impliedby$) Assume S is a submonoid. Then it's closed under multiplication, and so $(a, b), (a', b') \in S$ tells us $(aa', bb') \in S$, or $a \equiv b$, $a' \equiv b'$ implies $aa' \equiv bb'$. So, $\equiv$ is a congruence. □

Problem 98 (Section 1.8, Exercise 8)**.** Let $\{\equiv_i\}$ be a set of congruences on M. Define the intersection as the intersection of the corresponding subsets of $M \times M$. Verify that this is a congruence.

Proof. Intersection of submonoids is a submonoid, the corresponding $\equiv$ will be a congruence as a result. □

Problem 99 (Section 1.8, Exercise 9)**.** Let G_1, G_2 be subgroups of G, and let α be the map of $G_1 \times G_2$ into G by $\alpha(g_1, g_2) = g_1 g_2$. Show that the fiber over $g_1 g_2$ – that is, $\alpha^{-1}(g_1 g_2)$ – is the set of pairs $(g_1 k, k^{-1} g_2)$, where $k \in G_1 \cap G_2$. Hence, show that all fibers have the same cardinality, namely, that of $G_1 \cap G_2$. Use this to show that if G_1 and G_2 are finite, then

$$|G_1 G_2| = \frac{|G_1||G_2|}{|G_1 \cap G_2|}.$$

Proof. **Step 1:** We want to show

$$\alpha^{-1}(g_1 g_2) = \{(g_1 k, k^{-1} g_2) \ : \ k \in G_1 \cap G_2\}.$$

One direction is clear, which is that

$$\{(g_1 k, k^{-1} g_2) \ : \ k \in G_1 \cap G_2\} \subset \alpha^{-1}(g_1 g_2).$$

For the other direction, take $(a, b) \in \alpha^{-1}(g_1 g_2)$. We have that $\alpha(a, b) = ab = g_1 g_2$, so $g_1^{-1} a = g_2 b^{-1}$. So $g_1^{-1} a \in G_1 \cap G_2$, $g_2 b^{-1} \in G_1 \cap G_2$. So let $k \in G_1 \cap G_2$ be such that $k = g_1^{-1} a = g_2 b^{-1}$. Then we have $g_1 k = a$, $b = k^{-1} g_2$. So we have equality.
Step 2: We then want to establish that all fibers have the same cardinality. Let $f : \alpha^{-1}(g_1 g_2) \to K = G_1 \cap G_2$ via $f(g_1 k, k^{-1} g_2) = k$. We see that this is well-defined, since $(g_1 k, k^{-1} g_2) = (g_1 k', k'^{-1} g_2)$ implies $k = k'$, and so they map to the same thing. Injective and surjective are also clear.
Step 3: We see that

$$|G_1 \times G_2| = |G_1||G_2| = \sum_{g_1 g_2 \in G_1 G_2} \alpha^{-1}(g_1 g_2) = |G_1 \cap G_2| \sum_{g_1 g_2 \in G_1 G_2} 1 = |G_1 \cap G_2||G_1 G_2|.$$

□

Problem 100 (Section 1.8, Exercise 10)**.** Let G be a finite set, A and B non-vacuous subsets of G. Show that $G = AB$ if $|A| + |B| > |G|$.

Proof. Assume $|A| + |B| > |G|$. First, notice that $AB \subset G$, since G is closed under multiplication. Next, notice that we have

$$|A| + |B| = |A \cap B| + |A \cup B|.$$

If $|A| + |B| > |G|$, $|A \cup B| < |G|$, we get

$$|A \cap B| + |A \cup B| > |G| \leftrightarrow |A \cap B| > 0.$$

Hence, they are non-trivial. Now, notice that for all $g \in G$, we have $A^{-1}g = \{a^{-1}g \ : \ a \in A\}$ has the same order as A, and so $|A^{-1}g \cap B| \neq 0$. Thus, taking $y \in A^{-1}g \cap B$, we have $y = a^{-1}g = b$, or $ab = g$. Since we can do this for all $g \in G$, we have $G \subset AB$, giving the desired result. □

Problem 101 (Section 1.9, Exercise 4)**.** Determine $\mathrm{Aut}(G)$ for the following:

(i) G an infinite cyclic group,
(ii) a cyclic group of order 6,
(iii) for any finite cyclic group.

Proof. (i) $G \cong \mathbb{Z} = \langle 1, -1 \rangle$. Since this is cyclic, we must have generators are sent to generators, so we get either $-1 \mapsto 1$ or $-1 \mapsto -1$. Hence, $\mathrm{Aut}(G) \cong \mathbb{Z}_2$.
(ii) Again, generators have to map to generators, $\varphi(6) = 2$, so the only automorphisms are $1 \mapsto 1$, $1 \mapsto 5$, and so $\mathrm{Aut}(G) \cong \mathbb{Z}_2$.
(iii) From the prior arguments, $\mathrm{Aut}(G) \cong \mathbb{Z}_{\varphi(n)}$, where $|G| = n$.

□

Problem 102 (Section 1.9, Exercise 5)**.** Determine $\mathrm{Aut}(S_3)$.

Proof. We have $S_3 = \langle (12), (123) \rangle$. For this to be an automorphism, we need to map generators to generators. We have 3 options for where we map (12), 2 options for where we map (123), and so we have $|\mathrm{Aut}(S_3)| = 6$. Up to isomorphism there are two options for $\mathrm{Aut}(S_3)$; either it's $\mathbb{Z}_6$ or it's S_3. To see that it's not $\mathbb{Z}_6$, it suffices to show that it's not commutative. This is a lot of effort, and I don't feel like doing this. □

Problem 103 (Section 1.9, Exercise 7)**.** Let G be a group such that $\mathrm{Aut}(G) = 1$. Show that G is abelian and that every element of G satisfies the equation $x^2 = 1$. Show that if G is finite, then $|G| = 1, 2$.

Proof. **Step 1:** We first establish that G is abelian. Notice that $G/C \cong \mathrm{Inn} \leq \mathrm{Aut}(G)$. Since $\mathrm{Aut}(G) = 1$, this implies $C = G$.
Step 2: The inversion map is an automorphism for abelian groups, but since the automorphisms are all trivial this implies that $x^{-1} = x$, or every element has at most order 2.
Step 3: Cauchy's theorem gives us the desired result. □

Problem 104 (Section 1.9, Exercise 8)**.** Let α be an automorphism of a group G which fixes only the unit of G; that is, $\alpha(a) = a$ implies $a = 1$. Show that $f(a) = \alpha(a)a^{-1}$ is injective. Deduce that if G is finite, then every element of G has the form $\alpha(a)a^{-1}$.

Proof. To see it's injective, we note that $f(a) = f(b)$ implies $\alpha(a)a^{-1} = \alpha(b)b^{-1}$. Hence, $\alpha(ab^{-1}) = ab^{-1}$, which implies that $ab^{-1} = 1$, or $a = b$. If G is finite, then we have a map $f : G \to G$ which is injective, and so it's surjective and therefore bijective. So every element is of the form $\alpha(a)a^{-1}$. □

Problem 105 (Section 1.9, Exercise 9)**.** Let G and α be as given in the prior problem. Assume that $\alpha^2 = 1$. Show that G is abelian of odd order.

Proof. By the second part of the last problem, every element is of the form $\alpha(a)a^{-1}$. So

$$\alpha(\alpha(a)a^{-1}) = \alpha^2(a)\alpha(a)^{-1} = a\alpha(a)^{-1} = (\alpha(a)a^{-1})^{-1}$$

Since the inverse map is an automorphism, we get that the group is abelian.

Cauchy's theorem tells us that if G is not of odd order, there is an element $a \in G - \{e\}$ such that $a^2 = 1$. Notice that $\alpha(a) = a$, but this implies that $a = 1$, a contradiction. Hence, G must be of odd order. □

Problem 106 (Section 1.12, Exercise 10)**.** Let G be a group, H a transformation group acting on a set S, and let G^S denote the set of maps of S into G. Then G^S is a group if we define $(f_1 f_2)(s) = f_1(s)f_2(s)$, $f_i \in G^S$, $s \in S$. If $h \in H$ and $f \in G^S$, defined hf by $(hf)(s) = f(h^{-1}s)$. Verify that this defines an action of H on G^S by automorphisms.

Proof. **Step 1:** We verify that G^S is a group with this. We have that there is a map $f = 1$ for all $s \in S$, which we denote by I. This is the identity, since $(If_1)(s) = I(s)f_1(s) = f_1(s)$ for all $f_1 \in G^S$, $s \in S$. Same with left multiplication. For inverses, we define $f^{-1} \in G^S$ via $f^{-1}(s) = (f(s))^{-1}$. Then we have $(f^{-1}f)(s) = (f(s))^{-1}(f(s)) = 1$.
Step 2: We verify that this is an action. We need to check two things:

(i) We have $(1f)(s) = f(1^{-1}s) = f(s)$ for all $s \in S$, so $1f = f$ for all $f \in G^S$.

(ii) Notice that

$$(h_1h_2)f(s) = f(h_2^{-1}h_1^{-1}s) = h_2f(h_1^{-1}s) = h_1(h_2(f(s)))$$

for all $s \in S$, $f \in G^S$, so we get

$$(h_1h_2)f = h_1(h_2f).$$

Remark. By automorphisms, it may mean to show that this defines an automorphism $T : H \to \mathrm{Aut}(G^S)$. However, this is equivalent to showing what we've shown above.

□

Problem 107 (Section 1.13, Exercise 1)**.** Show that if P is a Sylow subgroup, then $N(N(P)) = N(P)$.

Proof. One inclusion is clear, that is, $N(P) \subset N(N(P))$. For the other, let $x \in N(N(P))$. Then we have that

$$xPx^{-1} \subset xN(P)x^{-1} = N(P),$$

so that P and xPx^{-1} are two Sylow subgroups of $N(P)$. So, there exists $a \in N(P)$ so that

$$P = aPa^{-1} = xPx^{-1},$$

and so we get that $x \in N(P)$.

Remark. Alternatively, $P \trianglelefteq N(P)$, so that P is the *only* Sylow subgroup of $N(P)$. Use this to also determine the result.

□

Problem 108 (Section 1.13, Exercise 2)**.** Show that there are no simple groups of order 148 or of order 56.

Proof. (1) Let $|G| = 148$. Write

$$|G| = 2^2 \cdot 37.$$

Now, the number of Sylow 37 subgroups of G is 1 (clearly), so we have that the Sylow 37 subgroup is normal. Hence, it is not simple.

(2) Write

$$|G| = 56 = 2^3 \cdot 7.$$

We have the number of Sylow 7 subgroups is

$$n_7(G) = \{1, 8\},$$

and the number of Sylow 2 subgroups is

$$n_2(G) = \{1, 7\}.$$

Assume $n_7(G) = 8$, $n_2(G) = 7$. Then we have that this accounts for $(6 \cdot 8) + (7 \cdot 7) + 1 = 98$ elements, which is an overcount. Hence, we cannot have that they are both not 1, so at least one must be normal. Hence, it's not simple.

□

Problem 109. Let G be a finite group of order 216. Show that G is not simple.

Proof. Recall that being simple means that the only normal subgroups of G are $\{1\}$ and itself. Write

$$216 = 2^3 \cdot 3^3.$$

Let n_2 denote the number of Sylow 2 subgroups. We have that

$$n_2 \equiv 1 \pmod 2, \quad n_2 \mid 27.$$

Hence,

$$n_2 = \{1, 3, 9, 27\}.$$

Likewise, we have that

$$n_3 \equiv 1 \pmod 3, \quad n_3 \mid 8,$$

so

$$n_3 = \{1, 4\}.$$

If $n_3 = 1$, we win, since this means that the Sylow 3-subgroup is normal. Assume for contradiction that $n_3 = 4$. Consider a map $\phi : G \to S_4$. Since $4! = 24 \neq 216$, we must have $\ker(\phi) \leq G$ is non-trivial. Hence, we have a normal subgroup. □

Problem 110. If $G = \langle x, y \ : \ x^4 = y^4 = 1, xy = yx^{-1} \rangle$, and $H = \langle y^2 \rangle \leq G$, then $H \trianglelefteq G$.

Proof. We check on the generators; this will be sufficient. Notice that for x, we have

$$xy^2 = xyy = yx^{-1}y = y^2x,$$

$$x1 = 1x,$$

and for y we have

$$yy^2 = y^3 = y^2y,$$

$$y1 = 1y.$$

Hence, it is normal. □

Problem 111. If $H \leq G$, then the number of conjugates of H in G is $[G : N_G(H)]$.

Proof. Let G act on the space of conjguates of H $K = \{gHg^{-1} \ : \ g \in G\}$ in the following way; $g \cdot (kHk^{-1}) = gkHk^{-1}g^{-1}$. We see that the orbit stabilizer theorem gives us that the size of the orbit of H (i.e. the number of conjugates of H) is given by $[G : \text{Stab}_G(H)]$. Notice that $\text{Stab}_G(H) = \{g \in G \ : \ gHg^{-1} = H\}$, which corresponds to the normalizer of H. Hence, this does correspond to the number of conjugates. □

Problem 112. All abelian groups are solvable.

Proof. We have a condition that a group is solvable iff $G^{(n)} = \{e\}$ for some n, where $G' = G^{(1)} = [G, G]$. Since G is abelian, $G' = \{e\}$, so it is indeed solvable. □

Problem 113. Let H and K be finite groups. Identify K with its isomorphic copy in $H \rtimes K$ via $k \mapsto (1, k)$. If $K \trianglelefteq H \rtimes K$, then $H \rtimes K \cong H \times K$.

Proof. This only happens if the action of K on H is trivial; in other words, $k(h) = h$ for all h. Since $K \trianglelefteq H \rtimes K$, we observe that (for all $h \in H$)

$$(h, 1) \cdot (1, k) \cdot (h^{-1}, 1) = (h, 1) \cdot (k(h^{-1}), k) = (h(k(h^{-1})), k) = (1, k').$$

So we have that $h(k(h^{-1})) = 1$ and $k = k'$. For the left hand side to be true, we require $k(h^{-1}) = h^{-1}$ for all $h \in H$. Since it's closed under inverses, this is equivalent to $k(h) = h$ for all $h \in H$, so the action is trivial for all $k \in K$. □

Problem 114. If G is simple and A is a set, then any action of G on A is either effective or trivial.

Proof. Recall that being simple means the only normal subgroups are the trivial subgroup and yourself. Let $T : G \to \mathrm{Sym}(A)$. We have that $\ker(T) \leq G$ is a normal subgroup, and so must either be 1 (i.e. the action is effective) or G (i.e. the action is trivial). □

Problem 115. Let P be a Sylow subgroup of G. Show that P is normal if and only if it is the unique Sylow p-subgroup of G.

Proof. We have that G acts by conjugation of the space of cosets of P, and the conjugation of a Sylow subgroup is a Sylow subgroup. The Sylow subgroup is normal iff $gPg^{-1} = P$ for all P, but this is true if and only if it is the unique Sylow p-subgroup. □

Problem 116. Let G and H be groups, $\varphi : G \to H$ be a homomorphism, and let E be a subgroup of H. Prove that $\varphi^{-1}(E)$ is a subgroup of G. If, in addition, $E \trianglelefteq H$, prove that $\varphi^{-1}(E) \trianglelefteq H$.

Proof. To show it's a subgroup, we need to show that $1 \in \varphi^{-1}(E)$ and it's closed under the operation as well as inverses. Since E is a subgroup, $1 \in E$, and φ a homomorphism implies $\varphi(1) = 1$, so $1 \in \varphi^{-1}(E)$. Let $a, b \in \varphi^{-1}(E)$. Then $\varphi(a), \varphi(b) \in E$, so $\varphi(a)\varphi(b) = \varphi(ab) \in E$, hence $ab \in \varphi^{-1}(E)$. If $a \in \varphi^{-1}(E)$, then $\varphi(a)^{-1} \in E$, so $\varphi(a^{-1}) \in E$, and thus $a^{-1} \in \varphi^{-1}(E)$.

Normality is a similar kind of argument. □

Problem 117. Let G be a finite group which acts transitively on a set S with $|S| \geq 2$. Show that there exists an element $g \in G$ which has no fixed points; i.e., for all $s \in S$, $g \cdot s \neq s$.

Proof. We proceed using Burnsides Lemma. Recall that the statement is

$$1 = \frac{1}{|G|} \sum_{g \in G} \chi(g),$$

where

$$\chi(g) = |\{s \in S \ : \ g \cdot s = s\}|.$$

Assume for contradiction that $\chi(g) \geq 1$ for all g. Notice that $\chi(e) \geq 2$, since by definition of a group action we have $e \cdot s = s$ for all $s \in S$. Hence, we get that

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) \geq 1 + \frac{1}{|G|} > 1,$$

a contradiction. □

Problem 118. Let $H, K \subset G$ be subgroups. Then HK is a subgroup iff $HK = KH$.

Proof. ($\implies$) Assume HK is a subgroup. Then we have $KH \subset HK$, since $K \subset HK$ and $H \subset HK$. Take $y^{-1} \in HK$, then $(y^{-1})^{-1} = y \in KH$ for all $y \in HK$, so $HK = KH$.
($\impliedby$) □

Problem 119. Show that any group of order 360 must have a group of order 10.

Proof. Write

$$360 = 3^2 \cdot 2^3 \cdot 5.$$

We see that

$$n_5(G) \equiv 1 \pmod 5,$$

and

$$n_5(G) \mid 3^2 \cdot 2^3.$$

So we have

$$n_5(G) = \{1, 6, 36\}.$$

Cauchy's theorem guarantees there is an element of order 2 in our group. If $n_5(G) = 1$, then we can multiply these two together (since they're both normal) to get a group of order 10. If $n_5 = 36$, take any Sylow 5-subgroup and denote it by P. We have that $[G : N_G(P)] = 36$, and so $N_G(P)$ is a subgroup of order 10. If $n_5 = 6$, look at $[G : N_G(P)] = 6$, so $N_G(P)$ is a subgroup of order 60. Repeat the process within $N_G(P)$; we have that

$$|N_G(P)| = 60 = 3 \cdot 2^2 \cdot 5,$$

and examine n_5 which is the number of Sylow 5 subgroups. We have $n_5 \equiv 1 \pmod 5$, $n_5 \mid 12$, so $n_5 = \{1, 6\}$. If $n_5 = 1$, we're done. Examine the case $n_5 = 6$. Let P' be a Sylow 5 subgroup. Then $[N_G(P) : N_{N_G(P)}(P')] = 6$, so $N_{N_G(P)}(P')$ is a subgroup of order 10. □

Problem 120. The intersection of a set of subrings is a subring.

Proof. Recall that $S \subset R$ is a *subring* if it is an additive subgroup of $(R, +, 0)$ and a multiplicative submonoid of $(R, \cdot, 1)$. Let $\{S_\alpha\}$ be a collection of subrings of R. Recall that the intersection of subgroups is a subgroup, and the intersection of submonoids is a submonoid, so we have

$$\bigcap_\alpha S_\alpha \subset R$$

is an additive subgroup and a multiplicative submonoid, and so a subring. □

Problem 121. Prove that

$$\binom{r}{k} + \binom{r}{k-1} = \binom{r+1}{k}.$$

Proof. We can use a combinatorial argument. Say we have a binary string of length $r + 1$, and say we want to choose binary strings with k 1's. Then we have that this is given by $\binom{r+1}{k}$. Alternatively, we can condition based on what the first bit is. If it is a 1, then we are looking at a binary string of length r, and we need to choose $k - 1$ more 1's; that is, $\binom{r}{k-1}$. However, if we have that the first bit is 0, then we have a string of length r and we need to choose k 1's; that is, $\binom{r}{k}$. Since this exhausts all combinations, we get that

$$\binom{r}{k} + \binom{r}{k-1} = \binom{r+1}{k}.$$

□

Problem 122. Prove the binomial theorem; that is

$$(a+b)^n = \binom{n}{0} a^n + \cdots + \binom{n}{n} b^n.$$

Proof. We go by induction. It holds in the case $n = 1$, clearly. Assume it holds for $n-1$. Then we have

$$(a+b)^{n-1} = \binom{n-1}{0}a^{n-1} + \binom{n-1}{1}a^{n-2}b + \cdots + \binom{n-1}{n-1}b^{n-1}.$$

Hence,

$$(a+b)^n = (a+b)^{n-1}(a+b) = \left(\binom{n-1}{0}a^{n-1} + \binom{n-1}{1}a^{n-2}b + \cdots + \binom{n-1}{n-1}b^{n-1}\right)(a+b).$$

Using distributivity, we get

$$(a+b)^n = \binom{n-1}{0}a^n + \binom{n-1}{1}a^{n-1}b + \cdots + \binom{n-1}{n-1}b^{n-1}a + \binom{n-1}{0}a^{n-1}b + \binom{n-1}{1}a^{n-2}b^2 + \cdots + \binom{n-1}{n-1}b^n.$$

Notice as well we can rewrite this as

$$\binom{n}{0}a^n + \binom{n-1}{1}a^{n-1}b + \cdots + \binom{n-1}{n-1}b^{n-1}a + \binom{n-1}{0}a^{n-1}b + \binom{n-1}{1}a^{n-2}b^2 + \cdots + \binom{n}{n}b^n.$$

Coupling terms, we have

$$\binom{n}{0}a^n + \left(\binom{n-1}{0} + \binom{n-1}{1}\right)a^{n-1}b + \cdots + \left(\binom{n-1}{n-2} + \binom{n-1}{n-1}\right)b^{n-1}a + \binom{n}{n}b^n.$$

Using the prior problem, this gives

$$\binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}b^{n-1}a + \binom{n}{n}b^n = (a+b)^n.$$

Thus, it holds for n, and so we have it holds by induction. □

Problem 123 (Section 2.1, Exercise 1)**.** Let C be the set of real-valued continuous functions on the real line $\mathbb{R}$. Show that C with the usual addition of functions and 0 is an abelian group, and that C with composition as the product and 1 the identity map is a monoid. Is C with these compositions and 0 and 1 a ring?

Proof. We first remark that, under pointwise addition, a collection of functions inherit the familiar properties of the codomain. So in this case, we see that 0 is continuous, and we have $(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x)$ for all $x \in \mathbb{R}$, $-f$ is continuous, $(f+(g+h))(x) = f(x) + (g+h)(x) = f(x) + g(x) + h(x) = (f+g)(x) + h(x) = ((f+g)+h)(x)$, and $f+g$ is continuous for all $f, g, h \in C$. Hence, it's an abelian group under addition. Clearly, under composition, we get a multiplicative monoid.

To see that it's a ring, we need to show that the distributive properties are satisfied. That is,

$$((f+g)\circ h)(x) = f(h(x)) + g(h(x)).$$

To see this, note

$$((f+g)\circ h)(x) = (f+g)(h(x)) = f(h(x)) + g(h(x)).$$

Next, we want

$$(f\circ(g+h))(x) = f(g(x)) + f(h(x)).$$

We have

$$(f\circ(g+h))(x) = f((g+h)(x)) = f(g(x) + h(x)).$$

However, it's not necessarily true that $f(g(x)+h(x)) = f(g(x)) + f(h(x))$. So we see this is not a ring. □

Problem 124 (Section 2.1, Exercise 2)**.** Show that in a ring R, $a(b-c) = ab - ac$ where $b - c \equiv b + (-c)$ and $n(ab) = (na)b = a(nb)$ if $n \in \mathbb{Z}$.

Proof. Let R be our ring. For the first part, we can rewrite the inside as

$$a(b-c) = a(b+(-c)).$$

The distributive laws then give

$$a(b+(-c)) = ab + a(-c).$$

Thus, it suffices to show that

$$a(-c) = (-a)c = -(ac).$$

We have

$$a(-c) + ac = a((-c)+c) = a(0) = 0,$$

so $a(-c) = -(ac)$. Likewise,

$$(-a)c + ac = ((-a)+a)c = (0)c = 0,$$

so $(-a)c = -(ac)$. Hence, we can write

$$a(b-c) = ab - ac,$$

as desired.

For the second part, we have

$$n(ab) = ab + ab + \cdots + ab$$

n times. Notice we can pull out the a by distributivity to get

$$ab + ab + \cdots + ab = a(b + b + \cdots + b) = a(nb).$$

Likewise, we can pull out the b to get

$$ab + ab + \cdots + ab = (a + a + \cdots + a)b = (na)b.$$

Hence, we have $n(ab) = (na)b = a(nb)$ for any $n \in \mathbb{Z}_{>0}$ (it's clear for $n = 0$). To get the same result for $n \in \mathbb{Z}_{<0}$, let $k = |n|$. We remark that

$$n(ab) = -ab - ab - \cdots - ab$$

k times, and we get (by prior work)

$$a(-b - b - \cdots - b) = a(-kb) = a(nb),$$

and a similar argument applies throughout. □

Problem 125 (Section 2.1, Exercise 3)**.** Show that if all the axioms for a ring except commutativity of addition are assumed, then commutativity follows, and hence we have a ring.

Proof. We use distributivity to get

$$(1+1)(a+b) = (1+1)a + (1+1)b = 2a + 2b,$$

and likewise

$$(1+1)(a+b) = a + b + a + b.$$

So we have

$$a + a + b + b = a + b + a + b \leftrightarrow a + b = b + a.$$

□

Problem 126. A subring of a domain is a domain.

Proof. Recall that a subring is a *domain*[1] if $R^\times = \{x \in R \ : \ x \neq 0\}$ forms a submonoid of R. Let $S \subset R$ be a subring. Then we have $(S, \cdot, 1)$ is a submonoid of $(R, \cdot, 1)$. Hence, $S^\times = R^\times \cap (S, \cdot, 1) = \{x \in S \ : \ x \neq 0\}$ is the intersection of two submonoids, and so a submonoid, and so S is a domain. □

[1]Also referred to as integral domain.

Remark. The property of being a domain means that there are no zero-divisors (assuming $R \neq 0$), since $R^\times$ being a submonoid means that it's closed under multiplication.

Problem 127. A ring $R \neq 0$ is a domain implies that it satisfies the cancellative law; that is, $a \neq 0$, $ab = ac$ implies $b = c$.

Proof. We have

$$ab = ac \iff a(b-c) = 0.$$

Since we are in a domain, we must have that either $a = 0$ or $b - c = 0$. By assumption, $a \neq 0$, so this forces $b - c = 0$, or $b = c$. □

Problem 128. A non-zero division ring satisfies the property that, for any $a \neq 0$, there exists a b such that $ab = 1 = ba$.

Proof. Recall that a *division ring* is a ring such that $R^\times$ is a subgroup of $(R, \cdot, 1)$. So since $a \neq 0$, we have that $a \in R^\times$, and since it's a subgroup we have that there must be an inverse; that is, an element $b \in R^\times$ such that $ab = ba = 1$. □

Problem 129. The set of units $U = \{x \in R \ : \ \exists y \in R, xy = yx = 1\}$ is a subgroup of $(R, \cdot, 1)$.

Proof. Let's first show that U is closed under multiplication. Let $a, b \in U$. Then we have $ab \in U$, since $(ab)^{-1} = b^{-1}a^{-1}$ is such that

$$(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab).$$

Next, we need to show that it's associative. This, however, is inherited from $(R, \cdot, 1)$. It's clear that it's closed under inverses. Finally, it's clear that $1 \in U$ as well. Hence, it's a subgroup. □

Remark. The group of units of $\mathbb{Z}$ is $\{-1, 1\}$.

Problem 130. A ring $R \neq 0$ is a domain if and only if the cancellation laws hold; that is, $a \neq 0$ and $ab = ac$ implies $b = c$ and vice versa.

Proof. ($\implies$) Let $R \neq 0$ be a domain. Then this means that $R^\times = \{r \ : \ r \neq 0, r \in R\}$ is a submonoid of $(R, \cdot, 1)$. We then wish to show that $ab = ac$ implies $b = c$ for $a \neq 0$. Notice that

$$ab = ac \leftrightarrow ab - ac = 0 \leftrightarrow a(b-c) = 0$$

using the fact that we have distributivity. Now, if $b - c \neq 0$, this implies that we have that $R^\times$ is not a submonoid, since it's not closed. Hence, we must have $b - c = 0$, or $b = c$. The same goes in the other direction.

($\impliedby$) Assume the cancellation law holds and $R \neq 0$. We wish to show that $R^\times$ is a submonoid. That is, $a, b \in R^\times$ implies $ab \in R^\times$. Assume otherwise; that is, we have a $a, b \in R^\times$ such that $ab = 0$. Notice that $a0 = 0$, so we have $ab = a0$, and the cancellation law tells us that $b = 0$, but this contradicts the fact that $b \in R^\times$. Hence, we must have that $ab \neq 0$, and so $ab \in R^\times$, so R is a domain. □

Problem 131 (Section 2.2, Exercise 2)**.** Show that a domain contains no idempotents ($e^2 = e$) except $e = 0$ and $e = 1$. An element z is called nilpotent if $z^n = 0$ for some $n \in \mathbb{Z}^+$. Show that 0 is the only nilpotent in a domain.

Proof. We first show the idempotent part. Assume we have $e^2 = e$, then this implies that $e^2 - e = 0$. Using the distributivity, we have $e(e-1) = 0$. Since we are in a domain, either $e = 0$ or $e - 1 = 0$, which forces either $e = 0$ or $e = 1$.

Let n be the smallest positive integer such that $z^n = 0$. We have that $z^n = z^{n-1}z = 0$. Since we are in a domain, this forces either $z^{n-1} = 0$ or $z = 0$. Since n is the smallest positive integer such that $z^n = 0$, this forces $z = 0$. Thus, 0 is the only nilpotent in a domain. □

Problem 132 (Section 2.2, Exercise 3)**.** Let z be an element of a ring for which there exists a $w \neq 0$ such that $zwz = 0$. Show that z is either a left or a right zero divisor.

Proof. If $z = 0$, then we clearly have that $zwz = 0$ for any $w \neq 0$ and z is both a left and right zero divisor, and so we are done. Assume $z \neq 0$. Then associativity of multiplication gives

$$zwz = z(wz) = (zw)z = 0.$$

Examine $z(wz) = 0$. If $wz = 0$, then this implies that z is a right zero divisor, and so we are done. Otherwise, we have $wz \neq 0$, and $z(wz) = 0$, so z is a left zero divisor. Thus, z must be either a left or right zero divisor. □

Problem 133 (Section 2.2, Exercise 4)**.** Show that if $1 - ab$ is invertible, then so is $1 - ba$.

Proof. Let c be such that

$$c(1 - ab) = 1.$$

Then we have

$$bca(1 - ba) = bca - bcaba = (bc - bcab)a = b(c - cab)a = bc(1 - ab)a = ba.$$

So we see that

$$(1 + bca)(1 - ba) = (1 - ba) + ba = 1,$$

and so we have an inverse. So $1 - ba$ is invertible. □

Problem 134 (Section 2.2, Exercise 5)**.** We first recall **Example 8** from **Section 2.1**. Let Γ be the set of real-valued continuous functions on the interval $[0, 1]$, where we define $f + g$ and fg as usual by $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. Let 0 and 1 be the constant functions 0 and 1 respectively. Then $(\Gamma, +, \cdot, 0, 1)$ is a ring.

Show that a function f in this example is a zero divisor if and only if the set of points x where $f(x) = 0$ contains an open interval. What are the idempotents of this ring? The nilpotents? The units?

Proof. We break this up into four parts. Throughout, $\{f = a\}$ denotes $\{x \in [0, 1] \ : \ f(x) = a\}$.

(a) We show that f is a zero divisor if and only if the set of points x where $f(x) = 0$ contains an open interval.
($\implies$) Assume f is a zero divisor, then we have there is a $g \in \Gamma$ non-zero such that $fg = 0$. Since $g \neq 0$ and g continuous, we must have that $g \neq 0$ contains some interval. Hence, $f = 0$ contains some interval.
($\impliedby$) Assume $f(x) = 0$ contains an open interval. That is, $(a, b) \subset \{f \neq 0\}$. Define $g = 0$ on $(a, b)^c$, and $g > 0$ on (a, b). Then we have that $fg = 0$, and so f is a zero-divisor.

(b) We now want to figure out what the idempotents are in the ring. That is, the functions $f \in \Gamma$ such that $f^2 = f$. Recall that this means that $f^2(x) = f(x)$ for all $x \in \mathbb{R}$. The structure depends on $\mathbb{R}$, and so from prior we know that the only idempotents are $f = 1, 0$.

(c) We now want to figure out the nilpotents. That is, the functions where $f^n = 0$, $n \in \mathbb{Z}^+$. Again, the structure depends on $\mathbb{R}$, so we are forced to have 0 as our only nilpotent.

(d) Finally, we want to figure out the units. If $f(x) = 0$, we see that there is no $g \in \Gamma$ such that $g(x)f(x) = 1$. So we are forced to have $\{f = 0\} = \varnothing$. Notice that this is a necessary and sufficient condition.

□

Problem 135 (Section 2.2, Exercise 6)**.** Let u be an element of a ring that has a right inverse. Prove that the following conditions on u are equivalent:

(1) u has more than one right inverse;
(2) u is not a unit;

(3) u is a left 0 divisor.

Proof. (1) $\implies$ (2): Assume that u has more than one right inverse. Let a, b be distinct right inverses for u. Then we wish to show that u has no left inverses. Assume for contradiction that g is a left inverse for u. Then we have

$$ua = ub \leftrightarrow gua = gub \leftrightarrow a = b,$$

but this contradicts our choice of a and b. Hence, there is no left inverse.
(2) $\implies$ (3): We go by contrapositive; that is, if u is not a left 0 divisor, then u is a unit. We have that u is not a left 0 divisor implies that $ug \neq 0$ for all g in the ring non-zero. We wish to show that u has a left inverse. Let a be the right inverse. To do so, we notice that

$$u = (ua)u = u(au),$$

and so subtracting from both sides we have

$$u(1 - au) = 0.$$

Since u is not a left 0 divisor, we must have $1 - au = 0$, or $1 = au$. Thus, we have a is the left inverse of u as well, and so u is a unit.
(3) $\implies$ (1): We assume that u is a left 0 divisor and we want to show that u has more than one right inverse. We have $g \neq 0$ in the ring such that $ug = 0$. Let a be the right inverse of u. Notice that

$$ua + ug = 1 + 0 = 1,$$

and factoring gives us $u(a + g) = 1$. Notice as well that $a + g \neq a$, since we have that $g \neq 0$, and so we have more than one right inverse. □

Problem 136 (Section 2.2, Exercise 7)**.** Prove that if an element of a ring has more than one right inverse, then it has infinitely many.

Proof. From prior, we've shown that multiple right inverses implies that it has a right zero divisor. Let a be a right inverse of u. Let $S = \{g \in R \ : \ ug = 0, g \neq 0\}$. We wish to show that $|S| = \infty$. Let $f : S \to S$ be defined by $f(g) = gu$. Then we see that f is injective, since it admits a right inverse. Therefore, we have that f is surjective if we assume $|S| < \infty$. But f surjective implies that for all $t \in S$, there is an $x \in S$ such that $xu = t$. Notice that this implies that there is some $y \in S$ such that $f(y) = tu - 1$, since $u(tu - 1) = (ut)u - u = 0$. That is, we have a solution to $yu = tu - 1$. But multiplying on the right by t, we have $yut = y = tut - t = 0$, which contradicts our set. So f cannot be surjective, but this contradicts the fact that $|S| < \infty$. Thus, we must have $|S| = \infty$.

Let $g \in S$. Then we have that

$$u(a + g) = ua + ug = ua = 1.$$

Since $|S| = \infty$, we have that there are infinitely many right inverses. □

Problem 137 (Section 2.2, Exercise 8)**.** Show that an element u of a ring is a unit with $v = u^{-1}$ if and only if either of the following conditions holds:
(1) $uvu = u$, $vu^2v = 1$,
(2) $uvu = u$ and v is the only element satisfying this.

Proof. (1) ($\implies$) if $v = u^{-1}$, then we have $uvu = u$, and $vu^2v = (vu)(uv) = (1)(1) = 1$.

($\impliedby$) Multiplying u on the right, we have

$$(uvu)uv = u \leftrightarrow u^2v = u.$$

Multiplying by v on the left gives

$$vu^2v = 1 = vu.$$

Hence, v is a left inverse for u. Multiplying u now on the right gives

$$vu^2vu = u \leftrightarrow vu^2 = u,$$

and multiplying v on the right gives

$$vu^2v = 1 = uv.$$

Hence, $v = u^{-1}$.

(2) ($\implies$) This is clear.
($\impliedby$) We examine the contrapositive; if u is not a unit, then $uvu \neq u$ or v is not the only element satisfying this. By an earlier problem, if u is not a unit, it admits multiple right inverses. So, we either have v is a right inverse, in which case it's not unique, or v is not a right inverse, in which case $uvu \neq u$.

□

Problem 138 (Section 2.2, Exercise 9)**.** Let a and b be elements of a ring such that a, b and $ab-1$ are units. Show that $a - b^{-1}$ and $(a - b^{-1})^{-1} - a^{-1}$ are units and the following identity holds:

$$((a - b^{-1})^{-1} - a^{-1})^{-1} = aba - a.$$

Proof. Notice that

$$(a - b^{-1})b = ab - 1,$$

which is a unit. Hence, we have

$$(a - b^{-1})(bc) = 1.$$

So it has a right inverse. Notice as well

$$\begin{aligned}(bc)(a - b^{-1}) &= bca - bcb^{-1} = bc(ab - 1)b^{-1} - a^{-1}(ab - 1)cb^{-1} + bcb^{-1} - a^{-1}cb^{-1} \\ &= 1 - a^{-1}b^{-1} + bcb^{-1} - a^{-1}cb^{-1} = 1 - a^{-1}b^{-1} + (b - a^{-1})cb^{-1} \\ &= 1 - a^{-1}b^{-1} + a^{-1}(ab - 1)cb^{-1} = 1 - a^{-1}b^{-1} + a^{-1}b^{-1} = 1.\end{aligned}$$

So this is a left inverse.

Next, we need to show that $(a - b^{-1})^{-1} - a^{-1} = bc - a^{-1}$ is a unit. Notice that this corresponds to

$$bc - a^{-1} = (b - a^{-1}c^{-1})c = (b - a^{-1}(ab - 1))c = (b - b + a^{-1})c = a^{-1}c.$$

So the inverse is $(ab - 1)a = aba - a$. Hence, it's a unit with corresponding inverse. □

Problem 139. Show that the matrix

$$\begin{pmatrix} 1 & 4 & 1 \\ 0 & 1 & -1 \\ -3 & -6 & -8 \end{pmatrix}$$

is invertible in $M_3(\mathbb{Z})$ and find its inverse.

Proof. Recall **Theorem 2.1**, which says that in a commutative ring R, a matrix is invertible if and only if it's determinant is invertible. Hence, we find the determinant of this matrix; going through the calculations, we see that it has determinant 1. Furthermore, this tells us that the adjoint is the inverse, and so we just need to find it. We have

$$\begin{aligned}A_{11} &:= -14 \\ A_{12} &:= 3 \\ A_{13} &:= 3 \\ A_{21} &:= 26 \\ A_{22} &:= -5 \\ A_{23} &:= -6\end{aligned}$$

$$A_{31} := -5$$
$$A_{32} := 1$$
$$A_{33} := 1,$$

so the adjoint is

$$\mathrm{Adj}(A) := \begin{pmatrix} -14 & 26 & -5 \\ 3 & -5 & 1 \\ 3 & -6 & 1 \end{pmatrix}.$$

□

Problem 140 (Section 2.3, Exercise 2)**.** Prove that if R is a commutative ring, then $AB = 1$ in $M_n(R)$ implies $BA = 1$.

Proof. Follows from the fact that $\det(AB) = \det(A)\det(B)$ and **Theorem 2.1**. □

Problem 141 (Section 2.3, Exercise 3)**.** Verify that for any $p \in R$ and $i \neq j$, $1 + pe_{ij}$ is invertible in $M_n(R)$ with inverse $1 - pe_{ij}$ (here, we have e_{ij} corresponds to looking at the matrix with zeroes at all but the (i, j) entry, where it has a 1). More generally, show that if z is a nilpotent element of a ring (that is, $z^n = 0$ for some positive integer n), then $1 - z$ is invertible. Also determine its inverse.

Proof. Notice that $e_{ij}^2 = 0$, and so we have

$$(1 + pe_{ij})(1 - pe_{ij}) = 1 - pe_{ij} + pe_{ij} - p^2 e_{ij}^2 = 1.$$

In general, let z be nilpotent such that $z^n = 0$. Then we have $1 - z$ is invertible, with inverse $(1 + z + z^2 + \cdots + z^{n-1})$. For the case $n = 3$, we have

$$(1 - z)(1 + z + z^2) = 1 + z + z^2 - z - z^2 - z^3 = 1.$$

In general, we get

$$(1 - z)(1 + z + \cdots + z^{n-1}) = 1 + z + \cdots + z^{n-1} - z - z^2 - \cdots - z^{n-1} - z^n = 1.$$

□

Problem 142 (Section 2.3, Exercise 4)**.** Show that $\mathrm{diag}(a_1, \ldots, a_n)$ is invertible in $M_n(R)$ if and only if every a_i is invertible in R. What is the inverse?

Proof. The solution is clear after noticing that diagonal matrices multiply element wise. That is,

$$\begin{pmatrix} a_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n \end{pmatrix} \begin{pmatrix} b_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & b_n \end{pmatrix} = \begin{pmatrix} a_1 b_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_n b_n \end{pmatrix}$$

□

Problem 143 (Section 2.3, Exercise 5)**.** Verify that for $a, b \in \mathbb{R}$, $a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is an isomorphism of $\mathbb{C}$ with a subring of $M_2(\mathbb{R})$.

Proof. We show that it's an injective homomorphism, and so an isomorphism onto it's image. Letting ϕ denote the map, we first note it's well-defined and injective clearly. To see it's a homomorphism, we have

$$\phi((a + bi) + (c + di)) = \phi((a + c) + (b + d)i) = \begin{pmatrix} a + c & b + d \\ -b - d & a + c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$
$$= \phi(a + bi) + \phi(c + di),$$

$$\phi(0) = 0,$$
$$\phi((a+bi)(c+di)) = \phi((ac-bd)+(ad+bc)i) = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$
$$= \phi(a+bi)\phi(c+di),$$
$$\phi(1) = 1.$$

So we have its an isomorphism onto its image, which is a subring of $M_2(\mathbb{R})$. □

Problem 144 (Section 2.3, Exercise 6)**.** Show that in any ring the set $C(S)$ of elements which commute with every element of a given subset S constitute a subring. If S is taken to be the whole ring, then $C = C(S)$ is called the center of the ring. Note that this subring is commutative. Determine $C(S)$ in $M_n(R)$ for $S = \{e_{ij} \ : \ i, j = 1, \ldots, n\}$. Also determine the center of $M_n(R)$.

Proof. Let $S \subset R$ be a subset, $C(S) = \{x \in R \ : \ xy = yx \text{ for all } y \in S\}$. We wish to show that this is a subring. That is, it's a subgroup under addition and a submonoid under multiplication. First, we show that it's closed under addition. Notice that, for $a, b \in C(S)$, $y \in S$, we have $(a+b)y = ay + by = ya + yb = y(a+b)$, so $a + b \in C(S)$. It's clearly associative. Next, $0 \in C(S)$, since $0y = 0 = y0$. Finally, if $a \in C(S)$, we have $-a \in C(S)$, since $(-a)y = -ay = -ya = y(-a)$. So it's a subgroup.

Next, we check it's a monoid. If $a, b \in C(S)$, $y \in S$, we have $y(ab) = (ya)b = (ay)b = a(yb) = a(by) = (ab)y$. So $ab \in C(S)$, and it's closed under multiplication. Associativeness holds clearly. Finally, $1 \in C(S)$, since $1y = y = y1$. So it's a submonoid. Hence, it's a subring. Clearly, this is going to be commutative.

Let $A \in M_n(R)$. For $A \in C(S)$, we need $Ae_{ij} = e_{ij}A$ for all i, j. Notice this can only happen in the case of $A = 0$. □

Problem 145 (Section 2.3, Exercise 8)**.** Show that if R is commutative and D is the set of diagonal matrices in $M_n(R)$, then $C(D) = D$.

Proof. Follows from the solution of exercise 4. □

Problem 146 (Section 2.3, Exercise 10)**.** Let R be a ring, R' a set, η a bijective map of R' onto R. Show that R' becomes a ring if one defines:

$$a' + b' = \eta^{-1}(\eta(a') + \eta(b')),$$
$$a'b' = \eta^{-1}(\eta(a')\eta(b')),$$
$$0' = \eta^{-1}(0),$$
$$1' = \eta^{-1}(1),$$

and that η is an isomorphism of R' with R. Use this to prove that if u is an invertible element of a ring, then $(R, +, \cdot u, 0, u^{-1}$

Proof. To see that R' is a ring, we need to check that it's an additive group under addition, multiplicative monoid under multiplication, and it satisfies distributivity. We first check its an additive group. First, it's closed, since $a' + b' \in R'$ for all $a', b' \in R'$. Next, we see that it's associative, since

$$a' + (b' + c') = a' + \eta^{-1}(\eta(b') + \eta(c')) = \eta^{-1}(\eta(a') + \eta^{-1}(\eta(b') + \eta(c')))$$

□

Problem 147 (Section 2.4, Exercise 1)**.** Define $\overline{x} = a_0 - a_1 i - a_2 j - a_3 k$ for $x = a_0 + a_1 i + a_2 j + a_3 k$. Show that

$$\overline{x + y} = \overline{x} + \overline{y},$$
$$\overline{xy} = \overline{x}\,\overline{y}.$$

Proof. We have

$$x = a_0 + a_1 i + a_2 j + a_3 k,$$
$$y = b_0 + b_1 i + b_2 j + b_3 k.$$

Hence

$$x + y = (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k,$$

$\overline{x+y} = (a_0+b_0)-(a_1+b_1)i-(a_2+b_2)j-(a_3+b_3)k = a_0-a_1i-a_2j-a_3k+b_0-b_1i-b_2j-b_3k = \overline{x}+\overline{y}$.
Same idea for $\overline{xy}$. □

Problem 148. Show that $x\overline{x} = N(x)$, where $N(x) = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Define $T(x) = 2a_0$. Show that x satisfies the quadratic equation $x^2 - T(x)x + N(x) = 0$.

Proof. We have

$$x\overline{x} = (a_0+a_1i+a_2j+a_3k)(a_0-a_1i-a_2j-a_3k) = a_0^2-a_0a_1i-a_0a_2j-a_0a_3k+a_0a_1i+a_1^2+a_1a_2k-a_1a_3ik$$
$$+a_0a_2j - a_2a_1ji + a_2^2 - a_2a_3jk + a_0a_3k - a_3a_1ki - a_3a_2kj + a_3^2.$$

Using the identities,

$$ij = k,\ ji = -k,\ jk = i,\ kj = -i,\ ki = j,\ ik = -j,$$

things cancel appropriately to get $a_0^2 + a_1^2 + a_2^2 + a_3^2$. Expanding things out in the quadratic gives the same result. □

Problem 149. Prove that $N(xy) = N(x)N(y)$.

Proof. We have

$$x = a_0 + a_1 i + a_2 j + a_3 k,$$
$$y = b_0 + b_1 i + b_2 j + b_3 k,$$

$$xy = (a_0+a_1i+a_2j+a_3k)(b_0+b_1i+b_2j+b_3k) = (a_0b_0+a_0b_1i+a_0b_2j+a_0b_3k)+(b_0a_1i-a_1b_1+a_1b_2k$$
$$-a_1b_3j) + (b_0a_2j - a_2b_1k - a_2b_2 + a_2b_3i) + (a_3b_0k + a_3b_1j - a_3b_2i - a_3b_3)$$
$$= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) + (a_0b_1 + b_0a_1 + a_2b_3 - a_3b_2)i + (a_0b_2 + b_0a_2 + a_3b_1 - a_1b_3)j$$
$$+(a_0b_3 + a_1b_2 + a_3b_0 - a_2b_1)k$$

and so

$$N(xy) = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3)^2 + (a_0b_1 + b_0a_1 + a_2b_3 - a_3b_2)^2 + (a_0b_2 + b_0a_2 + a_3b_1 - a_1b_3)^2$$
$$+(a_0b_3 + a_1b_2 + a_3b_0 - a_2b_1)^2$$
$$= a_0^2b_0^2 + a_0^2b_1^2 + a_0^2b_2^2 + a_0^2b_3^2 + a_1^2b_0^2 + a_1^2b_1^2 + \cdots + a_3^2b_3^2 = (a_0^2 + a_1^2 + a_2^2 + a_3^2)(b_0^2 + b_1^2 + b_2^2 + b_3^2).$$

□

Problem 150. Is $IJ \subset I \cap J$? Does $IJ = I \cap J$ if they are coprime?

Proof. Notice that $I \cap J$ is an ideal, and so it's closed under addition as well. Notice that elements in IJ are of the form $a_0b_0 + \cdots + a_nb_n$, $a_i \in I$, $b_i \in J$. Hence, since we're in an ideal, $a_ib_i \in I$ and $a_ib_i \in J$, so $a_ib_i \in I \cap J$. Closure under addition gives us all elements of this form are in $I \cap J$, and so $IJ \subset I \cap J$.

We then wish to determine when $I \cap J = IJ$. Recall that two ideals are coprime when $I + J = R$, R the ambient ring. Notice that

$$I \cap J \subset R(I \cap J) = (I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subset IJ + IJ = IJ.$$

□

Problem 151. The intersection of ideals is an ideal.

Proof. The intersection of additive subgroups is an additive subgroup. Next, let $\{I_\alpha\}$ be a collection of ideals. Let $a \in R$. We have

$$a\left(\bigcap_\alpha I_\alpha\right) \in I_\alpha$$

for all α, and so its in the intersection. Hence, it's an ideal. □

Problem 152. Every finite division ring is commutative.

Proof. We need to show that $ab = ba$. □

Problem 153 (Section 2.5, Exercise 1)**.** Let Γ be the ring of real-valued continuous functions on $[0, 1]$. Let S be a subset of $[0, 1]$, and let $Z_S = \{f \ : \ f(x) = 0, x \in S\}$. Verify that Z_S is an ideal. Let $S_1 = [0, 1/2]$, $S_2 = [1/2, 1]$, $I_1 = Z_{S_1}$, $I_2 = Z_{S_2}$. Show that $I_1 I_2 = I_1 \cap I_2 = 0$.

Proof. We first show it's an ideal. First, we establish it's an additive subgroup. Let $f, g \in Z_S$. Then we have that, for all $x \in S$, $(f + g)(x) = f(x) + g(x) = 0$, so $f + g \in Z_S$. Likewise, if $f \in Z_S$, then $-f(x) = -0 = 0$, so $-f \in Z_S$. So it's an additive subgroup. Next, let $g \in Z_S$, $f \in \Gamma$. We have that $(fg)(x) = f(x)g(x) = 0 = g(x)f(x) = (gf)(x)$, so $fg \in Z_S$. Hence, it's an ideal.

$0 \subset I_1 I_2 \subset I_1 \cap I_2$, and the only function which is 0 on S_1 and S_2 is 0, so $I_1 \cap I_2 = 0$. □

Problem 154 (Section 2.5, Exercise 2)**.** Show that the associative law holds for products of ideals:

$$I(JK) = (IJ)K,$$

where I, J, K are ideals.

Proof. Notice that

$$JK = \{b_1c_1 + \cdots + b_mc_m \ : \ b_i \in J, c_i \in K, m \in \mathbb{Z}^+\},$$

and

$$I(JK)$$

$$= \{a_1(b_{1,n}c_{1,n}+\cdots+b_{1,m}c_{1,m})+\cdots+a_n(b_{n,1}c_{n,1}+\cdots+b_{n,m}c_{n,m}) \ : \ a_i \in I, b_i \in J, c_i \in K, n, (i, m) \in \mathbb{Z}^+\} \subset (IJ)K,$$

and likewise for the other direction through expansion. □

Problem 155 (Section 2.5, Exercise 3)**.** Does the distributive law $I(J + K) = IJ + IK$ hold?

Proof. We have

$$I(J + K) = \{a_1(b_1 + c_1) + \cdots + a_m(b_m + c_m) \ : \ a_i \in I, b_i \in J, c_i \in K, m \in \mathbb{Z}^+\}$$

$$= \{(a_1b_1 + \cdots + a_mb_m) + (a_1c_1 + \cdots + a_mc_m) \ : \ a_i \in I, b_i \in J, c_i \in K, m \in \mathbb{Z}^+\} \subset IJ + IK.$$

Likewise, we see $IJ \subset I(J + K)$, $IK \subset I(J + K)$, so $IJ + IK \subset I(J + K)$. Hence, we have equality. □

Problem 156 (Section 2.5, Exercise 4)**.** If R is a ring, we define a right (left) ideal in R to be a subgroup of the additive group of R such that $ba \in I$ ($ab \in I$) for every $a \in R$, $b \in I$. Verify that the subset of matrices of the form

$$\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}$$

is a right ideal, and the subset of the form

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$$

is a left ideal in $M_2(R)$ for any R. Are either of these sets ideals?

Proof. First, it's clear to note that both of these are closed as additive subgroups. Next, take an arbitrary matrix in $M_2(R)$. We have that

$$\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ ae+bg & af+bh \end{pmatrix}$$

which is still in the ideal. The same idea holds for the other set.

Notice that

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} = \begin{pmatrix} fa & fb \\ ha & hb \end{pmatrix}$$

which is not in the set, and so this is not an ideal. The same idea holds for the other set. □

Problem 157 (Section 2.5, Exercise 5)**.** Prove the following extension of Theorem 2.2: A ring $R \neq 0$ is a division ring iff 0 and R are the only left (right) ideals in R.

Proof. ($\implies$) If R is a division ring, then every element $r \in R$ has an inverse. Hence, if I is an ideal which is non-zero, we have that, for $i \in I$ non-zero, $ii^{-1} = 1 \in I$. If $1 \in I$, we have that $I = R$. So the only non-zero right ideal is R (respectively same for left).
($\impliedby$) Let $a \in R$ non-zero, and examine Ra; that is, the ideal generated by a. Since this is non-zero, we must have that $Ra = R$, which implies that there is some $b \in R$ such that $ba = 1$. Likewise, we see that

$$a = a(ba) = (ab)a,$$

and so we have

$$a - (ab)a = a(1 - ab) = 0,$$

since a is non-zero, this tells us that $1 = ab$. So, a is invertible. Since the choice of a is arbitrary, we get that R is a division ring. □

Problem 158 (Section 2.5, Exercise 6)**.** Let R be a commutative ring and let N denote the set of nilpotent elements of R. Show that N is an ideal and R/N contains no non-zero nilpotent elements.

Proof. **Step 1:** We show that N is an ideal. To be an ideal, we need to be a subgroup of $(R, +, 0)$, and we need to satisfy the property that, for all $r \in R$, $rN \subset N$. First, notice that $0 \in N$ clearly. Next, let $a, b \in N$. Then we have $a^n = 0$, $b^m = 0$ for some $n, m \in \mathbb{Z}^+$. Notice that

$$(a+b)^{nm} = \sum_{k=0}^{nm} \binom{nm}{k} a^k b^{nm-k}.$$

If $k < n$, we have $nm - k > nm - n = n(m-1) > m$, and so $b^{nm-k} = 0$. If $k \geq n$, we have $a^n = 0$. Hence, $(a+b)^{nm} = 0$, and so $a + b \in N$. If $a \in N$, then we notice as well that $(-a) \in N$, since $(-a)^n = (-1)^n a^n = 0$. So we have that N is a subgroup.

Take $r \in R$, $a \in N$. Then we have that $(ar)^n = a^n r^n$, since it's a commutative ring, and so $(ar)^n = 0$. Hence, $ar \in N$ for all $r \in R$, $a \in N$, and so it is an ideal.
Step 2: Take $a \in R$, and let $\overline{a} \in R/N$ be it's canonical image. If $\overline{a}$ is nilpotent, we have that there is n such that $a^n \in N$. But $a^n \in N$ implies that $a \in N$, and so the only nilpotent element in R/N is 0. □

Problem 159 (Section 2.5, Exercise 8)**.** Let I be an ideal in R and let $M_n(I)$ denote the set of $n \times n$ matrices with entries in I. Show that $M_n(I)$ is an ideal in $M_n(R)$. Prove that every ideal in $M_n(R)$ has the form $M_n(I)$ for some ideal I of R, and that $I \mapsto M_n(I)$ is a bijective map of the set of ideals of R onto the set of ideals of $M_n(R)$.

Sketch of solution. We first show that $M_n(I)$ is an ideal of $M_n(R)$. Matrix multiplication gives us that for $A \in M_n(R)$, $A = (a_{ij})$, $B \in M_n(I)$, $B = (b_{ij})$, we have

$$c_{jk} = \sum_{i=1}^{n} a_{ji} b_{ik}.$$

Since I is an ideal, this is in I, so the product is in $M_n(I)$. Same idea for other direction. It's also clearly an additive subgroup, and so we have that this is an ideal.

Let $I \subset M_n(R)$ be an ideal. Define J to be the set of elements which are in some component of some matrix in I. This is an additive subgroup, then, and furthermore we get its an ideal, since $bJ \in J$ for all $b \in R$. Hence, it's an ideal, and so we get our bijection. □

Problem 160 (Section 2.6, Exercise 1)**.** Write down addition and multiplication tables for $\mathbb{Z}/(5)$ and $\mathbb{Z}/(6)$.

Proof. I'll do $\mathbb{Z}/(5)$ first. We have

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The ideals for this ring are (1) and (0).
Next, for $\mathbb{Z}/(6)$, we have

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The ideals in this ring are (0), (1), (2), (3). (2) and (3) are both prime and maximal.

□

Problem 161 (Section 2.6, Exercise 2)**.** Show that $\mathbb{Z}/(k)$ contains non-zero nilpotent elements if and only if k is divisible by the square of a prime. Determine the nilpotent elements of $\mathbb{Z}/(180)$.

Proof. ($\implies$) Let $k = p_1^{e_1} \cdots p_n^{e_n}$. By assumption, we have that there is an i such that $e_i \geq 2$. Let $t = \max\{e_1, \ldots, e_n\}$. We notice that $p_1 \cdots p_n \in \mathbb{Z}/(k)$ is such that it is not zero. Furthermore, we see that

$$(p_1 \cdots p_n)^t \equiv 0 \pmod{k}.$$

Hence, we have that there is a non-zero nilpotent element.
($\impliedby$) Let $a \in \mathbb{Z}/(k)$ be such that $a^t = 0$ for some $t > 1$. Let $p_1^{e_1} \cdots p_n^{e_n} = a$, where $e_i \geq 1$. Then this implies that

$$(p_1^{e_1} \cdots p_n^{e_n})^t \equiv 0 \pmod{k}.$$

Sine $t > 1$, we have that $p_i^2 \mid k$ for all $1 \leq i \leq n$. Hence, there is at least one prime whose square divides k.

We write

$$2^2 \cdot 3^2 \cdot 5 = 180.$$

We can get all of the nilpotent elements by taking different combinations of powers of these primes. That is, all the multiples of $2 \cdot 3 \cdot 5 = 30$ are nilpotent elements. So the list is $30, 60, 90, 120, 150$. □

Problem 162 (Section 2.6, Exercise 3)**.** Prove that if D is a finite division ring, then $a^{|D|} = a$ for every $a \in D$.

Proof. Since D is a division ring, we have $|D^\times| = |D| - 1$ (the only non-unit is 0), so we have that

$$a^{|D|-1} = 1$$

by basic group theory. Hence,

$$a^{|D|} = a.$$

□

Problem 163 (Section 2.7, Exercise 1)**.** Prove that if α is a homomorphism of the ring R into the ring R' and ζ is a homomorphism of R' into R'', then $\zeta \circ \alpha$ is a homomorphism of R into R''.

Proof. Notice that

$$\zeta \circ \alpha(0) = \zeta(0) = 0.$$
$$\zeta \circ \alpha(1) = \zeta(1) = 1.$$

Next, notice that for $x, y \in R$, we have

$$\zeta \circ \alpha(x + y) = \zeta(\alpha(x) + \alpha(y)) = \zeta(\alpha(x)) + \zeta(\alpha(y)) = \zeta \circ \alpha(x) + \zeta \circ \alpha(y),$$
$$\zeta \circ \alpha(xy) = \zeta(\alpha(x)\alpha(y)) = \zeta(\alpha(x))\zeta(\alpha(y)).$$

Hence, we have that $\zeta \circ \alpha$ is a homomorphism. □

Problem 164 (Section 2.7, Exercise 2)**.** Show that if u is a unit in R and ζ is a homomorphism of R into R', then $\zeta(u)$ is a unit in R'. Suppose ζ is an epimorphism. Does this imply that ζ is an epimorphism of the group of units of R into the group of units of R'?

Proof. We proceed as follows:

(1) Let u be a unit. Then there exists a u' such that $uu' = 1$. Hence,

$$\zeta(uu') = \zeta(u)\zeta(u') = \zeta(1) = 1.$$

Therefore, we see that u is mapped to a unit in R'.

(2) No, there may be less units in R than in R', so even though ζ hits everything we may have a $u \in R''$ such that the element which is mapped to u is not a unit.

□

Problem 165 (Section 2.7, Exercise 3)**.** Let I be an ideal in R, n a positive integer. Apply the fundamental theorem on homomorphisms to prove that $M_n(R)/M_n(I) \cong M_n(R/I)$.

Proof. Let $\phi : M_n(R) \to M_n(R/I)$ be given by taking the quotient of the coefficients mod I. Need to check that this is surjective and is a homomorphism. This is surjective, since $R \to R/I$ is surjective, and we have that the kernel is going to be all the matrices with coefficients in I. To see that it is a homomorphism, let $A = (a_{ij}), B = (b_{ij}) \in M_n(R)$. Then letting $AB = C$, we have

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

So applying ϕ gives

$$\phi(c_{ij}) = \phi\left(\sum_{k=1}^{n} a_{ik}b_{kj}\right) = \sum_{k=1}^{n} \phi(a_{ik})\phi(b_{kj}),$$

and so

$$\phi(AB) = \phi(A)\phi(B).$$

Hence, the fundamental theorem gives

$$M_n(R)/M_n(I) \cong M_n(R/I).$$

□

Problem 166 (Section 2.7, Exercise 4)**.** Show that if R is a commutative ring of prime characteristic p, then $a \mapsto a^p$ is an endomorphism of R. Is this an automorphism?

Proof. Recall that the characteristic of a ring R is the smallest positive number p such that

$$1 + \cdots + 1 = p = 0.$$

We want to then check that $\varphi : R \to R$, $\zeta(a) = a^p$ is an endomorphism. To check that, we have

$$\zeta(0) = 0^p = 0,$$

$$\zeta(1) = 1^p = 1,$$

$$\zeta(a+b) = (a+b)^p = \sum_{n=0}^{p} \binom{p}{n} a^n b^{p-n} = a^p + b^p,$$

since every other factor will have some factor of p in it and so will evaluate to 0. Finally, we have

$$\zeta(ab) = (ab)^p = a^p b^p.$$

Hence, it's an endomorphism.

For it to be an automorphism, we need it to be bijective. For injectivity, we see

$$\zeta(a) = \zeta(b) \iff a^p = b^p.$$

We see this does not necessarily hold unless we are in a domain. □

Problem 167 (Section 2.7, Exercise 5)**.** Let F be a finite field of characteristic p (a prime). Show that $p - 1 \mid |F| - 1$. Hence, conclude that if $|F|$ is even, then the characteristic is two.

Proof. We have the map $\varphi : \mathbb{Z} \to R$ given by $\varphi(1) = 1$, $\varphi(0) = 0$, $\varphi(n) = n\varphi(1)$. The kernel of this map is (p), and so we get that there is a subring $R \leq F$ which is isomorphic to $\mathbb{Z}/(p)$. The units of this subring form a subgroup of $U(F)$, and so Lagrange tells us that

$$|U(R)| \mid |U(F)| \leftrightarrow p - 1 \mid |F| - 1.$$

If $|F|$ is even, then $|F| - 1$ is odd. The only prime p which has the property that $p - 1$ divides an odd number is 2; hence, the characteristic of F is 2. □

Problem 168 (Section 2.7, Exercise 6)**.** A ring is *simple* if $R \neq 0$ and R and 0 are the only ideals in R. Show that the characteristic of a simple ring is either 0 or p for a prime.

Proof. Examine the set

$$tR = \{tr \ : \ t \in \mathbb{Z}, r \in R\}$$

(here, tr is defined by r added to itself t times). We see that this is clearly an ideal. It's an additive subgroup clearly, and if $r' \in R$ is multiplied with an element $tr \in tR$, we have

$$r'tr = r'(r + r + \cdots + r) = r'r + r'r + \cdots + r'r = t(r'r) \in tR,$$

and analogously,

$$trr' = (r + \cdots + r)r' = rr' + \cdots + rr' = t(rr') \in tR.$$

Since R is a simple ring, we have $tR = (0)$ or $tR = R$. Let p be the characteristic of the ring R. Then we have that $pR = (0)$, and for all $0 < m < p$, $mR = R$. Assume p was not prime nor 0, then we have $mn = p$ for $m, n < p$. Hence, $mnR = (0)$. But $mR = R$, $nR = R$, and so $mnR = m(nR) = mR = R$, which results in a contradiction since we assumed $R \neq 0$. Hence, if $p \neq 0$, we must have that p is prime. □

Problem 169 (Section 2.7, Exercise 7)**.** If S is a subset of a ring (field) R, then the subring (subfield) generated by S is defined to be the intersection of all the subrings (subfields) containing S. If this is R itself, then S is called a set of generators of the ring (field) R. Show that if η_1 and η_2 are homomorphisms of the ring R into a second ring and $\eta_1(s) = \eta_2(s)$ for every s in a set of generators of the ring R, then $\eta_1 = \eta_2$.

Proof. We need to show that for all $x \in R$, $\eta_1(x) = \eta_2(x)$. Let Z be the collection of elements such that $\eta_1(x) = \eta_2(x)$. We first show that this is a ring. Since these are homomorphisms, $0, 1 \in Z$. Next, if $a, b \in Z$, then we have $a+b \in Z$, since $\eta_1(a+b) = \eta_1(a)+\eta_1(b) = \eta_2(a)+\eta_2(b) = \eta_2(a+b)$. We also have that $-a \in Z$, since $\eta_1(-a) = -\eta_1(a) = -\eta_2(a) = \eta_2(-a)$. Finally, $ab \in Z$, since $\eta_1(ab) = \eta_1(a)\eta_1(b) = \eta_2(a)\eta_2(b) = \eta_2(ab)$. So $Z \subset R$ is a subring. Since $S \subset Z$, and R is the smallest ring which contains S, we must have that $Z = R$. Hence, we have that for all $x \in R$, $\eta_1(x) = \eta_2(x)$. □

Problem 170 (Section 2.7, Exercise 8)**.** Show that every homomorphism of a division ring into a ring $R \neq 0$ is a monomorphism.

Proof. Let D be a division ring, $R \neq 0$ a ring, and $\eta : D \to R$ a homomorphism. It suffices to show that $\ker(\eta) = 0$. Let $a \in \ker(\eta)$. Then we have that $\eta(a) = 0$. Since D is a division ring, if $a \neq 0$, we have that there is a $b \in D$ such that $ab = 1$. Hence, $\eta(a)\eta(b) = \eta(ab) = \eta(1) = 0$. This is a contradiction, since a homomorphism η must map 1 to 1, and $R \neq 0$. Hence, we must have that $a = 0$, which means the kernel is trivial. □

Problem 171 (Section 2.7, Exercise 12)**.** Use exercise 11 (the Chinese Remainder theorem) to prove that if m and n are relatively prime integers, then $\varphi(mn) = \varphi(m)\varphi(n)$, where φ is the Euler φ-function. Show also that if p is a prime, then $\varphi(p^e) = p^e - p^{e-1}$. Hence, prove that if $n = p_1^{e_1} \cdots p_r^{e_r}$, p_i distinct primes, then

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Proof. Since m, n are relatively prime, we have (m), (n) are relatively prime ideals, and so

$$\mathbb{Z}/(mn) \cong \mathbb{Z}/(m) \oplus \mathbb{Z}/(n).$$

These are isomorphic as rings, and so their units are isomorphic. Hence, $\varphi(mn) = \varphi(m)\varphi(n)$.

Next, we need to show that $\varphi(p^e) = p^e - p^{e-1}$. We count the number of elements coprime to p^e. These are the elements which are less than p^e such that they do not have a factor of p. We have that this comes out to $\varphi(p^e) = p^{e-1}(p-1)$, since there are $(p-1)$ factors coprime to p, and we repeat the process of counting this p^{e-1} times.

The formula is clear from these two facts. The primes are all coprime, so

$$\varphi(p_1^{e_1} \cdots p_r^{e_r}) = \prod_{i=1}^{r} \varphi(p_i^{e_i}) = \prod_{i=1}^{r} (p^{e_i} - p^{e_i - 1}).$$

Factoring out p^{e_i}, we get

$$\varphi(n) = \prod_{i=1}^{r} p^{e_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

□

Problem 172 (Section 2.7, Exercise 13)**.** Show that the only ring homomorphism of $\mathbb{R}$ into $\mathbb{R}$ is the identity.

Proof. Let $\phi : \mathbb{R} \to \mathbb{R}$ be a homomorphism. This tells us that $\phi(0) = 0$, $\phi(1) = 1$. For integers p, we see that this is determined by

$$\phi(p) = \phi(1 + \cdots + 1) = p\phi(1) = p.$$

For rationals $1/q$, we see that

$$\phi(1) = \phi(1/q + \cdots + 1/q) = q\phi(1/q) \leftrightarrow \phi(1/q) = 1/q.$$

So for rationals p/q, we have

$$\phi(p/q) = p/q.$$

So $\phi(x)$ is the identity on $\mathbb{Q}$. We want to show that it's the identity on irrational numbers then. Take $x \in \mathbb{R} - \mathbb{Q}$. First, assume that $x > 0$. We have that there is a $y, z \in \mathbb{Q}$ such that $z > x > y > 0$, $|z - y| < 1/n$, $|\phi(z) - \phi(y)| < 1/n$. Taking $n \to \infty$ forces $\phi(z) = \phi(y) = \phi(x)$ when $y = z = x$, so we have the identity. Same idea applies for negatives. □

Problem 173 (Section 2.7, Exercise 15)**.** Define a maximal ideal of a ring R to be a proper ideal I such that there exists no proper ideal I' such that $I \subsetneq I'$. Show that an ideal I of a commutative ring is maximal if and only if R/I is a field.

Proof. ($\implies$) Assume I is maximal. Let $a \in R - I$. Then we have that $I \subset (a) + I \subset R$, and since $a \notin I$ this implies that $(a) + I = R$. In other words, the ideal generated by $\overline{a} \in R/I$ is the whole ring, and so therefore $\overline{a}$ is invertible. Since every non-zero element is invertible, it is a field.

Remark. Notice that a non-zero field is an integral domain. Assume otherwise; that is, $ab = 0$, $a \neq 0$, $b \neq 0$. Then we have that there are c, d such that $ca = 1$, $db = 1$. Hence, $(cd)(ab) = 1 = 0$, which is a contradiction, since a non-zero field must have the property that $1 \neq 0$.

($\impliedby$) If R/I is a field, it has only two ideals; (0) and (1). By the correspondence theorem, this tells us that any ideal containing I must either be I or the whole ring, and so the ideal is maximal. □

Problem 174 (Section 2.7, Exercise 16)**.** Define a prime ideal I of a commutative ring R by the conditions $I \neq R$ and if $ab \in I$ then either $a \in I$ or $b \in I$. Show that if I is maximal, then I is prime.

Proof. Let $ab \in I$ but $a \notin I$, $b \notin I$. Then $\overline{a}, \overline{b} \neq 0 \in R/I$, however, $\overline{a}\overline{b} = 0$. This contradicts the fact that we are in a field. □

Problem 175 (Section 2.7, Exercise 17)**.** Determine the ideals and the maximal ideals and prime ideals of $\mathbb{Z}/(60)$.

Claim 20. The ideals of $\mathbb{Z}/(k)$ are of the form (d), where $d \mid k$.

Proof. Let $I \subset \mathbb{Z}$ be an ideal. Since $\mathbb{Z}$ is a PID, we must have it is principally generated; that is, $I = (d)$. Next, the correspondence theorem tells us that the ideals of $\mathbb{Z}/(k)$ are of the form $(d)/(k)$, where $(k) \subset (d)$. Recall that if $(k) \subset (d)$, then $k \in (d)$, so that $d \mid k$. □

Proof of Exercise 17. By the claim, all the ideals of (60) are generated by divisors of 60. Noting that $60 = 2^2 \cdot 3 \cdot 5$, we have $(0), (1), (2), (3), (4), (5), (6), (10), (12), (15), (20), (30)$ are all the ideals.

In a PID, an ideal is prime if and only if it is maximal. The prime ideals here are the ones which are generated by primes, so we have (2), (3), (5) are all the prime/maximal ideals. □

Problem 176 (Section 2.8, Exercise 7)**.** Define a Jordan homomorphism η of a ring R into a ring R' by the conditions:

(1) η is an additive group homomorphism;
(2) $\eta(1) = 1$;
(3) $\eta(aba) = \eta(a)\eta(b)\eta(a)$.

Show that any homomorphism or anti-homomorphism is a Jordan homomorphism. Show that Jordan homomorphisms satisfy:

(1) $\eta(a^k) = \eta(a)^k$ for all $k \in \mathbb{N}$;
(2) $\eta(ab + ba) = \eta(a)\eta(b) + \eta(b)\eta(a)$;
(3) $\eta(abc + cba) = \eta(a)\eta(b)\eta(c) + \eta(c)\eta(b)\eta(a)$.

Proof. It's clear that a homomorphism is a Jordan homomorphism. Recall a anti-homomorphism is one which switches the order of multiplication, and so

$$\eta((ab)a) = \eta(a)\eta(ab) = \eta(a)\eta(b)\eta(a).$$

Hence, an anti-homomorphism is a Jordan homomorphism. We now show the other three properties.

(1) For this, it suffices to show that $\eta(a^2) = \eta(a)^2$. Notice that $\eta(a^3) = \eta(a)^3$ clearly. Next, notice that

$$\eta(a(1+a)a) = \eta(a)\eta(1+a)\eta(a) = \eta(a)\left[\eta(1) + \eta(a)\right]\eta(a) = \eta(a)^2 + \eta(a)^3,$$

and similarly

$$\eta(a(1+a)a) = \eta(a^2 + a^3) = \eta(a^2) + \eta(a^3) = \eta(a^2) + \eta(a)^3.$$

So cancelling $\eta(a)^3$ from both sides gives

$$\eta(a^2) = \eta(a)^2.$$

(2) Now, we write

$$\eta((a+b)^2) = \eta(a+b)^2 = \eta(a)^2 + \eta(a)\eta(b) + \eta(b)\eta(a) + \eta(b)^2,$$

and similarly

$$\eta((a+b)^2) = \eta(a^2 + ab + ba + b^2) = \eta(a)^2 + \eta(ab + ba) + \eta(b)^2,$$

so cancelling the squares leaves

$$\eta(ab + ba) = \eta(a)\eta(b) + \eta(b)\eta(a).$$

(3) Here, write

$$\eta((b+c)a(b+c)).$$

Much in the same way that everything cancelled before, we are left with the desired result.

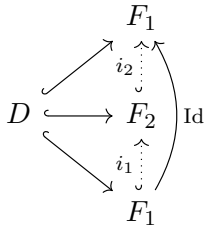
□

Problem 177 (Section 2.9, Exercise 1)**.** What is the field of fractions of a field?

Proof. It is isomorphic to the field itself. See next problem for proof of why this is the case. □

Problem 178 (Section 2.9, Exercise 2)**.** Show that if D is a domain and F_1, F_2 are fields such that D is a subring of each and each is generated by D, then there is a unique isomorphism of F_1 onto F_2 that is the identity map on D.

Proof. Use the universal property of field of fractions. We have



Since the diagrams commute, and the mappings are unique, we get

$$i_2 \circ i_1 = \mathrm{Id}.$$

Since i_2 is injective, the existence of a right inverse makes it a bijection, and so we have it is an isomorphism. Furthermore, i_2 is the identity on D. □

Problem 179 (Section 2.9, Exercise 3)**.** Show that any commutative monoid satisfying the cancellation law ($ab = ac \implies b = c$) can embedded into an abelian group.

Proof. The idea is that the units for a domain form a commutative monoid satisfying the cancellation law, and so since we can embed a domain into a field, we can embed these units into the group of units of a field.

Let M be a commutative monoid satisfying the cancellation law. Take the product set $M \times M$, and define $(a, b) \sim (c, d)$ if and only if $ad = bc$. We see that this defines a relation on $M \times M$;

(1) We see $(a, b) \sim (a, b)$, since $ab = ab$.
(2) We have $(a, b) \sim (c, d)$ implies $ad = cb \iff cb = ad$ or $(c, d) \sim (a, b)$.
(3) If $(a, b) \sim (c, d)$, $(c, d) \sim (e, f)$ we have $ad = cb$, $cf = ed$, and so we have

$$ad = cb \leftrightarrow adf = cbf \leftrightarrow adf = edb \leftrightarrow af = eb,$$

so $(a, b) \sim (e, f)$.

So it is indeed an equivalence relation. We can then quotient by this equivalence class to get $(M \times M)/\sim$. Notice that, denoting $[(a, b)] \in (M \times M)/\sim =: G$ by a/b, we have that G is a group, with $1/1 = 1$ as the identity. To see this, first notice it's clearly closed under multiplication; $(a/b)(c/d) = ac/bd$. It's also clearly associative, inheriting this from the monoid. $(1/1)$ is the identity, since $(a/b)(1/1) = (1/1)(a/b) = a/b$. Finally, for any $a/b \in G$, we have b/a is the inverse, since $ab/ab = (a/a)(b/b)$, and $a/a \sim 1/1$, since $a = a$. Hence, it's a group.

We can embed our monoid into G by taking the mapping $\zeta : M \to G$ via $\zeta(a) = a/1$. This is a homomorphism, since $\zeta(ab) = ab/1 = (a/1)(b/1) = \zeta(a)\zeta(b)$, $\zeta(1) = 1/1 = 1$, and we have that it's injective, since if $\zeta(a) = a/1 = b/1 = \zeta(b)$, then $a = b$. □

Problem 180 (Section 2.9, Exercise 4)**.** Show that if $a^m = b^m$ and $a^n = b^n$ for m and n relatively prime positive integers, and a and b in a commutative domain, then $a = b$.

Proof. If a or b are zero, then we have that the other is nilpotent, and since the only nilpotent in a commutative domain is zero, we have that it is zero. So assume that $a, b \neq 0$. Since they're relatively prime, we have that there are $c, d \in \mathbb{Z}$ such that $cm + dn = 1$. At least one of c, d needs

to be bigger than 0; assume c is larger than 0. Then since $a^m = b^m$, we have $a^{mc} = b^{mc}$. Notice that

$$a^{mc} = b^{mc} \implies a^{mc+dn} = b^{mc+dn} \iff a = b$$

after using factoring and cancellation. Hence, have they are equal. □

Remark. From here on out, all rings are commutative (recall commutative means that for all $a, b \in R$ we have $ab = ba$).

Problem 181. Finish the proof of Theorem 2.10. That is, prove the following (universal property):

Let R, S be commutative rings, η a homomorphism of R into S, u an element of S. Let $R[x]$ be the ring of polynomials over R in the indeterminate x. Then η has one and only one extension to a homomorphism η_u of $R[x]$ into S mapping x into u.

Proof. Let $A = a_0 + a_1x + \cdots + a_nx^n$. Then we have

$$\eta_u(A) = a_0' + a_1'u + \cdots + a_n'u^n,$$

where we let $a' = \eta(a)$. If $B = b_0 + \cdots + b_mx^m$, then $AB = p_0 + \cdots + p_{n+m}x^{n+m}$, where $p_i = \sum_{j+k=i} a_jb_k$. Then

$$\eta_u(AB) = p_0' + \cdots + p_{n+m}'u^{n+m},$$

and

$$p_i' = \sum_{j+k=i} a_j'b_k'$$

since η is a ring homomorphism. On the other hand,

$$\eta_u(A)\eta_u(B) = (a_0' + \cdots + a_n'x^n)(b_0' + \cdots + b_m'u^m) = p_0' + \cdots + p_{n+m}'u^{n+m} = \eta_u(AB).$$

Let $n = m$ without loss of generality (if they are not equal, set the coefficients which are missing to be 0). Notice as well that

$$\eta_u(A) + \eta_u(B) = (a_0' + \cdots + a_n'x^n) + (b_0' + \cdots + b_n'x^n) = (a_0' + b_0') + \cdots + (a_n' + b_n')x^n = \eta_u(A + B)$$

using the homomorphism property of η. Notice as well that, by construction, η_u is an extension of η, and η_u is a homomorphism of $R[x]$ into S. By **Section 2.7, Exercise 7**, this gives us that this is unique, since x and R generate $R[x]$.s □

Remark. We call this map $\eta_u : R[x] \to R[u] \subset S$ the **evaluation map**. Notice that η_u is a surjection, and so by the fundamental theorem, we have $R[x]/\ker(\eta_u) \cong R[u]$. Furthermore, since η_u is the identity on R, we must have $\ker(\eta_u) \cap R = 0$.

Remark. Notice that if we have an ideal I such that $I \cap R = 0$, then there is a ring $R[u]$ such that $R[x]/I \cong R[u]$. We get this via **Theorem 2.10**, by noticing that $R \subset R[x]/I = S$ is an ambient ring, and $\eta : R \to S$ is the identity, so we can extend it uniquely to a map $\eta' : R[x] \to R[x]/I$.

Remark. Algebraically independent is equivalent to transcendental, algebraic implies a non-trivial relation.

Problem 182. Show that $\sqrt{3} + \sqrt{5}$ is algebraic over $\mathbb{Q}$.

Proof. To be algebraic means that there is a polynomial with coefficients in $\mathbb{Q}$ such that $\sqrt{3} + \sqrt{5}$ is a root. Let $a = \sqrt{3} + \sqrt{5}$. Notice that

$$a^2(\sqrt{3} + \sqrt{5})^2 = 3 + 2\sqrt{15} + 5 = 8 + 2\sqrt{15}.$$

Hence

$$a^2 - 8 = 2\sqrt{15}.$$

Squaring both sides gives

$$(a^2 - 8)^2 = 60,$$

so

$$(a^2 - 8)^2 - 60 = 0.$$

So it is in fact algebraic over $\mathbb{Z}$. □

Problem 183. Let $F \subset K$ be fields, let $u \neq 0$ in K be algebraic over F. Show that u^{-1} is algebraic over F.

Proof. Since u is algebraic over F, we have that there is a $f(x) \in F[x]$ such that $f(u) = 0$. Write

$$f(x) = a_0 + \cdots + a_n x^n,$$

then

$$f(u) = a_0 + \cdots + a_n u^n = 0.$$

Multiplying by u^{-n} to both sides gives

$$u^{-n} f(u) = a_0 u^{-n} + \cdots + a_n = g(u^{-1}) = 0.$$

Notice that, since the $a_i \in F$, we have that $g(x) \in F[x]$ is such that $g(u^{-1}) = 0$. Hence, u^{-1} is algebraic over F as well. □

Problem 184. Suppose that u is algebraic over the field $F \subset K$, and $a \in F$. Show that $u + a$ is algebraic over F, find the minimal polynomial of $u + a$, and show that $u + a$ and u have the same degree over F.

Proof. Since u is algebraic over the field F, there is an $f(x) \in F[x]$ such that

$$f(x) = a_0 + \cdots + a_n x^n,$$
$$f(u) = a_0 + \cdots + a_n u^n = 0.$$

Define

$$g(x) = f(x - a).$$

We have

$$g(x) = a_0 + a_1(x - a) + \cdots + a_n(x - a)^n = b_0 + b_1 x + \cdots + b_n x^n,$$

where b_i are the appropriate coefficients in F. Furthermore, we see that

$$g(u + a) = a_0 + a_1(u + a - a) + \cdots + a_n(u + a - a)^n = a_0 + a_1 u + \cdots + a_n u^n = 0.$$

Hence, $u + a$ is algebraic over F. Furthermore, this has the same degree as u. To see that it's minimal, we note that this is also monic and irreducible, since $f(x)$ was irreducible. □

Problem 185 (Section 2.10, Exercise 1)**.** Show that the complex number

$$\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$$

is algebraic over $\mathbb{Q}$. Show that $\mathbb{Q}[\omega] \cong \mathbb{Q}[x]/(I)$, where I is the ideal generated by $(x^2 + x + 1)$.

Proof. Notice

$$2\omega + 1 = \sqrt{3}i.$$

Hence,

$$(2\omega + 1)^2 = -3,$$

so

$$(2\omega + 1)^2 + 3 = 0.$$

Replacing ω with x, we have

$$f(x) := 4x^2 + 4x + 4$$

is such that

$$f(\omega) = 0.$$

Thus, ω is algebraic over $\mathbb{Q}$.

Next, let $\zeta : \mathbb{Q}[x] \to \mathbb{Q}[\omega]$ defined by

$$\zeta(f(x)) = f(\omega),$$

i.e. it's the evaluation map. First, note it's a well-defined surjective homomorphism (epimorphism). Then the kernel is

$$\ker(\zeta) = \{f(x) \in \mathbb{Q}[x] \ : \ f(\omega) = 0\}.$$

We have that

$$(x^2 + x + 1) \subset \ker(\zeta)$$

from above. To get the other direction, take $f \in \ker(\zeta)$ non-zero. We have either $\deg(f) \geq 2$ or $\deg(f) < 2$. If $\deg(f) < 2$, this implies there is some linear polynomial so that $f(\omega) = 0$. However, any linear polynomial will still have complex irrational components, and so this is impossible. Hence, we must have $\deg(f) \geq 2$. Since $\deg(f) \geq 2$, we can invoke the division algorithm, letting $g = x^2 + x + 1$, to get

$$f(x) = q(x)g(x) + r(x),$$

where $-\infty < \deg(r(x)) < 2$. We have that

$$f(\omega) = q(\omega)g(\omega) + r(\omega) \leftrightarrow r(\omega) = 0,$$

but this can only happen if $r = 0$. Hence, $g \mid f$.

Thus, we have that $f \in (x^2 + x + 1)$, and so $\ker(\zeta) \subset (x^2 + x + 1)$. Hence, we have equality, and so the isomorphism theorem gives

$$\mathbb{Q}[x]/(I) \cong \mathbb{Q}[\omega].$$

□

Problem 186 (Section 2.10, Exercise 2)**.** Show the following:

(1) $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.
(2) The real numbers $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are linearly independent over $\mathbb{Q}$.
(3) $u = \sqrt{2} + \sqrt{3}$ is algebraic.
(4) Determine the ideal I such that

$$\mathbb{Q}[x]/I \cong \mathbb{Q}[u].$$

Proof.

(1) We first show that there are no $a, b \in \mathbb{Q}$ such that $a + b\sqrt{2} = \sqrt{3}$. Notice if there were, we would have that $a = \sqrt{3} - b\sqrt{2}$. This can only happen if a is 0, since the right hand side is entirely irrational, but this means that $b\sqrt{2} = \sqrt{3}$, or $b = \sqrt{3}/\sqrt{2}$. Since this is irrational as well, we have that there is no such b, and so $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

(2) We have that $1, \sqrt{2}$, and $\sqrt{3}$ are all linearly independent over $\mathbb{Q}$ by (1). Notice that if

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$$

for some a, b, c, d not all 0, then this implies that

$$\sqrt{6} = a + b\sqrt{2} + c\sqrt{3},$$

where a, b, c are appropriately normalized by $-d$. Notice that a must be 0, and so we have

$$\sqrt{6} = b\sqrt{2} + c\sqrt{3}.$$

Since $\sqrt{6} = \sqrt{2 \cdot 3} = \sqrt{2}\sqrt{3}$, we have that

$$\sqrt{6} - b\sqrt{2} = c\sqrt{3} \iff \sqrt{2}(\sqrt{3} - b) = c\sqrt{3}.$$

Squaring both sides gives

$$2(\sqrt{3} - b)^2 = 3c,$$

after letting c be c^2 since it's arbitrary anyways. Dividing both sides by 2 and squaring gives

$$3 + 2\sqrt{3}b + b^2 = 3c.$$

So $\sqrt{6}$ is in the span if and only if we have b, c non-zero rationals which solve this polynomial. By normalizing, we have that this is equivalent to non-zero b, c integers which solve this polynomial. We see this only happens if $b = 0$, $c = 1$, a contradiction.

(3) To see this is algebraic, notice that

$$u^2 = 5 + 2\sqrt{6}.$$

Hence,

$$u^2 - 5 = 2\sqrt{6},$$

and squaring both sides again gives

$$(u^2 - 5)^2 = 24,$$

so we have

$$(u^2 - 5)^2 - 24 = 0,$$

or after expanding, u is the root of the polynomial

$$x^4 - 10x^2 + 1.$$

Hence, it's algebraic.

(4) The above is the minimal polynomial where this will be a root, and so we get that $I = (x^4 - 10x^2 + 1)$ is the appropriate polynomial.

□

Problem 187 (Section 2.10, Exercise 3)**.** Let I be an ideal in R and let $I[x_1, \ldots, x_r]$ denote the subset of $R[x_1, \ldots, x_r]$ of polynomials with coefficients in I. Show that $I[x_1, \ldots, x_r]$ is an ideal in $R[x_1, \ldots, x_r]$, and that

$$R[x_1, \ldots, x_r]/I[x_1, \ldots, x_r] \cong (R/I)[y_1, \ldots, y_r].$$

Remark. Notice that

$$(R/I)[y_1, \ldots, y_r] \cong (R/I)[x_1, \ldots, x_r].$$

Proof. To show it's an ideal, we first show it's an additive subgroup under addition. For notations sake, label $J = I[x_1, \ldots, x_r]$ and $S = R[x_1, \ldots, x_r]$. Taking $f, g \in J$, we have $f + g$ adds component wise, and so will be in J again. Take $f \in S$, $g \in J$; that is,

$$f = a_0 + a_1 x + \cdots + a_n x^n,$$

$$g = b_0 + b_1 x + \cdots + b_m x^m,$$

then we have

$$fg = \sum_{i=1}^{nm} \left(\sum_{j+k=i} a_j b_i \right) x^i.$$

Since I is an ideal, $a_j b_i \in I$, and since it's a subgroup under addition the sum of these will be in I. Hence, $fg \in J$, so it is an ideal.

Let $\varphi : S \to (R/I)[y_1, \ldots, y_r]$ be defined by $\varphi(a_0 + \cdots + a_n x^n) = b_0 + \cdots + b_n y^n$, where $b_i = a_i + I$. This is clearly well-defined, it's a homomorphism since $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(fg) = \varphi(f)\varphi(g)$, and $\varphi(f + g) = \varphi(f) + \varphi(g)$. It's also clearly surjective, and so since the kernel is J, we have $S/J \cong (R/I)[y_1, \ldots, y_r]$. □

Problem 188 (Section 2.10, Exercise 7)**.** Let $R[[x]]$ denote the set of unrestricted sequences $(a_0, a_1, \ldots)$, where $a_i \in R$. Show that one gets a ring from $R[[x]]$ if one defines $+, \cdot, 0, 1$ as in the polynomial ring. This is called the ring of formal power series in one indeterminate.

Proof. Recall to show a ring, we need to show that it's an abelian group under addition, monoid under mulitplication, and satisfies the distributive properties. We first check the group property.

Let $A = (a_0, a_1, \ldots)$ and $B = (b_0, b_1, \ldots)$. We first note closure, since $A + B = (a_0 + b_0, \ldots) \in R[[x]]$. Next, we note associativeness, since it's associative in each component. Next, we note that $A + (0, \ldots) = (a_0 + 0, \ldots) = (a_0, \ldots) = A$, and likewise for the other direction, so 0 is an identity. Next, $A + (-A) = (a_0, \ldots) + (-a_0, \ldots) = (a_0 - a_0, \ldots) = (0, \ldots) = 0$, so it's closed under inverses. Finally, since R is commutative, we have $a_i + b_i = b_i + a_i$ in each component, and so $A + B = B + A$. So it's an abelian group.

Next, we check it's a monoid under multiplication. First, we have closure, since

$$AB = (c_0, \ldots)$$

where

$$c_n = \sum_{i+j=n} a_i b_j.$$

Since $c_n \in R$ for all n, we have that it's closed. Next, we check associativeness. That is, if $C = (c_0, \ldots)$, we have

$$A(BC) = A \cdot \left(\sum_{i+j=0} b_i c_j, \ldots \right) = \left(\sum_{i+l=0} a_i \sum_{j+k=l} b_j c_k, \ldots \right)$$

$$= \left(\sum_{i+j+k=0} a_i b_j c_k, \ldots \right) = \left(\sum_{i+k=l} a_i b_k \sum_{l+j=0} c_j, \ldots \right) = \left(\sum_{i+k=0} a_i b_k, \ldots \right) \cdot C = (AB)C.$$

So we have it's associative. Finally, we see that $1 = (1, 0, \ldots) \in R[[x]]$ acts as the identity, since

$$A \cdot (1, 0, \ldots) = (a_0, a_1, \ldots) = A.$$

Finally, we need to check distributivity. First, we check

$$A \cdot (B + C) = AB + AC.$$

Notice that

$$A \cdot (b_0 + c_0, \ldots) = \left(\sum_{i+j=0} a_i (b_j + c_j), \ldots \right) = \left(\sum_{i+j=0} a_i b_j + \sum_{i+j=0} a_i c_j, \ldots \right) = AB + AC.$$

Next, we check

$$(A + B) \cdot C = AC + BC.$$

Notice that

$$(A + B) \cdot C = (a_0 + b_0, \ldots) \cdot C = \left(\sum_{i+j=0} (a_i + b_i) c_j, \ldots \right) = AC + BC.$$

So we have it's distributive. Hence, it's a ring. □

Problem 189 (Section 2.10, Exercise 8)**.** Let M be a monoid, R a commutative ring, and $R[M]$ the set of maps $m \to f(m)$ of M into R such that $f(m) = 0$ for all but a finite number of m. Define addition, multiplication, 0, and 1 in $R[M]$ by

$$(f + g)(m) = f(m) + g(m),$$

$$(fg)(m) = \sum_{pq=m} f(p)g(q),$$
$$0(m) = 0,$$
$$1(m) = 1,$$
$$1(m) = 0 \text{ if } m \neq 1.$$

(a) Show that $R[M]$ is a ring.
(b) Show that the set of maps a' such that $a'(1) = a$ and $a'(m) = 0$ if $m \neq 1$ is a subring isomorphic to R. Identify the ring indicated.
(c) Show that the set of maps m' such that $m'(m) = 1$ and $m'(n) = 0$ if $n \neq m$ is a submonoid of the multiplicative monoid of $R[M]$ isomorphic to M. Identify the monoid indicated.
(d) Show that R is the center of $R[M]$, and every element of $R[M]$ can be written as a linear combination of elements of M with coefficients in R; that is, in the form $\sum r_i m_i, r_i \in R$, $m_i \in M$.
(e) Show that $\sum r_i m_i = 0$ if and only if every $r_i = 0$.
(f) Show that if σ is a homomorphism of R into a ring S such that $\sigma(R)$ is contained in the center of S, and if τ is a homomorphism of M into the multiplicative monoid of S, then there exists a unique homomorphism of $R[M]$ into S coinciding with σ on R and with τ on M.

If M is a group, $R[M]$ is called the group algebra of M over R.

Proof. (a) We show that $R[M]$ is an abelian group under addition and a monoid under multiplication. We first check closure under addition. Throughout, f, g, h are arbitrary elements. Notice that for $f, g \in R[M]$, we have

$$(f + g)(m) = f(m) + g(m),$$

and this is 0 for all but a finite number of m, since f and g respectively are 0 for all but a finite number of M. Hence, $f + g \in R[M]$. Next, we have that

$$((f+g)+h)(m) = (f+g)(m)+h(m) = (f(m)+g(m))+h(m) = f(m)+(g(m)+h(m)) = (f+(g+h))(m)$$

for all $m \in M$, using the associative property of R. Hence, we have

$$f + (g + h) = (f + g) + h.$$

Next, we check that 0 is the identity. This, however, follows again using the underlying structure of R; for all $f \in R[M]$, we have

$$(f + 0)m = f(m) + 0(m) = f(m) = 0(m) + f(m) = (0 + f)(m)$$

for all m, and so

$$f + 0 = f = 0 + f.$$

Next, we check for inverses. Define $-f$ to be $-f(m)$ for all m. Then we have

$$(f + (-f))(m) = f(m) + -f(m) = 0 = -f(m) + f(m) = ((-f) + f)(m)$$

for all m, and so

$$f + (-f) = 0 = (-f) + f.$$

Hence, we have inverses by the underlying structure of R. Finally, we check that this is abelian under addition, but again this follows by the structure of R; we have

$$(f + g)(m) = f(m) + g(m) = g(m) + f(m) = (g + f)(m)$$

for all m, and so

$$f + g = g + f.$$

We now check that it is a monoid under multiplication. We have closure, since

$$(fg)(m) = \sum_{pq=m} f(p)g(q)$$

for all m, and so it's still in $R[M]$. We check associativity. That is,

$$((fg)h)(m) = \sum_{pq=m} (fg)(p)h(q) = \sum_{pq=m} \left(\sum_{jk=p} f(j)g(k) \right) h(q)$$

$$\sum_{jkq=m} f(j)g(k)h(q) = \sum_{jt=m} f(j) \sum_{kq=t} g(k)h(q) = \sum_{jt=m} f(j)(gh)(t) = (f(gh))(m),$$

and so we have associativity. Finally, $1(1) = 1$ is the identity, since

$$(f1)(m) = \sum_{pq=m} f(p)1(q) = f(m),$$

and likewise

$$(1f)(m) = \sum_{pq=m} 1(p)f(q) = f(m).$$

We then need to check the distributive laws. That is, for all $f, g, h \in R[M]$, we have

$$f(g+h) = fg + fh,$$

and

$$(f+g)h = fh + gh.$$

For the first, notice that we have for all m,

$$(f(g+h))(m) = \sum_{pq=m} f(p)(g+h)(q) = \sum_{pq=m} f(p)g(q) + f(p)h(q) = (fg)(m) + (fh)(m),$$

using the underlying ring properties. Since this applies for all m, we get the first property. For the other, we analogously have

$$((f+g)h)(m) = \sum_{pq=m} (f+g)(p)h(q) = \sum_{pq=m} f(p)h(q) + g(p)h(q) = (fh)(m) + (gh)(m),$$

again using the underlying ring properties. Since m arbitrary, we get the second property, so we have distributivity. Hence, it's a ring.

(b) We first show that the set of maps a' such that $a'(1) = a$ and $a'(m) = 0$ if $m \neq 1$ is a subring. Let R' denote this set. Notice that we have $1 \in R'$ and $0 \in R'$ clearly. Next, notice that it's a subgroup under addition, since for arbitrary a', b', and m we have

$$(a' - b')(m) = a'(m) - b'(m),$$

which is $a - b$ if $m = 1$ and 0 otherwise. Hence, $a' - b' \in R'$. We see that it's a submonoid under multiplication, since

$$(a'b')(m) = \sum_{pq=m} a'(p)b'(q),$$

which is ab if $m = 1$ and 0 otherwise. So this is indeed a subring.

To get that it's isomorphic to R, we need to create a map $f : R \to R'$ which is a homomorphism and bijective. Let $f : R \to R'$ be the obvious map $f(a) = a'$. Then this is well-defined, since if $a = b$, $f(a) = a' = b' = f(b)$. This is injective, since $f(a) = 0$ happens if and only if $a = 0$, so the kernel is trivial. Finally, it's surjective, since for any map $a' \in R$, we have that $a'(1) = a$, and so we have $f(a) = a'$. So it's a bijection. Furthermore, $f(1) = 1$, $f(0) = 0$, and

we have $f(a+b) = (a+b)' = a' + b'$ by the work above, and $f(ab) = (ab)' = a'b'$ by the work above. So it's an isomorphism.

This is the dual of R, which we will just identify as R under this isomorphism.

(c) We first show that M', the set of all maps m' where $m'(m) = 1$ and $m'(n) = 0$ for $n \neq m$, is a submonoid of the multiplicative monoid. To do so, we need to check that 1 is in it, and that it's closed under multiplication. We clearly see that $1 \in M'$ by definition, though. To see it's closed under multiplication, we have

$$m'n'(t) = \sum_{pq=t} m'(p)n'(q),$$

which is equal to mn if $t = mn$ and 0 otherwise.

We now need to show that this is isomorphic to M. Let $f : M \to M'$ be defined by $f(m) = m'$. Then this is well-defined, since if $m = n$, $f(m) = m' = n' = f(n)$ by definition. It's injective, since if $f(m) = f(n)$, then we have $m' = n'$, which can only happen if $m = n$. It's clearly surjective, since $m'(m) = m$, so taking m we have $f(m) = m'$, and so it's a bijection. To get that it's a homomorphism, we have $f(1) = 1$, and $f(ab) = (ab)' = a'b' = f(a)f(b)$ by prior work.

This is the dual of M, which we identify as M under this isomorphism.

(d) We first show that R is the center of $R[M]$. Take $f \in R[M]$, $r \in R$, and identify r with it's dual in $R[M]$; that is, the function r' such that $r'(1) = r$ and $r'(m) = 0$ for $m \neq 1$. Then we have that, for m arbitrary,

$$(r'f)(m) = \sum_{pq=m} r'(p)f(q) = r'(1)f(m) = rf(m) = f(m)r = \sum_{pq=m} f(p)r'(q) = (fr')(m).$$

So we get $r'f = fr'$, and so $r' \in C(R[M])$. Since the choice of r' was arbitrary, we get $R \subset C(R[M])$. We then need to show that $C(R[M]) \subset R$. Take c in the center, then we have that

$$(fc)(m) = \sum_{pq=m} f(p)c(q) = \sum_{pq=m} c(p)f(q) = (cf)(m)$$

for m arbitrary. If c is not in R, then we have that $c(t) \neq 0$ for some $t \neq 1$. Since this applies for all f, m, take without loss of generality l, m, and f such that $tl = m$, $f(l) \neq 0 \neq f(t)$, and $c(l) = 0$. Then we have that $(fc)(m) \neq (cf)(m)$ by the above, and so $cf \neq fc$. Hence, c must be in R, and so $R = C(R[M])$.

We now show that every element of $R[M]$ can be written in a linear combination of elements of M with coefficients in R. Take $f \in R[M]$. We have that $f(m) \in R$ for all m, and so we have

$$f(m) = (r'm')(m) = r.$$

Hence, since f is zero for all but a finite number of m, we can write that it's finite on $m_1, \ldots, m_n$, and we have $f(m_i) = r_i \in R$. Using the identification, we get

$$f = \sum_{i=1}^{n} r_i m_i,$$

since

$$f(m_i) = \sum_{i=1}^{n} r_i(m_i)m_i(m_i) = r_i.$$

The fact that R is in the center let's us have all of the r_i on the left.

(e) We now need to show that

$$\sum r_i m_i = 0$$

if and only if every $r_i = 0$. We interchangeably use the function and element identification to get the result. The converse direction is clear, so we proceed with the forward direction. Assume we have

$$\sum r_i m_i = 0.$$

Then for every m_i, we have

$$(\sum r_i m_i)(m_i) = \sum r_i(m_i) m_i(m_i) = r_i = 0.$$

Thus, we get $r_i = 0$. Doing this for all m_i gives us the desired result.

(f) Let $\sigma : R \to S$ be a homomorphism such that $\sigma(R) \subset C(S)$. Let $\tau : M \to (S, \cdot, 1)$. We construct the ring homomorphism $\gamma : R[M] \to S$ as follows; we have

$$\gamma(f) = \gamma\left(\sum_i r_i m_i\right) = \sum_i \sigma(r_i)\tau(m_i).$$

We first check that this is indeed a ring homomorphism; clearly $\gamma(0) = \sigma(0)\tau(0) = 0$, $\gamma(1) = \sigma(1)\tau(1) = 1$ since these are homomorphisms. Next, we have

$$\gamma(f+g) = \gamma\left(\sum_i r_i m_i + \sum_j a_j b_j\right) = \gamma\left(\sum_i (r_i + a_i) m_i\right),$$

where we take $r_i = 0$ if $m_i = 0$ and likewise for a_j, b_j (so that we can extend it to the whole sum). Hence, we get

$$\gamma\left(\sum_i (r_i + a_i) m_i\right) = \sum_i \sigma(r_i + a_i)\tau(m_i) = \sum_i \sigma(r_i)\tau(m_i) + \sigma(a_i)\tau(m_i) = \gamma(f) + \gamma(g),$$

using the homomorphism property for σ. Finally, we check

$$\gamma(fg) = \gamma\left(\sum_i c_i n_i\right) = \sum_i \sigma(c_i)\tau(n_i),$$

where this is defined via a convolution of sums; that is, $c_i = \sum_{p+q=i} r_p a_q$ and $n_i = \sum_{p+q=i} m_p b_q$, and so using the homomorphism property of σ and τ we get that

$$\gamma(fg) = \sum_i \sigma(c_i)\tau(n_i) = \left(\sum_i \sigma(r_i)\tau(m_i)\right)\left(\sum_j \sigma(a_j)\tau(b_j)\right) = \gamma(f)\gamma(g).$$

So we have established existence.

For uniqueness, assume there was another such map, say δ. Then we want to check that $\delta(f) = \gamma(f)$ for any choice of f. First, we have that $\delta(r) = \gamma(r)$ and $\delta(m) = \gamma(m)$ for all $r \in R$, $m \in M$. Next, notice that the homomorphism property of δ says that

$$\delta(rm) = \delta(r)\delta(m) = \gamma(r)\gamma(m) = \gamma(rm),$$

and so by (d), since $f = \sum r_i m_i$ for all f, we get

$$\delta(f) = \delta\left(\sum r_i m_i\right) = \sum \delta(r_i)\delta(m_i) = \sum \gamma(r_i)\gamma(m_i) = \gamma\left(\sum r_i m_i\right) = \gamma(f).$$

Since this applies for all f, we have that $\delta = \gamma$, and so the homomorphism is unique.

□

Problem 190. Let F be a field. Show that an ideal $I = (f(x))$ in $F[x]$ is maximal if and only if $f(x)$ is irreducible. Does this argument hold over a PID?

Proof. ($\implies$) Assume I maximal. Then we have that, for any ideal J such that $I \subset J \subset R$, we must have $J = R$ or $J = I$. Since $F[x]$ is a PID, this implies that $J = (g(x))$ for some $g(x) \in F[x]$. So this implies that if $g(x) \mid f(x)$, we have either $f(x) \sim g(x)$ or $g(x)$ is a unit. Hence, $f(x)$ must be irreducible.
($\impliedby$) Assume $f(x)$ irreducible, let $I = (f(x))$. Take J such that $I \subset J$. Since J is a PID, we have $J = (g(x))$. Notice $I \subset J$ implies $g(x) \mid f(x)$. Since $f(x)$ irreducible, we have either $f(x) \sim g(x)$, in which case $I = J$, or $g(x)$ is a unit, in which case $J = R$. Thus, I must be maximal.

Nothing we used in the argument was specific to $F[x]$, and we see it does hold for any PID. □

Remark. Notice that this tells us that, over a PID, a non-zero prime ideal is maximal.

Problem 191. Is the ring $\mathbb{Z}[x]/(x^3 + 1, 2)$ a field?

Proof. By prior work, we notice that

$$\mathbb{Z}[x]/(x^3 + 1, 2) \cong \mathbb{F}_2[x]/(x^3 + 1).$$

Over $\mathbb{F}_2[x]$, $x^3 + 1$ has root 1. So it can be written as $x^3 + 1 = (x + 1)q(x)$, $\deg(q) = 2$. Since it's not irreducible, this is not a maximal ideal, so we see that it's not a field. □

Problem 192. Find all the ideals in $\mathbb{Z}[x]/(x^3 + 1, 2)$.

Proof. By the last problem, we see that it suffices to find all the ideals which contain $x^3 + 1$. Since $x^3 + 1$ factors, we just need to find $q(x)$. So $q(x) = x^2 + bx + c$, and we have

$$(x + 1)(x^2 + bx + c) = x^3 + (b + 1)x^2 + (b + c)x + c.$$

This forces $c = 1$, $b + c = 0$, $b + 1 = 0$. So $b = 1$, and we have

$$q(x) = x^2 + x + 1.$$

Since $q(1) \neq 0$, we have that $(x^2 + x + 1)$ and $(x + 1)$ are two ideals in $\mathbb{F}_2[x]$, and these are the only ideals (non-trivial). □

Problem 193 (Section 2.11, Exercise 3)**.**

(1) Show that $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ are not isomorphic.
(2) Let $\mathbb{F}_p$ be the finite field with p elements, and let $R_1 = \mathbb{F}_p[x]/(x^2 - 2)$, $R_2 = \mathbb{F}_p[x]/(x^2 - 3)$. Determine whether $R_1 \cong R_2$ in each of the cases in which $p = 2, 5, 11$.

Proof.

(1) Notice

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[\sqrt{2}],$$
$$\mathbb{Q}[x]/(x^2 - 3) \cong \mathbb{Q}[\sqrt{3}],$$

$(x^2 - 2) \neq (x^2 - 3)$ in $\mathbb{Q}[x]$, so they cannot be isomorphic.

(2) We construct an isomorphism $\phi : \mathbb{F}_2[x]/(x^2 - 2) \to \mathbb{F}_2[x]/(x^2 - 3)$. Define $\phi(1) = 1$, $\phi(x) = x + 1$. We first see this is an isomorphism on $\mathbb{F}_2[x]$. Notice it's injective, since $\phi(x) = \phi(y) \implies x + 1 = y + 1 \implies x = y$, and $\phi(a) = \phi(b) \iff a = b$. It's surjective, x^n is hit by $(x - 1)^n$. So since $\phi(x^2 - 2) = (x + 1)^2 - 2 = x^2 + 2x + 1 - 2 = x^2 - 1 = x^2 - 3$, we have that it descends to an isomorphism on $\mathbb{F}_2/(x^2 - 2)$ to $\mathbb{F}_2[x]/(x^2 - 3)$.

Next, we want to do it for $\mathbb{F}_5[x]$. Notice $x^2 - 2$ is irreducible in $\mathbb{F}_5$, so $\mathbb{F}_5[x]/(x^2 - 2)$ is a field. In particular, it's a field with 25 elements. Notice that $x^2 - 3$ is also irreducible over $\mathbb{F}_5$, and so $\mathbb{F}_5[x]/(x^2 - 3)$ is a field with 25 elements. Fields of the same size are isomorphic, so we are done.

Over $\mathbb{F}_{11}[x]$, we see that $x^2 - 2$ is still irreducible, but $x^2 - 3$ is not; notice that $(5)^2 - 3 = 25 - 3 = 22 \equiv 0 \pmod{11}$. Hence, they are not isomorphic over $\mathbb{F}_{11}[x]$.

□

Problem 194 (Section 2.11, Exercise 4)**.** Show that $x^3 + x^2 + 1$ is irreducible in $\mathbb{F}_2[x]$ and that $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ is a field with 8 elements.

Proof. Assume it were not irreducible; we have then that $x^3 + x^2 + 1 = fg$, where $f, g \in \mathbb{F}_2[x]$. By the degree formula, we must have $\deg(f) + \deg(g) = 3$, and for it to not be irreducible (since this is a field), we need $\deg(f), \deg(g) > 0$. Hence, we have $\deg(f) = 1, \deg(g) = 2$ and $\deg(g) = 2, \deg(f) = 1$ are our two options. It suffices to consider one of these scenarios, and so we have

$$f = a_0 + a_1 x + a_2 x^2,$$

$$g = b_0 + b_1 x.$$

Notice that we need $a_2 b_1 = 1$, so this forces them both to be 1. Likewise, $a_0 b_0 = 1$, so this forces both of them to be 1. So we have

$$f = 1 + a_1 x + x^2,$$

$$g = 1 + x.$$

Expanding gives

$$fg = 1 + x(a_1 + 1) + (a_1 + 1)x^2 + x^3.$$

Notice that this tells us that $a_1 + 1 = 0$ and $a_1 + 1 = 1$, which is impossible. Hence, it does not factor.

Examine $f \in \mathbb{F}_2[x]/(x^3 + x^2 + 1) = F$. Factoring out by the polynomial is equivalent to setting $x^3 = x^2 + 1$. Notice that for x^4, we have $x^4 = (x^3)x = (x^2 + 1)x = x^3 + x$. We claim that, for every $n > 3$, we can reduce the degree of this polynomial by at least one by doing this. Notice that $x^n = x^{3k+r}$, where $0 \leq r < 3$ by the division algorithm, and so we have $x^n = x^{3k}x^r = (x^2 + 1)^k x^r$. The degree of this is now less than n, and so we have successfully reduced this by at least one. Hence, it holds for all $n \geq 3$. Doing this inductively gives that the degree of any polynomial in F will have degree less than 3, and so it suffices to count all possible non trivial combinations of this. Thus, we have

$$0, 1, x, x + 1, x^2, x^2 + x, x^2 + 1, x^2 + x + 1$$

are all the elements in this field (it's a field since it's an irreducible polynomial, and hence maximal).
□

Problem 195 (Section 2.11, Exercise 5)**.** Construct fields with 25 and 125 elements.

Proof. It suffices by the last problem to find irreducible polynomials of degrees 2 and 3 in $\mathbb{F}_5[x]$. From earlier, we see $x^2 - 2$ is irreducible in $\mathbb{F}_5[x]$, so this will give us a field with 25 elements.

We have $x^3 + x^2 + x - 2$ is irreducible, so this will give us a field with 125 elements. □

Problem 196 (Section 2.11, Exercise 6)**.** Show that $x^3 - x$ has 6 roots in $\mathbb{Z}/(6)$.

Proof. We have

$$\mathbb{Z}/(6) = \{0, 1, 2, 3, 4, 5\}.$$

Going through,

Number	Value of $x^3 - x$
0	0
1	0
2	0
3	0
4	0
5	0

so we have 6 roots.

Remark. If we weren't allowed to brute force, we would factor $x^3-x = x(x^2-1) = x(x+1)(x-1)$. Notice that for all $x \in \mathbb{Z}/(6)$, we have $x+1 = 0$, $x-1 = 0$, or some combination of $x, x+1, x-1$ gives us factors which are 2 and 3.

□

Problem 197 (Section 2.11, Exercise 8)**.** Show that the quaternion division ring $\mathbb{H}$ contains an infinite number of elements u satisfying $u^2 = -1$.

Proof. Recall that all the elements in $\mathbb{H}$ are of the form $a + bi + cj + dk$, $a, b, c, d \in \mathbb{R}$. We have then that

$$(a + bi + cj + dk)(a + bi + cj + dk) = -1$$

gives us the following system of equations;

$$a^2 - b^2 - c^2 - d^2 = -1,$$

$$2ab = 2ac = 2ad = 0.$$

Notice this forces $a = 0$, and so we have

$$b^2 + c^2 + d^2 = 1.$$

This corresponds to the unit sphere S^2 and so we have that there are infinitely many solutions. □

Problem 198 (Section 2.11, Exercise 9, 10)**.** Show that the ideal $(3, x^3 - x^2 + 2x - 1)$ in $\mathbb{Z}[x]$ is not principal.

Proof. If it were principle, we have a $f \in \mathbb{Z}[x]$ such that

$$(f) = (3, x^3 - x^2 + 2x - 1).$$

Notice that $(3) \subset (f)$, and so $f \mid 3$. Since 3 prime, this forces $f(x) = 3$ or $f(x) = \pm 1$. Hence, $(f) \subset (3, x^3 - x^2 + 2x - 1)$. In the other direction, we need to show that $x^3 - x^2 + 2x - 1 \in (3)$. However, for any polynomial p, we have that $3p$ will not be monic, since the coefficients are over $\mathbb{Z}$. Hence, there is no polynomial such that $x^3 - x^2 + 2x - 1 = 3p$, and so it cannot be principle.

Notice that it *is* a prime ideal (and in fact maximal). We have

$$\mathbb{Z}[x]/(3, x^3 - x^2 + 2x - 1) \cong \mathbb{F}_3[x]/(x^3 + 2x^2 + 2x + 2),$$

and since $x^3 + 2x^2 + 2x + 2$ has no roots in $\mathbb{F}_3$, we get it's irreducible, and hence this is a domain.

Remark. Notice how this contrasts **Theorem 2.15**; for a domain D which is a PID, we may not have $D[x]$ a PID.

□

Problem 199. Is $I = \{f \in \mathbb{R}[x, y] \ : \ f(1, 0) = f(0, 1) = 0\}$ a prime ideal?

Proof. Take $x, y \in \mathbb{R}[x, y]$. Then $f(x, y) = xy$ is such that $f(0, 1) = f(1, 0) = 0$, but neither x nor y are in I. So it is not a prime ideal. □

Problem 200 (Section 2.11, Exercise 11)**.** Let R be a ring without non-zero nilpotent elements. Prove that if $f(x) \in R[x]$ is a zero divisor, then there exists an element $a \neq 0$ in R such that $af(x) = 0$.

Proof. If $f(x)$ is a zero divisor, we have that there is a $g(x)$ such that

$$f(x) = a_0 + \cdots + a_n x^n,$$

$$g(x) = b_0 + \cdots + b_m x^m,$$

$$fg(x) = \sum_{i=0}^{nm} \left(\sum_{j+k=i} a_j b_k \right) x^i = 0$$

That is, for every $0 \leq i \leq nm$,

$$\sum_{j+k=i} a_j b_k = 0.$$

Notice that a_0 is a zero divisor. We then have that

$$a_1 b_0 + a_0 b_1 = 0.$$

Multiplying by b_0 throughout gives

$$a_1 b_0^2 + a_0 b_0 b_1 = 0.$$

Assume this pattern holds up to $n-1$. That is, $a_{n-1} b_0^n = 0$. Then we have that

$$a_n b_0 + a_{n-1} b_1 + \cdots + b_n a_0 = 0,$$

and multiplying by b_0^n throughout gives

$$a_n b_0^{n+1} = 0.$$

Hence, the pattern holds. Thus, we have that $b_0^{\deg(f)}$ is a non-zero element (since there are no non-zero nilpotent elements) such that

$$b_0^{\deg(f)} f = 0.$$

□

Problem 201 (Section 2.11, Exercise 12)**.** Let F be a field of q elements, $F^\times = \{a_1, \ldots, a_{q-1}\}$ the set of non-zero elements of F. Show that $a_1 \cdots a_{q-1} = -1$.

Proof. By **Theorem 2.18**, we have that $F^\times$ is cyclic. Let g be the generator. Then we have

$$a_1 \cdots a_{q-1} = g \cdots g^{q-1} = g^{q(q-1) - \frac{q(q-1)}{2}} = g^{\frac{q(q-1)}{2}}.$$

By Fermat's, we see that $g^q = g$. Hence, we get that this is equal to $g^{(q-1)/2}$. If q is odd, then $q-1$ is even, and so $(q-1)/2$ is an integer. So this is well-defined, and furthermore we have $q - 1/2 < q - 1$, so $g^{(q-1)/2} \neq 1$. Let $c = g^{(q-1)/2}$. We have that $c^2 - 1 = 0$. We can factor the polynomial $x^2 - 1$ in the field to get $x^2 - 1 = (x+1)(x-1)$. So it's only solutions are $x = -1, 1$. Since $c \neq 1$, we must have that $c = -1$, and so for q odd we get

$$a_1 \cdots a_{q-1} = -1.$$

If q is even, notice that it's characteristic is 2, so $1 = -1$. Notice that we can rewrite this as

$$\left(g^{(q-1)}\right)^{q/2} = g^{q/2}.$$

Moreover, we have that $g^{q/2}$ is a root of the polynomial $x^2 - x = 0$, which factors to be $x(x-1) = 0$. Since $g \neq 0$, we must have that $g^{q/2} = 1 = -1$. □

Problem 202 (Section 2.11, Exercise 13)**.** Prove Wilson's theorem: If p is a prime in $\mathbb{Z}$, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. Examine the field $\mathbb{Z}/p\mathbb{Z}$. We have that it's units are $\{1, \ldots, p-1\}$. By the prior problem, we have that $1 \cdots (p-1) = (p-1)! \equiv -1 \pmod{p}$. □

Problem 203 (Section 2.11, Exercise 16)**.** Let $f(x), g(x) \neq 0$ be elements of $F[x]$ with $\deg(g) = m$. Show that $f(x)$ can be written in one and only one way in the form

$$f(x) = a_0(x) + a_1(x)g(x) + \cdots + a_n(x)g(x)^n,$$

where $\deg(a_i(x)) < m$.

Proof. We use the division algorithm. First, let $\deg(f) = k$. Then we have that there exists q, r such that

$$k = qm + r,$$

where $0 \leq r < m$. Notice as well that $g(x)^q$ has degree $\deg(g^q) = qm$. Hence, using the division algorithm on f with g^q, we have that

$$f = g(x)^q a_q(x) + p(x),$$

where $\deg(a_q(x)) = r$, $\deg(p(x)) < \deg(g(x)^q) = qm$. Continuing down the line, we have that this algorithm terminates, with

$$f(x) = g(x)^q a_q(x) + \cdots + a_0(x),$$

where some $a_i(x)$ may be 0. The division algorithm gives uniqueness. □

Problem 204 (Section 2.12, Exercise 1)**.** Prove the following extension of **Theorem 2.19**: If $f(x_1, \ldots, x_r) \in F[x_1, \ldots, x_r]$, F infinite, and $f(a_1, \ldots, a_r) = 0$ for all $(a_1, \ldots, a_r)$ for which a second polynomial $g(x_1, \ldots, x_r) \neq 0$ has values $g(a_1, \ldots, a_r) \neq 0$, then

$$f(x_1, \ldots, x_r) = 0.$$

Proof. The way I understand this problem, this is an elaborate way of saying that f evaluates to 0 for all $a \in F^r$. In this case, $f \in \ker(\zeta)$, where $\zeta : F[x_1, \ldots, x_r] \to F[s_1, \ldots, s_r]$, and since F is infinite, this is an isomorphism, and so $f = 0$. It seems ill posed, however. □

Problem 205 (Section 2.12, Exercise 2)**.** Prove that every function in r variables over F is a polynomial function (here, $|F| = q$).

Proof. We first count the number of polynomials. Notice that there are q options for each variable, so it suffices to count the number of variables. For one variable, we have q possible variables, so the answer is q^q, which also gives the number of functions. For two variables, we consider the one variable case and think of $F[x, y] = F[x][y]$. That is, $f \in F[x, y]$ can be thought of as

$$f = A_0(x) + A_1(x)y + \cdots + A_n(x)y^n.$$

The degree only goes up to $q - 1$, so we have $(q^q)^q = q^{2q}$ polynomials over this field. Continuing inductively, we find for r variables we have $q^{(r-1)q}$ possible polynomials.

For functions, considering the one variable case, we have q^q possible functions. For the two variable case, we again get $(q^q)^q$ (the number of functions from a set M to a set N of size m, n respectively is m^n). For for r variables we look at $F \times \cdots \times F$ r-times into F, and so inductively we get $q^{(r-1)q}$ possible functions. Since the polynomials are a subset of the set of all functions, and they have equal size, we get that they are equal. □

Problem 206. Show that x_i are algebraic over $R[p_1, \ldots, p_r]$.

Proof. To show the x_i are algebraic, notice that

$$g(x) = (x - x_1) \cdots (x - x_r) = x^r - p_1 x^{r-1} + p_2 x^{r-2} - \cdots + (-1)^r p_r.$$

Notice as well that

$$g(x_i) = 0,$$

so

$$x_i^r - p_1 x_i^{r-1} + p_2 x_i^{r-2} - \cdots + (-1)^r p_r = 0.$$

Hence, they are algebraic. □

Problem 207. Show that

$$P(x) = x_1^3 + x_2^3 + x_3^2$$

is a symmetric polynomial, and write it in terms of the symmetric polynomials.

Throughout, let $s_1 = x_1 + x_2 + x_3$, $s_2 = x_1x_2 + x_1x_3 + x_2x_3$, $s_3 = x_1x_2x_3$.

Proof. Let $\pi \in S_3$. Then $\zeta(\pi)(x_1^3 + x_2^3 + x_3^3) = x_{\pi(1)}^3 + x_{\pi(2)}^3 + x_{\pi(3)}^3$. Since π is bijective, we see clearly that this is equal to $x_1^3 + x_2^3 + x_3^3$. Hence, it's invariant under permuting the variables.

Next, we try to calculate the representation. Using the monomial ordering, we notice that

$$x_1^3 + x_2^3 + x_3^3 - s_1^3 = -3x_1^2x_2 - 3x_1^2x_3 - 3x_1x_2^2 - 6x_1x_2x_3 - 3x_1x_3^2 - 3x_2^2x_3 - 3x_2x_3^2.$$

We add on $3s_1s_2$ to get

$$x_1^3 + x_2^3 + x_3^3 - s_1^3 + 3s_1s_2 = 3x_1x_2x_3.$$

Hence, we have

$$x_1^3 + x_2^3 + x_3^3 = s_1^3 - 3s_1s_2 + 3s_3.$$

□

Problem 208. Show that the symmetric polynomials are algebraically independent.

Proof. First, by definition, the x_i are algebraically independent. Next, assume we had some non-trivial relation

$$\sum_{(d)} \alpha_{(d)} s_1^{d_1} \cdots s_n^{d_n} = 0.$$

After factoring out, we see that we are left with non-trivial monomials of the form

$$\sum_{(d)} \beta_{(d)} x_1^{d_1} \cdots x_n^{d_n} = 0.$$

In particular, letting $k_i = d_1 + \cdots + d_i$, we have that there is a maximal non-trivial monomial

$$\beta_{(k)} x_1^{k_1} \cdots x_n^{k_n}.$$

We have that there is a non-trivial relation after cancelling relative terms, which contradicts the algebraic independence of the x_i. □

Remark. We define the following:

(1) We call b a factor of a if $b \mid a$; that is, there is a k such that $bk = a$.
(2) We call b a proper factor of a if $b \mid a$ and $a \nmid b$.
(3) We say a and b are associated if $a \mid b$ and $b \mid a$.
(4) We call an element b irreducible if it is not irreducible and has no proper factors other than units.
(5) We call an element b prime if $b \mid ac$ implies $b \mid a$ or $b \mid c$ (contrapositive: $b \nmid a$ and $b \nmid c$ implies $b \nmid ac$.
(6) The prime condition tells us that irreducible elements are prime.
(7) The divisor chain condition says that every chain of proper factors eventually terminates (in terms of associates).
(8) The gcd of two elements is the greatest d such that d divides both of them (greatest in this sense means that if t divides both, then t divides d).
(9) The gcd condition says that every two elements admit a gcd.

Problem 209 (Section 2.14, Exercise 1)**.** Show that if M is factorial, then $ab \sim [a, b](a, b)$ in M (recall $[a, b]$ is lcm and (a, b) is gcd).

Proof. Using the fact that it's a commutative ring and grouping, as well as throwing in irreducibles which divide b but not a and giving them 0 powers (and vice versa), we have

$$a = d_1^{e_1} \cdots d_n^{e_n},$$

where $e_i \geq 0$ and d_i primes. We have

$$b = d_1^{k_1} \cdots d_n^{d_n},$$

where $k_i \geq 0$ and d_i primes. Hence

$$ab = d_1^{e_1+k_1} \cdots d_n^{e_n+k_n}.$$

Notice that

$$(a, b) \sim d_1^{\min(e_1,k_1)} \cdots d_n^{\min(e_n,k_n)} = T$$

This clearly divides, so $(a, b) \mid T$, and we clearly have the other direction as well. So $T \sim (a, b)$. Similarly,

$$[a, b] \sim d_1^{\max(e_1,k_1)} \cdots d_n^{\max(e_1,k_1)}.$$

Since

$$ab = d_1^{\min(e_1,k_1)+\max(e_1,k_1)} \cdots d_n^{\min(e_n,k_n)+\max(e_1,k_1)},$$

we get $[a, b](a, b) \sim ab$. □

Problem 210 (Section 2.14, Exercise 2)**.** Let M be a commutative monoid with cancellation law.

(1) Show that the relation of associateness $\sim$ is a congruence relation.
(2) Let $\overline{M}$ be the corresponding quotient monoid, i.e. $\overline{M} = M/\sim$. Show that $\overline{M}$ satisfies the cancellation law, and that $\overline{1}$ is the only unit in $\overline{M}$.
(3) Show that M is factorial if and only if $\overline{M}$ is factorial.

Proof.

(1) To get that it's a congruence relation, we need $a \sim b$ and $c \sim d$ implies $a + c \sim b + d$ and $ac \sim bd$. Since $a \sim b$, there is a unit u such that $ua = b$ and likewise there is a unit t such that $tc = d$. So $b + d \mid ut(a + c)$, so $b + d \mid a + c$, and likewise we have $a + c \mid (ut)^{-1}(b + d)$, so $a + c \mid b + d$. Hence, $a + c \sim b + d$. Likewise, we have $ut(ac) = bd$, so $ac \sim bd$.
(2) Let $ab = ac$ in $\overline{M}$. Since we are in a congruence relation, this tells us that $ab - ac = 0$, or $a(b - c) = 0$. Since $a \neq 0$, this means $b = c$. So we have the cancellation law.

    The fact that 1 is the only unit derives from the fact that every unit is associated to 1.
(3) ($\implies$) If M is factorial, let $a \in M$. Then $a = b_1 \cdots b_n$, and where b_i are irreducible. Hence, we have that $\overline{a} = \overline{b_1} \cdots \overline{b_n}$. This is, in fact, unique, since we quotiented. Hence, $\overline{M}$ is factorial.

    ($\impliedby$) Assume $\overline{M}$ is factorial. Then $\overline{a} = \overline{b_1} \cdots \overline{b_n}$, where $\overline{b_i}$ are all irreducible. Since these are all associates, we have that they differ up to units. Hence, $a = \overline{b_1} \cdots \overline{b_n}$ after multiplying by appropriate units. We see this is (essentially) unique, since if we had another, it would also be a factorization in $\overline{M}$, and so must be the one given above (up to units, which get killed).

□

Problem 211 (Section 2.14, Exercise 3)**.** Show that $\mathbb{Z}[\sqrt{-5}]$ satisfies the divisor chain condition (abbreviated dcc).

Proof. Let $a \in \mathbb{Z}[\sqrt{-5}]$. Let $a_1 \mid a$, and for every $i \geq 1$, $a_{i+1} \mid a_i$. We wish to show that there is an n such that $a_n \sim a_{n+1} \sim \cdots$. To get this, we go by norms. Recall that if $a_1 \mid a$, we have $N(a_1) \mid N(a)$. Continuing down, we get a chain $\cdots N(a_2) \mid N(a_1) \mid N(a)$. Since $N(a_i) \in \mathbb{Z}$, we have that eventually there must be an n so that $N(a_n) \sim N(a_{n+1}) \sim \cdots$. If we show that $N(a) \sim N(b)$ and $a \mid b$ implies $a \sim b$, we are done. Notice $N(a) \sim N(b)$ is equivalent to $N(a) = N(b)$. Hence,

we see that $a \sim b$, and so we are done, since $a \mid b$ implies that there is a c such that $ca = b$, $N(ca) = N(b) = N(a)$ so $N(c) = 1$, a unit. $\square$

Problem 212 (Section 2.14, Exercise 4)**.** Show that $\mathbb{Z}[x]$ satisfies the dcc.

Proof. Let $f \in \mathbb{Z}[x]$, and take the chain f_i such that $\cdots f_2 \mid f_1 \mid f$. We would like to show that there exists an n such that $f_n \sim f_{n+1} \sim \cdots$. Notice the dcc also dictates that these are proper factors. Since $f_1 \mid f$, we have that $\deg(f_1) \leq \deg(f)$. Continuing down the line, we have that $\deg(f_i) \leq \deg(f_{i-1})$ (where $f_0 := f$) for all i. If $\deg(f_i) < \deg(f_{i-1})$, we are continue. If it decreases, we must eventually have that $f = 0, \pm 1$, since it will eventually become constant. Once we are one of these, we win. So it suffices to show that we will always have it's decreasing.

In essence, this boils down to showing that if $\deg(f) = \deg(g)$, and g is a proper factor, then there are only finitely many options for what g could be. Since we're getting a proper factor every time, we have that the selection is decreasing, and so eventually we must have that the degree drops.

To prove this claim, suppose $\deg(f) = \deg(g)$, $g \mid f$ but $f \nmid g$. We can write

$$f = a_0 + \cdots + a_n x^n,$$

$$g = b_0 + \cdots + b_n x^n,$$

and we require $a_n, b_n \neq 0$. If $g \mid f$, there is a polynomial p such that $pg = f$. Since their degrees are the same, though, the multiplicative property forces p to be a constant. Furthermore, it must be such that $b_i \mid a_i$ for all i, and so p must be this constant. Since the coefficients are in $\mathbb{Z}$, this gives us only finitely many options for what these could be, if there is an option. $\square$

Problem 213. If R is a PID, then R is a UFD.

Proof. Recall that R is a UFD if and only if it satisfies the gcd condition and the dcc (descending chain condition). Let's first establish the gcd condition.

Let $a, b \in R$. Then we have that $(a, b) = (d)$, since R is a PID. Notice that $(d) \subset (a, b)$, so this means that $d \in (a, b)$, so there are $r, s \in R$ such that $ra + sb = d$. Suppose $g \mid a$, $g \mid b$. Then there are e, f such that $gf = a$, $ge = b$, so

$$ra + sb = r(gf) + s(ge) = d \leftrightarrow g(rf + se) = d,$$

hence $g \mid d$. So d is the gcd of a and b, and it's unique up to units.

Next, suppose $\cdots a_3 \mid a_2 \mid a_1 \mid a$ be a chain of proper factors. Then this implies that $(a) \subset (a_1) \subset \cdots$. Let $I = \bigcup_{i=1}^{\infty}(a_i)$. This is an ideal, since this is an ascending chain of ideals. Hence, since R is a PID, we have $I = (e)$. Furthermore, we see that $e \in (a_i)$ for some i, since $e \in I$, and so we have that $(e) \subset (a_i)$. Since $(a_i) \subset (e)$ by assumption, we get $(e) = (a_i)$. Hence, we have that $a_{i+1} \mid a_i$, and $a_i \mid a_{i+1}$ since $(a_i) \cup (a_{i+1}) = (a_i)$, so $a_{i+1} \sim a_i$. Hence, the chain terminates eventually, and so we have the dcc condition.

Thus, R is a UFD. $\square$

Problem 214 (Section 2.15, Exercise 2)**.** Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain with respect to $\delta(m + n\sqrt{2}) = |m^2 - 2n^2|$.

Proof. Notice first that

$$\delta(ab) = \delta(a)\delta(b)$$

(this is just a routine calculation). Note that, for $a = m + n\sqrt{2}$, $b = r + s\sqrt{2}$, we have

$$\frac{a}{b} = \frac{m + n\sqrt{2}}{r + s\sqrt{2}} = \frac{(m + n\sqrt{2})(r - s\sqrt{2})}{r^2 - 2s^2} = \mu + \nu\sqrt{2},$$

where μ, ν are rational numbers. Choose ϵ, δ integers such that $|\epsilon - \mu| < 1/2$, $|\delta - \nu| < 1/2$. Let $u = \mu - \epsilon$, $v = \nu - \delta$, then $|u| < 1/2$, $|v| < 1/2$. Now, $u + \epsilon = \mu$, $v + \delta = \nu$, and so

$$a = b((u + \epsilon) + (v + \delta)\sqrt{2}) = bq + r,$$

where $q = \epsilon + \delta\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, $r = b(u + v\sqrt{2})$ $r = a - bq$, so $r \in \mathbb{Z}[\sqrt{2}]$. Notice as well that

$$\delta(b(u + v\sqrt{2})) = \delta(b)\delta(u + v\sqrt{2}),$$

$$\delta(u + v\sqrt{2}) = |u^2 - 2v^2| \leq |u|^2 + 2|v|^2 < 1,$$

so

$$\delta(r) < \delta(b)$$

as desired. □

Problem 215 (Section 2.15, Exercise 6)**.** Let D be a Euclidean domain whose function δ satisfies

(1) $\delta(ab) = \delta(a)\delta(b)$
(2) $\delta(a + b) \leq \max(\delta(a), \delta(b))$.

Show that either D is a field or $D = F[x]$, F a field, x an indeterminate.

Proof. TODO □

Problem 216 (Section 2.15, Exercise 12)**.** Apply the algorithm for finding the gcd to the foregoing polynomials:

$$x^3 + x^2 + x - 3$$
$$x^4 - x^3 + 3x^2 + x - 4$$

in $\mathbb{Q}[x]$.

Proof. We have the degree of the second polynomial is higher, so we write

$$x^4 - x^3 + 3x^2 + x - 4 = x(x^3 + x^2 + x - 3) + (-2x^3 + 2x^2 + 4x - 4),$$

$$x^3 + x^2 + x - 3 = -\frac{1}{2}(-2x^3 + 2x^2 + 4x - 4) + (2x^2 + 3x - 5),$$

$$-2x^3 + 2x^2 + 4x - 4 = -x(2x^2 + 3x - 5) + (5x^2 - x - 4),$$

$$2x^2 + 3x - 5 = \frac{2}{5}(5x^2 - x - 4) + \frac{1}{5}(17x - 17),$$

$$5x^2 - x - 4 = \frac{25}{17}x\left(\frac{17x}{5} - \frac{17}{5}\right) + (4x - 4),$$

$$\frac{17x}{5} - \frac{17}{5} = \frac{17}{20}(4x - 4).$$

Hence, the gcd of these two polynomials is $4x - 4$, or it's associated to $x - 1$. □

Problem 217 (Section 2.15, Exercise 17)**.** Define the Mobius function $\mu(n)$ of positive integers by the following rules:

(1) $\mu(1) = 1$;
(2) $\mu(n) = 0$ if n has a square factor;
(3) $\mu(n) = (-1)^s$ if $n = p_1 p_2 \cdots p_s$, p_i distinct primes.

Prove that μ is multiplicative in the sense that $\mu(n_1 n_2) = \mu(n_1)\mu(n_2)$ if $(n_1, n_2) = 1$. Also prove that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n \neq 1 \end{cases}.$$

Proof. Write $n_1 = p_1^{e_1} \cdots p_n^{e_n}$, $n_2 = q_1^{f_1} \cdots q_m^{f_m}$, $q_i \neq p_j$ for any i, j. If either $n_1, n_2 = 1$, then it's clear that it's multiplicative. If $e_i \geq 2$ or $f_i \geq 2$, then we see it's also multiplicative, since the result will be 0 either way. So it's dependent on the case where $e_i = 1$, $f_j = 1$ for all i, j. In this case, we see that $\mu(n_1 n_2) = (-1)^{m+n} = (-1)^n(-1)^m = \mu(n_1)\mu(n_2)$. So it's multiplicative.

Write $n = p_1^{e_1} \cdots p_n^{e_n}$. Then we have

$$\sum_{d|n} \mu(d)$$

ends up being the sum of all combinations of p_i, f_i, where $0 \leq f_i \leq e_i$. Since anything greater than 1 results in 0, we end up with

$$\sum_{d|n} \mu(d) = 1 + \binom{n}{1}(-1) + \binom{n}{2}(-1)^2 + \cdots + \binom{n}{n}(-1)^n.$$

Recall the binomial theorem gives

$$(1 + (-1))^n = \sum_{j=0}^{n} \binom{n}{j}(-1)^j,$$

so we have

$$\sum_{d|n} \mu(d) = (1 + (-1))^n,$$

where here n denotes the length of the prime factorization. The only element with no primes dividing it is 1, and so we have that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n \neq 1 \end{cases}.$$

□

Problem 218 (Section 2.15, Exercise 18)**.** Prove the Mobius inversion formula: if $f(n)$ is a function of positive integers with values in a ring, and

$$g(n) = \sum_{d|n} f(d),$$

then

$$f(n) = \sum_{d|n} \mu(n/d) g(d).$$

Proof. We can rewrite this as

$$\sum_{d|n} \mu(n/d) \left(\sum_{k|d} f(k) \right) = \sum_{k|n} f(k) \left(\sum_{k|d|n} \mu(n/d) \right)$$
$$= \sum_{k|n} f(k) \left(\sum_{t|m} \mu(m/t) \right),$$

where $t = d/k$, $m = n/k$. By the prior problem, this is non-zero (i.e. 1) if and only if $m = 1$, which means $n/k = 1$, which means $n = k$, so we have that this is equal to $f(n)$. □

Problem 219 (Section 2.15, Exercise 19)**.** Prove that if φ is the Euler φ-function, then

$$\varphi(n) = \sum_{d|n} \mu(n/d) d.$$

Proof. By the Mobius inversion formula, we have that

$$\varphi(n) = \sum_{d|n} \mu(n/d)g(d),$$

where

$$g(n) = \sum_{d|n} \varphi(d).$$

Let's first show it for $n = p^e$. We have that (defining $p^{-1} = 0$)

$$g(n) = \sum_{i=0}^{e} \varphi(p^i) = \sum_{i=0}^{e} (p^i - p^{i-1}) = p^e.$$

Now, assume that $n = p^e q^f$. Then

$$g(n) = \sum_{d|n} \varphi(d).$$

Each d will be of the form $p^a q^b$, $0 \leq a \leq e$, $0 \leq b \leq f$, and so we get

$$g(n) = \sum_{a=0}^{e} \sum_{b=0}^{f} \varphi(p^a q^b) = \sum_{a=0}^{e} \sum_{b=0}^{f} \varphi(p^a)\varphi(q^b) = \sum_{a=0}^{e} \sum_{b=0}^{f} (p^a - p^{a-1})(q^b - q^{b-1}) = p^e q^f = n.$$

Inducting like this gives the result. So, we have

$$g(n) = n,$$

and hence

$$\varphi(n) = \sum_{d|n} \mu(n/d)d.$$

□

Problem 220 (Section 2.16, Exercise 1)**.** Prove that if $f(x)$ is a monic polynomial with integer coefficients, then any rational root of $f(x)$ is an integer.

Proof. Let p/q be coprime numbers such that

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

evaluated at p/q is

$$f(p/q) = a_0 + a_1(p/q) + \cdots + (p/q)^n = 0.$$

Notice that this means

$$q^n f(p/q) = q^n a_0 + pq^{n-1} a_1 + \cdots + p^n = 0.$$

Notice this corresponds to

$$p^n + q(a_{n-1} + \cdots + q^{n-1} a_0) = 0,$$

so

$$-p^n = q(a_{n-1} + \cdots + q^{n-1} a_0).$$

So $q \mid -p^n$ or $q \mid p^n$. If $q \mid p^n$, this means $q \mid p$. This can only happen if $q = 1$, so that p/q is an integer. □

Problem 221 (Section 2.16, Exercise 5)**.** Suppose D is a domain which is not a field, then $D[x]$ is not a pid.

Proof. Assume for contradiction that $D[x]$ is a pid. Let $(x) \subset D[x]$ be an ideal. Since x is irreducible, then (x) is maximal. Hence, $D[x]/(x)$ is a field. However, $D[x]/(x) \cong D$. This is a contradiction, since we assumed that D is a domain which is not a field, and so we must have that $D[x]$ is not a pid. □

Problem 222. Let R be a finite commutative ring with 1. Show that every prime ideal is maximal.

Proof. We first show that every finite integral domain is a field. Let R be a finite integral domain and let $f_a : R \to R$ given by $f_a(x) = ax$, where $a \neq 0$. We first check that this is injective. Notice that if $f_a(x) = f_a(y)$, then we have that $ax = ay$, so $a(x - y) = 0$. Since $a \neq 0$, R an integral domain, this forces $x = y$. Hence, we have that it's injective, and since it's an injection from a set to itself, it must be surjective. In other words, a must be invertible. Since this is true of all $a \neq 0$, we get that R must be a field.

Now, take R a finite commutative ring with identity. Let $p \subset R$ be a prime ideal. We see that R/p is an integral domain which is finite, and hence it must be a field. But this then forces p to be a maximal ideal. □

Problem 223 (Section 3.2, Exercise 1)**.** Let M be a left R-module and let η be a homomorphism of a ring S into R. Show that M becomes a left S-module if we define $ax = \eta(a)(x)$ for $a \in S$, $x \in M$.

Proof. We still have that M is an abelian group, and so it suffices to show the four properties hold. That is,

$$\begin{gathered} a(x+y) = \eta(a)(x+y) = \eta(a)(x) + \eta(a)(y) = ax + ay, \\ (a+b)x = \eta(a+b)(x) = \eta(a)(x) + \eta(b)(x) = ax + bx. \\ (ab)x = \eta(ab)(x) = \eta(a)\eta(b)x = \eta(a)(\eta(b)x) = a(bx). \\ \eta(1)x = 1x = x. \end{gathered}$$

So M is a left S-module. □

Problem 224 (Section 3.2, Exercise 2)**.** Let M be a left R-module and let $B = \{b \in R \ : \ bx = 0 \text{ for all } x \in M\}$. Verify that B is an ideal in R. Show that if C is any ideal contained in B, then M becomes a left R/C module by defining $(a + C)x = ax$.

Proof. Let $a, b \in B$. Then $a - b \in B$, since $(a - b)x = ax - bx = 0 - 0 = 0$. So its an additive subgroup. Next, let $r \in R$. Then $(ra)x = r(ax) = r(0) = 0$, $(ar)x = a(rx) = 0$, so B is an ideal. Let $C \subset B$ be an ideal. Then for all $c \in C$, $ca = 0$. We need to show the four laws hold:

$$\begin{gathered} (a+b+C)x = (a+b)x = ax + bx = (a+C)x + (b+C)x, \\ (a+C)(x+y) = a(x+y) = ax + ay = (a+C)x + (a+C)y, \\ (ab+C)x = (ab)x = a(bx) = (a+C)((b+C)x), \\ (1+C)x = 1x = x. \end{gathered}$$

So M is a left R/C-module. □

Problem 225 (Section 3.2, Exercise 3)**.** Let M be a left R-module, S a subring of R. Show that M is a left S-module if we define bx, $b \in S$, $x \in M$ as given in M as a left R-module. In particular, the ring R can be regarded as a left S-module in this way.

Proof. This is clear by **Exercise 1**. □

Problem 226 (Section 3.2, Exercise 4)**.** Let $V = \mathbb{R}^{(n)}$ be the vector space of n-tuples of real numbers with the usual addition and multiplication by elements of $\mathbb{R}$. Let T be the linear transformations defined by

$$T(x_1, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1}).$$

Consider V as a left $\mathbb{R}[\lambda]$-module (i.e. $(a_n\lambda^n + \cdots + a_1\lambda + a_0) \cdot v = a_nT^n(v) + \cdots + a_1T(v) + a_0$), and determine

(1) λx,
(2) $(\lambda^2 + 2)x$,

(3) $(\lambda^{n-1} + \cdots + 1)x$.

What elements satisfy $(\lambda^2 - 1)x = 0$?

Proof. (1) Using the action, we have

$$\lambda \cdot (x_1, \ldots, x_n) = T(x_1, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1}).$$

(2) Using the action, we get

$$(\lambda^2 + 2) \cdot (x_1, \ldots, x_n) = T^2(x_1, \ldots, x_n) + 2 = (x_{n-1}, x_n, x_1, \ldots, x_{n-2}) + 2(x_1, \ldots, x_n).$$

(3) We have

$$T(x_1, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1}),$$
$$T^2(x_1, \ldots, x_n) = (x_{n-1}, x_n, x_1, \ldots, x_{n-2}),$$
$$\cdots$$
$$T^k(x_1, \ldots, x_n) = (x_{n-k+1}, x_{n-k+2}, \ldots, x_n, x_1, \ldots, x_{n-k}).$$

Hence,

$$(\lambda^{n-1} + \cdots + 1)x =$$
$$(x_2, x_3, \ldots, x_n, x_1) + (x_3, \ldots, x_n, x_1, x_2) + \cdots + (x_n, x_1, \ldots, x_{n-1}) + 1.$$

Finally, we see that

$$(\lambda^2 - 1) \cdot x = T^2(x_1, \ldots, x_n) - (x_1, \ldots, x_n) = (x_{n-1}, x_n, x_1, \ldots, x_{n-2}) - (x_1, \ldots, x_n)$$
$$= (x_{n-1} - x_1, x_n - x_2, x_1 - x_3, \ldots, x_{n-2} - x_n) = 0,$$

so the collection of elements with

$$x_{n-1} = x_1, x_n = x_2, x_i = x_{i+2} \text{ for } 1 \leq i \leq n-2.$$

□

Problem 227 (Section 3.2, Exercise 8)**.** Let M be a finite abelian group which is non-zero. Can M be made into a left $\mathbb{Q}$-module?

Proof. No; consider the case of $\mathbb{Z}/4\mathbb{Z}$. Then

$$0 = \frac{1}{4}(4(1)) = \left(\frac{1}{4} \cdot 4\right) 1 = 1,$$

a contradiction. □

Problem 228. Let R be a commutative ring, $I \subset R$ an ideal. Show that I is a left R-module, defined in the obvious way.

Proof. By definition, I is an abelian group under addition. Notice that we define $r \cdot a$ for $r \in R$, $a \in I$ via $ra \in I$, since I an ideal. We then need to show that distributive properties hold; but this is clear by the ring axioms. Hence, I is a left R-module. □

Problem 229 (Section 3.2, Exercise 6)**.** Let M be an abelian group written additively. Show that there is only one way in making M into a left $\mathbb{Z} - module$.

Proof. We first show existence, then uniqueness. Let $r \in \mathbb{Z}$, $a \in M$. Define $ra = a + a + \cdots + a$ r times. Then we see that

$$r(a + b) = (a + b) + \cdots + (a + b) = ra + rb,$$
$$(r + s)a = ra + sa,$$
$$r(sa) = r(a + \cdots + a) = sa + \cdots + sa = (rs)a,$$
$$1a = a.$$

So it's a left $\mathbb{Z}$-module. We then check uniqueness. Notice that any other way would be defined by $1a = a$, $(1+1)a = 1a + 1a = 2a$, and we can deduce from this that this holds for any integer n. Thus, it is unique. □

Problem 230 (Section 3.3, Exericse 1)**.** Determine $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/(n))$ and $\mathrm{Hom}(\mathbb{Z}/(n), \mathbb{Z})$, $n > 0$, as $\mathbb{Z}$-modules.

Proof. Let $\varphi \in \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/(n))$. We see that φ is determined entirely by where it sends generators. Since it's just Hom, and not isomorphisms, we get a homomorphism for each element of $\mathbb{Z}/(n)$. Moreover, each of these are distinct, so we get that

$$\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/(n)) \cong \mathbb{Z}/(n).$$

Now, for $\varphi \in \mathrm{Hom}(\mathbb{Z}/(n), \mathbb{Z})$, let's see what happens when we take an element and map it. Taking $\varphi(1) = z$, we see that

$$nz = n\varphi(1) = \varphi(n) = \varphi(0) = 0.$$

Since $\mathbb{Z}$ is an integral domain, this means that either n or z is zero. Thus, we must have that $z = 0$, since by assumption $n > 0$. So we get $\mathrm{Hom}(\mathbb{Z}/(n), \mathbb{Z}) = 0$. □

Problem 231. Determine $\mathrm{Hom}(\mathbb{Z}/(m), \mathbb{Z}/(n))$, $m, n > 0$ as $\mathbb{Z}$-modules.

Proof. We follow the same calculation as before. Taking $\varphi \in \mathrm{Hom}(\mathbb{Z}/(m), \mathbb{Z}/(n))$, we see that $\varphi(1) = z$ implies that $nz = 0$. So this means that $m \mid nz$. Hence, $nz = mk$. Letting $d = \gcd(m, n)$, $n' = n/d$, $m' = m/d$, we get $n'z = m'k$, so that $z = (m'k)/n'$. Notice this gives us d options for z, and so we have that

$$\mathrm{Hom}(\mathbb{Z}/(m), \mathbb{Z}/(n)) \cong \mathbb{Z}/(d).$$

□

Problem 232 (Section 3.3, Exercise 3)**.** Show that

$$\mathrm{Hom}(\mathbb{Z}^{(2)}, \mathbb{Z}) \cong (\mathbb{Z}^{(2)}, +, 0).$$

Proof. Follow the same procedure as before. Take $\varphi \in \mathrm{Hom}(\mathbb{Z}^{(2)}, \mathbb{Z})$, we see that it's determined by $\varphi(1,0)$ and $\varphi(0,1)$. Hence, consider the morphism $\psi : \mathbb{Z}^{(2)} \to \mathrm{Hom}(\mathbb{Z}^{(2)}, \mathbb{Z})$ by $\psi(a,b) = \varphi_{(a,b)}$, where $\varphi_{(a,b)}(1,0) = a$, $\varphi_{(a,b)}(0,1) = b$. The kernel of this mapping is going to be 0, so it's injective, and we see it surjects by the remark at the beginning. Moreover, it is a morphism, and so an isomorphism. □

Problem 233 (Section 3.3, Exercise 4)**.** Prove that for any R and R-module M, $\mathrm{Hom}(R, M) \cong (M, +, 0)$.

Proof. Define the map by $\psi : \mathrm{Hom}(R, M) \to M$ by $\psi(\varphi) = \varphi(1)$. We check this is a homomorphism;

$$\psi(\alpha + \beta) = (\alpha + \beta)(1) = \alpha(1) + \beta(1) = \psi(\alpha) + \psi(\beta).$$

We now check the module homomorphism condition: let $r \in R$, then we have

$$\psi(r\alpha) = (r\alpha)(1) = r\alpha(1) = r\psi(\alpha).$$

Hence, it's an R-module homomorphism. Now, notice that

$$\ker(\psi) = \{\alpha \in \mathrm{Hom}(R, M) \ : \ \alpha(1) = 0\}.$$

Notice that if $\alpha(1) = 0$, we have that α is the 0 map; taking any $r \in R$, we have

$$\alpha(r) = r\alpha(1) = r(0) = 0.$$

So the kernel is trivial, hence it's injective.

For surjectivity, for $m \in M$ define the morphism $\alpha : R \to M$ by $\alpha(1) = m$. We see this is a R-module homomorphism, since

$$\alpha(a+b) = \alpha((a+b)1) = (a+b)\alpha(1) = (a+b)m = am + bm = a\alpha(1) + b\alpha(1) = \alpha(a) + \alpha(b),$$

and for any $r \in R$ we have

$$\alpha(ra) = \alpha((ra)1) = (ra)\alpha(1) = (ra)m = r(am) = r(a\alpha(1)) = r(\alpha(a)).$$

So we have found an α such that $\psi(\alpha) = m$. Hence, it's an isomorphism. □

Problem 234. Let R be a commutative ring and let A, B, and M be R-modules. Show that

$$\mathrm{Hom}(A \times B, M) \cong \mathrm{Hom}(A, M) \times \mathrm{Hom}(B, M).$$

Proof. For notational simplicity, let $N = \mathrm{Hom}(A \times B, M)$, $N_1 = \mathrm{Hom}(A, M)$, $N_2 = \mathrm{Hom}(B, M)$. We want to construct a map $\psi : N_1 \times N_2 \to N$. Define it by

$$\psi((\alpha, \beta)) = (\alpha \times \beta) : A \times B \to M, \qquad (\alpha \times \beta)(a, b) = \alpha(a) + \beta(b).$$

We first check that its well-defined. Let $(\alpha, \beta) = (\gamma, \delta)$. Then

$$\psi((\alpha, \beta)) = (\alpha \times \beta),$$
$$\psi((\gamma, \delta)) = (\gamma \times \delta),$$
$$(\alpha \times \beta)(a, b) = \alpha(a) + \beta(b) = \gamma(a) + \delta(b) = (\gamma \times \delta)(a, b).$$

We check this is a homomorphism. Let $(\alpha, \beta), (\gamma, \delta) \in N_1 \times N_2$. Then

$$\psi((\alpha, \beta) + (\gamma, \delta)) = \psi((\alpha + \gamma, \beta + \delta)) = (\alpha + \gamma) \times (\beta + \delta),$$

and we see that

$$(\alpha+\gamma)\times(\beta+\delta)(a, b) = \alpha(a)+\gamma(a)+\beta(b)+\delta(b) = (\alpha(a)+\beta(b))+(\gamma(a)+\delta(b)) = (\alpha\times\beta)(a, b)+(\gamma\times\delta)(a, b),$$

so that

$$\psi((\alpha + \gamma, \beta + \delta)) = \psi((\alpha, \beta)) + \psi((\gamma, \delta)).$$

Let $r \in R$, then

$$\psi((r\alpha, r\beta)) = (r\alpha \times r\beta),$$

with

$$(r\alpha \times r\beta)(a, b) = r\alpha(a) + r\beta(b) = r(\alpha(a) + \beta(b)) = r\psi((\alpha, \beta)).$$

So it's an R-module homomorphism. We check that it's an isomorphism. Notice that the kernel is trivial, since it being the zero map means *both* maps must be zero. To see it's surjective, suppose $\alpha \in N$. Then we have $\alpha(\cdot, 0) = \phi_1 : A \to M$, $\alpha(0, \cdot) = \phi_2 : B \to M$, and $\phi_1 + \phi_2 = \alpha$. Then $\psi((\phi_1, \phi_2)) = \alpha$, and we have it's surjective. So it is an isomorphism. □

Problem 235.

Problem 236 (Section 3.3, Exercise 8)**.** A left (right) ideal I of R is called a *maximal* if $R \neq I$ and there exist no left (right) ideals I' such that $I \subsetneq I' \subsetneq R$. Show that a module M is irreducible if and only if $M \cong R/I$, where I is a maximal left ideal of R.

Proof. Recall that a module is irreducible if $M \neq 0$ and 0 and M are the only submodules of M.

($\Longrightarrow$) Assume that M is irreducible. By prior exercises, we see that $M = Dx$, $x \in M$, $x \neq 0$. Let $I = \mathrm{ann}(x)$. Then we see that this is a maximal ideal; we have $R/I \cong M$, take any other ideal I', and we see that $I \subsetneq I' \subsetneq R$ is impossible, since this would force a submodule to exist.

($\Longleftarrow$) Similar argument. □

Problem 237 (Section 3.3, Exercise 9)**.** Show that if M_1 and M_2 are irreducible modules, then any non-zero homomorphism of M_1 into M_2 is an isomorphism. Hence, show that if M is irreducible, then $\mathrm{End}_R(M)$ is a division ring.

Proof. Let $\varphi : M_1 \to M_2$ be an non-zero homomorphism. Then $\varphi(1) = a \in M_2$. Since M_2 is irreducible, it is cyclic, and this is a generator of M_2. In other words, we get that φ is surjective. If $\varphi(k) = 0$ for some $k \neq 0$, we have that k generates M_1, so φ is the zero map, a contradiction. Hence, φ must be injective as well, and so an isomorphism.

Any two non-zero maps compose into a non-zero map, so $\mathrm{End}_R(M)$ is a division ring, since there are no zero divisors. □

Problem 238 (Section 3.4, Exercise 1)**.** Let R be arbitrary, and let $(e_1, \ldots, e_n)$ be a base for $R^{(n)}$. Show that $(f_1, \ldots, f_m)$, $f_j = \sum_{j=1}^{n} a_{jj'} e_{j'}$ is a base for $R^{(m)}$ if and only if there exist an $n \times m$ matrix B such that $AB = 1_m$, $BA = 1_n$, where $A = (a_{ij})$m 1_m is the usual $m \times m$ unit matrix. Hence show that $R^{(m)} \cong R^{(n)}$ if and only if there exists $A \in M_{m,n}(R)$, $B \in M_{n,m}(R)$ such that $AB = 1_m$, $BA = 1_n$.

Proof. We mimic the proof of the noncommutative version to find the result.

($\implies$) Let M be a module such that M has a basis of n elements and a basis of m elements. Let $(e_1, \ldots, e_n)$ be one basis, and $(f_1, \ldots, f_m)$ be the other. Then we have that

$$f_j = \sum_{i=1}^{n} a_{ji} e_i,$$

$$e_k = \sum_{i=1}^{m} b_{ij} f_i.$$

Substituting it in both ways gives

$$f_j = \sum_{i,k=1}^{n,m} a_{ji} b_{ik} f_k,$$

$$e_k = \sum_{j,l=1}^{n,m} b_{kj} a_{jl} e_l.$$

Hence, we see that

$$\sum_{i,k=1}^{n,m} a_{ji} b_{ik} = \delta_{jk},$$

$$\sum_{j,l=1}^{n,m} b_{kj} a_{jl} = \delta_{kl}.$$

In other words, we have found a matrix B (using $B = (b_{ij})$) such that $AB = 1_m$, $BA = 1_n$.
($\impliedby$) If there exists a matrix, then we can create the basis clearly.

We can deduce the result in the same way as the commutative case. □

Problem 239 (Section 3.4, Exercise 2)**.** Let $\eta \in \mathrm{End}_R(R^{(n)})$ and let A be the matrix of η relative to the base $(e_1, \ldots, e_n)$. Let $f_i = \sum p_{ij} e_j$, where $P = (p_{ij}) \in \mathrm{GL}_n(R)$. Verify that the matrix of η relative to the base $(f_1, \ldots, f_n)$ is PAP^{-1}.

Proof. This follows by simply noting that $P(e_j) = f_j$, so $e_j = P^{-1}(f_j)$. Then we have that $\eta(e_j)$ corresponds to the jth column of A, and applying P to this and using linearity let's us expand it in terms of the f; in other words, we get the matrix corresponding to the basis of (f_j) relative to η. □

Problem 240 (Section 3.4, Exercise 4)**.** Let R be commutative. Show that if η is a surjective endomorphism of $R^{(n)}$, then η is bijective. Does the same hold if η is injective?

Proof. We have $\eta : R^{(n)} \to R^{(n)}$ is a surjective homomorphism. Notice that to be surjective, it must map basis elements to basis elements; hence, choosing $(e_1, \ldots, e_n)$ to be an ordered basis, we have $\eta(e_i) = f_i$, where $(f_1, \ldots, f_n)$ is also a basis. It suffices to show that the kernel is trivial; that is, $\ker(\eta) = \{x \ : \ \eta(x) = 0\} = 0$. Taking $x \in \ker(\eta)$, we notice that we can write it as

$$x = \sum a_i e_i,$$

and so

$$\eta(x) = \eta\left(\sum a_i e_i\right) = \sum a_i \eta(e_i) = \sum a_i f_i = 0.$$

Since $(f_1, \ldots, f_n)$ is a basis, we have that the a_i must all be 0. Hence, $x = 0$, so η is injective.

The same does not hold true if η is injective. Consider $\eta : \mathbb{Z} \to \mathbb{Z}$ via $\eta(x) = 2x$. It is injective but not surjective. □

Problem 241 (Section 3.4, Exercise 5)**.** Let R be commutative, and let M and N be R-modules. If $a \in R$, $\eta \in \mathrm{Hom}(M, N)$, define $a\eta$ by $(a\eta)(x) = a(\eta(x)) = \eta(ax)$. Show that $a\eta \in \mathrm{Hom}(M, N)$ and that the action of R on $\mathrm{Hom}(M, N)$ convertes the latter into an R-module. Show that $\mathrm{Hom}(R^{(m)}, R^{(n)})$ is free of rank mn.

Proof. We first show that $a\eta \in \mathrm{Hom}(M, N)$. It needs to be an R-module homomorphism between M and N. Notice that

$$(a\eta)(0) = \eta(a \cdot 0) = \eta(0) = 0,$$

since η is a homomorphism. Next, let $a, b \in M$. Then

$$(a\eta)(m + n) = \eta(a(m + n)) = \eta(am + an) = \eta(am) + \eta(an) = (a\eta)(m) + (a\eta)(n).$$

Finally, we need to show it commutes with the R-action. Let $r \in R$. Then

$$r(a\eta)(m) = r\eta(am) = \eta(ram) = \eta(arm) = (a\eta)(rm).$$

So this is indeed an R-module homomorphism.

We then need to check that this is an R-module. That is, we need to check the four axioms. Let $a, b \in R$, $\eta, \gamma \in \mathrm{Hom}(M, N)$, and take $m \in M$ arbitrary. Then we have

$$a(\eta + \gamma)(m) = (\eta + \gamma)(am) = \eta(am) + \gamma(am) = (a\eta)(m) + (a\gamma)(m),$$

so

$$a(\eta + \gamma) = a\eta + a\gamma.$$

Next, we check

$$(a + b)\eta(m) = \eta((a + b)m) = \eta(am + bm) = \eta(am) + \eta(bm) = (a\eta)(m) + (b\eta)(m),$$

so

$$(a + b)\eta = (a\eta) + (b\eta).$$

Next, we check

$$(ab)\eta(m) = \eta(abm) = \eta(b(am)) = b\eta(am) = a(b\eta(m)),$$

so

$$(ab)\eta = a(b\eta).$$

Finally, it's clear that

$$1\eta(m) = \eta(1m) = \eta(m),$$

so

$$1\eta = \eta.$$

Since the four axioms are satisfied, we have that $\mathrm{Hom}(M, N)$ is an R-module under this action.

Finally, we need to check that $\mathrm{Hom}(R^{(m)}, R^{(n)})$ is a free module of rank mn. Let $\{e_1, \ldots, e_m\}$ be a basis of $R^{(m)}$, $\{f_1, \ldots, f_n\}$ be a basis of $R^{(n)}$. Then define $f_{ij}(e_t) = \delta itw_j$, linear over R on

the basis. We first check that this is a homomorphism. Notice that $f_{ij}(0) = 0$ clearly. Next, let $a, b \in R^{(m)}$. We have

$$a = \sum_{c=1}^{m} t_c e_c,$$

$$b = \sum_{c=1}^{m} g_c e_c,$$

and so

$$f_{ij}(a) = f\left(\sum_{c=1}^{m} t_c e_c\right) = \sum_{i=1}^{m} t_c f_{ij}(e_c) = t_i w_j,$$

$$f_{ij}(b) = f\left(\sum_{c=1}^{m} g_c e_c\right) = \sum_{i=1}^{m} g_c f_{ij}(e_c) = g_i w_j,$$

and

$$f_{ij}(a+b) = f\left(\sum_{c=1}^{m} (t_c + g_c) e_c\right) = \sum_{i=1}^{m} (t_c + g_c) f_{ij}(e_c) = (t_c + g_c) w_j = t_c w_j + g_c w_j = f_{ij}(a) + f_{ij}(b),$$

so it is a homomorphism. We then check that it spans. Let $\eta \in \mathrm{Hom}(R^{(m)}, R^{(n)})$. Then we see that for all $1 \leq i \leq m$ we either have $\eta(e_i) = w_k$ for some $1 \leq k \leq n$ or $\eta(e_i) = 0$. In such a case, we have that $\eta(e_i) = f_{ik}(e_i)$. Going through, we get that η can be expressed as a sum of these, and we notice that the sum of these f_{ik} agree with η on all of M, so they are equal as functions. Hence, the f_{ik} span.

Next, we check that it does indeed form a basis; that is, it satisfies the uniqueness. Assume that we have

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} f_{ij} = 0.$$

Then we wish to show that $a_{ij} = 0$ for all i, j. Notice that this means for arbitrary $m \in M$ that

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} f_{ij}(m) = 0.$$

Taking $m = e_1$, we have

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} f_{ij}(e_i) = \sum_{j=1}^{n} a_{1j} f_{1j}(e_1) = \sum_{j=1}^{n} a_{1j} w_j = 0.$$

Since w_j is a basis, this forces $a_{1j} = 0$ for all j. Going through, we see that we can do this for each i, and this will force $a_{ij} = 0$ for all i for all j. Hence, we have the uniqueness, and so this is a base, and so we have that $\mathrm{Hom}(R^{(m)}, R^{(n)}$ is a free module of rank mn. □

Problem 242. Check the following claims:

(1) Let $M_1, \ldots, M_n$ be independent submodules of M. Put $N_1 = M_1 + \cdots + M_{r_1}$, $N_2 = M_{r+1} + \cdots + M_{r_1+r_2}$, etc. Then $N_1, \ldots$ are independent.

(2) Let $M_1, \ldots, M_n$ be independent, and suppose $M_i = M_{i1} \oplus M_{i2} \oplus \cdots \oplus M_{ir_1}$, $1 \leq i \leq n$, where the M_{ij} are submodules of M_i. Then the submodules $M_{i1}, \ldots, M_{1r_1}, M_{21}, \ldots, M_{2r_2}, \ldots, M_{n1}, \ldots, M_{nr_n}$ are independent.

Proof. (1) Recall that to be independent means that

$$M_i \cap \left(\sum_{j \neq i} M_j \right) = 0.$$

We see that

$$N_1 \cap \left(\sum_{i \neq 1} N_i \right) = 0,$$

since expanding gives

$$(M_1 + \cdots + M_{r_1}) \cap \left(\sum_{i > r_1} M_i \right) = \sum_{j=1}^{r_1} \left(M_j \cap \left(\sum_{i > r_1} M_i \right) \right) = 0,$$

since submodules of independent modules are independent.

(2) TODO (Same idea as above though).

□

Problem 243 (Section 3.5, Exercise 3)**.** Show that $\mathbb{Z}/(p^e)$, $e > 0$, regarded as a $\mathbb{Z}$ module is not a direct sum of any two non-zero submodules. Does the same hold for $\mathbb{Z}$? Does it hold for $\mathbb{Z}/(n)$ for any other positive integers n?

Proof. Assume we could, that is, we have

$$M_1 \oplus M_2 = \mathbb{Z}/(p^e).$$

Take $m_1 \in M_1$, $m_2 \in M_2$. Since we are in a field, we have that there are m_1', m_2' so that

$$1 = m_1 m_1' = m_2 m_2',$$

so $M_1 \cap M_2 \neq 0$.

Assume we could do it for $\mathbb{Z}$; that is, $\mathbb{Z} = M_1 \oplus M_2$. Take $m_1 \in M_1$, $m_2 \in M_2$. Let $d = \operatorname{lcm}(m_1, m_2)$. Again, we see that $am_1 = d = bm_2$, so $M_1 \cap M_2 \neq 0$.

Finally, it's possible for $\mathbb{Z}/(n)$, n not of the form p^e. Use fundamental theorem for finite abelian groups.

Remark. This problem is trivialized by a future result. We are showing that these modules are indecomposable.

□

Problem 244 (Section 3.5, Exercise 4)**.** Show that if $M = M_1 \oplus M_2$, then $M_1 \cong M/M_2$ and $M_2 \cong M/M_1$.

Proof. Define a map $\pi_1 : M \to M_1$ via $\pi_1(x, y) = x$. Notice that this map is surjective clearly, and notice as well that this is a module homomorphism; if $r \in R$, we have that

$$\pi_1(r(x, y)) = \pi_1((rx, ry)) = rx = r\pi_1((x, y)),$$

$$\pi_1((a, b) + (x, y)) = \pi_1((a + x, b + y)) = a + x = \pi_1((a, b)) + \pi_1((x, y)).$$

Notice as well that $\ker(\pi_1) = \{(x, y) \ : \ \pi_1(x, y) = 0\} = \{0\} \cap M_2$. Clearly, we have $M_2 \cong \{0\} \cap M_2$, so we get that $M/\ker(\pi_1) \cong M/M_2 \cong M_1$ by the isomorphism theorem. There is a symmetric argument for the other one. □

Problem 245 (Section 3.6, Exercise 1)**.** Find a base for the submodule of $\mathbb{Z}^{(3)}$ generated by $f_1 = (1, 0, -1)$, $f_2 = (2, -3, 1)$, $f_3 = (0, 3, 1)$ and $f_4 = (3, 1, 5)$.

Proof. We have

$$\begin{pmatrix} 1 & 0 & -1 \\ 2 & -3 & 1 \\ 0 & 3 & 1 \\ 3 & 1 & 5 \end{pmatrix}.$$

Row reducing gives

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

So the basis is the standard basis. □

Problem 246. Find a basis and the invariant factors for the submodule of $\mathbb{Z}^(3)$ generated by $x_1 = (1, 0, -1)$, $x_2 = (4, 3, -1)$, $x_3 = (0, 9, 3)$ and $x_4 = (3, 12, 3)$.

Proof. We first find the invariant factors. We set up the matrix again

$$\begin{pmatrix} 1 & 0 & -1 \\ 4 & -3 & -1 \\ 0 & 9 & 3 \\ 3 & 12 & 3 \end{pmatrix}.$$

Row reducing gives

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 3 & 3 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}.$$

So the basis is $\{(1, 0, -1), (0, 3, 3), (0, 0, 6)\}$. We get that the Smith form is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}.$$

□

Problem 247. Find the Smith normal form for the following matrix.

$$\begin{pmatrix} -2 & 0 & 10 \\ 0 & -3 & -4 \\ 1 & 2 & -1 \end{pmatrix}$$

Proof. Row reducing gives

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 4 & 0 \end{pmatrix}.$$

We then focus on the matrix

$$\begin{pmatrix} 1 & 2 \\ 4 & 0 \end{pmatrix}.$$

Row reducing gives

$$\begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}.$$

Hence, the Smith normal form is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 8 \end{pmatrix}.$$

□

Problem 248 (Section 3.7, Exercise 5)**.** Prove that if F is a field, then any matrix in $M_n(F)$ of determinant 1 is a product of elementary matrices of type I.

Proof. Recall that an elementary matrix of type I is a matrix of the form

$$T_{ij}(b) = 1 + be_{ij}.$$

First, we verify that this gives a matrix of determinant 1. But this is clear, since this is either an upper triangular or lower triangular matrix, and so the determinant is the product along the diagonal. Hence, we get that the determinant is 1. Notice that the multiplicative property of the determinant will give us that a product of type 1 matrices will have determinant 1.

We now take a matrix who's determinant is 1. We prove this by inducting on the size of the matrix. It's clear for a 1×1 matrix. Assume it holds for $n-1$. Then for an $n \times n$ matrix, using elementary matrices of type I, we can kill everything other than the element in the top left. Since the determinant is 1, we can rearrange so that 1 is in the top left. We then use the inductive hypothesis to get it for the $n-1 \times n-1$ inside matrix, and we're done. □

Problem 249 (Section 3.7, Exercise 6)**.** Let D be a pid, $a_i \in D$, $1 \leq i \leq n$. Let d be the gcd of the a_i. Show that there exists an invertible matrix $Q \in GL_n(D)$ such that

$$(a_1, \ldots, a_n)Q = (d, 0, \ldots, 0).$$

Proof. Notice that we can write the gcd as a sum of the a_i, that is, there exists $b_i \in D$ such that

$$\sum b_i a_i = d.$$

Hence, let (b_i) be the first column of Q. □

Problem 250 (Section 3.8, Exercise 1)**.** Determine the structure of $\mathbb{Z}^{(3)}/K$, where K is generated by $f_1 = (2, 1, -3)$, $f_2 = (1, -1, 2)$.

Proof. Let $M \cong \mathbb{Z}^{(3)}/K$. We have that $\mathbb{Z}^{(3)}$ has basis $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$. We wish to find a basis for our module M via the proof of the fundamental structure theorem. Notice that we have

$$f_1 = 2e_1 + e_2 + -3e_3,$$
$$f_2 = e_1 - e_2 + 2e_3,$$

so we have a relations matrix

$$A = \begin{pmatrix} 2 & 1 & -3 \\ 1 & -1 & 2 \end{pmatrix}.$$

We wish to row reduce this to it's normal form. Notice that it's normal form is

$$\begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & -3 \\ 1 & -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 1 \\ 2 & 0 & 7 \\ 1 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Hence, we have that there is a basis of e_1, e_2, e_3 such that the first two vectors are a basis of K. In other words, we get that $Z^{(3)}/K \cong \mathbb{Z}$. □

Problem 251 (Section 3.9, Exercise 1)**.** Let $D = \mathbb{R}[\lambda]$ and suppose M is a direct sum of cylic modules whose order ideals are generated by the polynomials $(x-1)^3, (x^2+1)^2, (x-1)(x^2+1)^4, (x+2)(x^2+1)^2$. Determine the elementary divisors and invariant factors of M.

Proof. The invariant factors are

$$\{(\lambda-1)^3,(\lambda-1),(\lambda^2+1)^2,(\lambda^2+1)^2,(\lambda^2+1)^4,(\lambda+2),(\lambda^2+1)^2.$$

This gives us elementary divisors

$$\begin{aligned} d_3 &= (\lambda-1)^3(\lambda^2+1)^4(\lambda+2),\\ d_2 &= (\lambda-1)(\lambda^2+1)^2,\\ d_1 &= (\lambda^2+1)^2. \end{aligned}$$

□

Problem 252 (Section 3.9, Exercise 3)**.** Define the rank of a finitely generated module M over a pid D to be the rank of the free module $M/\text{tor}(M)$. Show that if $M \cong D^{(n)}/K$, then rank of M is $n - \text{rank}(K)$. Show that if N is a submodule of M, then N and M/N are finitely generated and $\text{rank}(M) = \text{rank}(N) + \text{rank}(M/N)$.

Proof. Recall that the submodule of a free module is free. Hence, we have that $K \cong D^{(m)}$, where $m = \text{rank}(K)$, so $D^{(n)}/K \cong D^{(n-m)} \cong M$. Hence, rank of M is $n - m = n - \text{rank}(K)$.

If M is finitely generated, we have it is of the form $M \cong D^{(n)}/K$. Then any submodule $N \leq M$ will be of the form N'/K, where $N' \leq D^{(n)}$. Take $\pi : M \to M/N$ be the canonical surjection. Then we claim that if $x_1,\dots,x_n$ generate M, then $\pi(x_1),\dots,\pi(x_n)$ generate M/N. Take $y \in M/N$, then y is of the form $\pi(x)$ for some $x \in M$, and so

$$\pi(x) = \pi\left(\sum a_i x_i\right) = \sum a_i \pi(x_i) = \pi(y).$$

Hence, they span M/N, so M/N is finitely generated.

A rank nullity argument gives us the desired result here; that is, use the exactness of $0 \to N \to M \to M/N \to 0$, the fact that it descends to both the torsion and free parts, and then use the fact that the free part of M is a direct sum of the free parts of the other two. □

Problem 253 (Section 3.9, Exercise 4)**.** Let M be a torsion module for the pid D with invariant factor ideals $(d_s) \subset \cdots \subset (d_2) \subset (d_1)$. Show that any homomorphic image $\overline{M}$ of M is a torsion module. Show that the invariant factor ideals for the homomorphic image $(\overline{d}_t) \subset \cdots \subset (\overline{d}_1)$ satisfies $t \leq s$, $\overline{d}_t \mid d_s,\dots,\overline{d}_1 \mid d_{s-t+1}$.

Proof. We first work with the case that M is primary. Let $\varphi : M \to N$, $M = Dx$, $\text{ann}(x) = (d) \neq 0$. Then we see that $\varphi(Dx) = D\varphi(x) = \overline{M}$ is the homomorphic image of M. We check that this is torsion. Notice that $d\varphi(x) = \varphi(dx) = \varphi(0) = 0$, so $(d) \subset \text{ann}(x) = (d')$. In other words, $d' \mid d$. Note that it may be possible that the homomorphic image is 0, in which case we simply write $\overline{M} = 0$.

For the general case, let $M = Dx_1 \oplus \cdots \oplus Dx_r$. Examine $M/(Dx_1 \oplus \cdots \oplus Dx_{r-1}) \cong Dx_r$. Taking the homomorphic image of this gives us $\overline{M}/\overline{Dx_1 \oplus \cdots \oplus Dx_{r-1}} \cong D\overline{x_r}$. By the primary case, we see that inducting gives us the desired result. □

Problem 254 (Section 3.9, Exercise 7)**.** Call a submodule of N pure if, for any $y \in N$, $a \in D$, $ax = y$ is solvable in M (that is, there exists an $x \in M$ such that $ax = y$) if and only if $ax = y$ is solvable in N. Show that if N is a direct summand, then N is pure (here, direct summand means that $M = N \oplus L$). Show that if N is a pure submodule of M and $\text{ann}(x + N) = (d)$, then x can be chosen in its coset $x + N$ so that $\text{ann}(x) = (d)$.

Proof. Fix $a \in D$, $y \in N$ so that there is a $x \in M$ such that $ax = y$. Since N is a direct summand of M, we have $M = N \oplus L$. Let $\pi : M \to N$ be the canonical surjection. TODO □

Problem 255 (Section 3.10, Exercise 1)**.** Determine the number of non-isomorphic abelian groups of order 360.

Proof. We have

$$360 = 3^2 \cdot 5 \cdot 2^3.$$

These are given by

$$C_3 \times C_3 \times C_5 \times C_2 \times C_2 \times C_2,$$
$$C_3 \times C_3 \times C_5 \times C_4 \times C_2,$$
$$C_3 \times C_3 \times C_5 \times C_8,$$
$$C_9 \times C_5 \times C_2 \times C_2 \times C_2,$$
$$C_9 \times C_5 \times C_4 \times C_2,$$
$$C_9 \times C_5 \times C_8,$$

so in total 6. □

Problem 256 (Section 3.10, Exercise 4)**.** Verify that the characteristic polynomial of

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & -2 & 0 & 1 \\ -2 & 0 & -1 & -2 \end{pmatrix}$$

is a product of linear factors in $\mathbb{Q}[\lambda]$. Determine the rational and Jordan canonical forms for A in $M_4(\mathbb{Q})$.

Proof. We solve

$$\det(\lambda 1 - A) = (\lambda - 1)^2((\lambda(\lambda + 2) + 1 = (\lambda - 1)^2(\lambda^2 + 2\lambda + 1) = (\lambda - 1)^2(\lambda + 1)^2.$$

So it is a product of linear factors. We want to find the minimal polynomial then. We have $m(\lambda) = (\lambda-1)(\lambda+1)^2$. So the invariant factors are $(\lambda-1), (\lambda-1)(\lambda+1)^2$. The Rational Canonical form is then

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix},$$

with Jordan canonical form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

□

Problem 257 (Section 3.10, Exercise 5)**.** Prove that if F is a field, the matrices $A, B \in M_n(F)$ are similar if and only if the matrices $\lambda 1 - A$, $\lambda 1 - B$ are equivalent in $M_n(F[\lambda])$.

Proof. Recall two matrices A and B are similar if there exists a $P \in \mathrm{GL}_n(F)$ so that

$$PAP^{-1} = B.$$

Recall that two matrices are equivalent if there exists $P, Q \in \mathrm{GL}_n(F)$ so that

$$PAQ^{-1} = B.$$

($\implies$) If A and B are similar, then we have

$$PAP^{-1} = B,$$

so

$$P(\lambda 1 - A)P^{-1} = (PP^{-1})\lambda 1 - PAP^{-1} = \lambda 1 - B,$$

hence they are equivalent.
$(\Longleftarrow)$ □

Problem 258 (Section 3.10, Exercise 6)**.** Prove that any matrix A is similar to its transpose A^t.

Proof. Look at the Jordan form of a matrix. We have that the Jordan blocks are similar, and so letting J denote the Jordan form of A, we have

$$PAP^{-1} = J \sim J^t = (P^{-1})^t A^t P^t.$$

□

Problem 259 (Section 3.10, Exercise 10)**.** Show that $A^2 = A$, then A is similar to the matrix $\text{diag}(1, \dots, 1, 0, \dots, 0)$.

Proof. By the results of Cayley-Hamilton, we get that $m(\lambda) \mid \lambda^2 - \lambda = \lambda(\lambda - 1)$. Hence, the minimal polynomial divides $\lambda^2 - \lambda$, it has distinct roots, and so the matrix is similar to $\text{diag}(1, \dots, 1, 0, \dots, 0)$ per earlier exercises. □

Problem 260 (Section 4.6, Exercise 1)**.** Show that an abelian group has a composition series iff it is finite.

Proof. We need to first prove another problem.

Problem 261. Let G be an abelian simple group. Prove that G is finite and $|G| = p$ for some prime p.

Proof. We have that every subgroup of G is a normal subgroup. Let $g \in G$, $g \neq e$, then $\langle g \rangle \neq e$ is a subgroup, and since G is simple we have that $G = \langle g \rangle$. Hence, G is cyclic. Now, we have $\langle g^2 \rangle$ is another subgroup, and either it's trivial or G. If $g^2 = 1$, then $|G| = 2$. Otherwise, we have $\langle g^2 \rangle = G$, so $g = g^{2n}$, so $g^{2n-1} = e$ and $|G|$ is finite. Let p be a prime dividing $|G|$, then we have that $g^{|G|/p} = x$ is such that x has order p. Since $\langle x \rangle = G$, we get that $|G| = p$. □

$(\Longrightarrow)$ Assume that G is infinite and abelian, and assume that it has a composition series. We have then

$$1 = G_s \trianglelefteq G_{s-1} \trianglelefteq \cdots \trianglelefteq G_1 = G.$$

Then we have G_i/G_{i-1} is an abelian simple group, and so by the exercise we get that it's of order prime p. Hence, we get that $|G|$ is finite, a contradiction.
$(\Longleftarrow)$ Any finite group admits a composition series. □

Problem 262 (Section 4.6, Exercise 2)**.** Let G be cyclic of order n, finite. Let $G = G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_{s+1} = 1$ be a composition series. Put $|G_i| = n_i$. Show that $p_i = n_i/n_{i+1}$ is prime. Conversely, show that if $n = n_1, n_2, \dots, n_{s+1} = 1$ is a sequence of integers such that n_i/n_{i+1} is a prime, then we have a composition series for which $|G_i| = n_i$. Use this result to deduce the fundamental theorem of arithmetic for $\mathbb{Z}$.

Proof. **Step 1:** We have $|G_i/G_{i+1}| = |G_i|/|G_{i+1}| = p_i$. We have that p_i is a power of a prime, say p^n, $n \geq 1$. We need to show that $n = 1$. Assume that $n \geq 2$, then we have that $|G_i/G_{i+1}| = p^n$. Then we can find a normal subgroup of order p^k, $k \leq n$, and so we have that G_{i+1} is not maximal, contradicting our assumption of this being a composition series. So, we must have that $p_i = p$, where p is a prime.
Step 2: Every cyclic subgroup of order n is isomorphic, and using the fact that we can always find a composition series for a group G, we can use Jordan Holder to get that we will always have the factors n_i up to permuting them around. So we have the desired result.
Step 3: Examine the cyclic group $G = \mathbb{Z}_n$. We have that $|G_s| = p_1$, where p_1 is a prime. Continuing, $G_{s-1} = p_1 p_2$, where p_2 is a prime (using **Step 1**). Continuing down to G, we have that

$|G| = p_1 \cdots p_s$. By **Step 2**, the choice of these primes is unique (any other composition series will also result in the same primes), and so we have $n = p_1 \cdots p_s$. This tells us that every integer factors (uniquely up to rearrangement) into a product of primes, giving us the fundamental theorem of arithmetic. □

Problem 263 (Section 4.6, Exercise 8)**.** Prove that if H is a proper subgroup of a nilpotent group, then the normalizer $H \subsetneq N(H)$.

Proof. We have $H \subset N(H)$, so it suffices to show $x \in N(H)$ such that $x \notin H$. Since H is proper, G nilpotent, we have that there is a k such that $G^{k+1} \subset H$ and $H \subset G^k$. Take $x \in G^k - H$. Then we have, for all $y \in H$, $(x, y) \in G^{k+1} \subset H$. But this implies that $(x, y) \in H$. Since $y \in H$, this tells us that $xyx^{-1} \in H$, which implies $x \in N(H)$. □

Problem 264. Let G be a group and K a normal subgroup of G. Show that G has a composition series if and only if both K and G/K have composition series.

Proof. ($\implies$) Assume G has a composition series. Then we have

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{s+1} = 1,$$

where these are maximal normal subgroups. Hence, $K \leq G_1$. □

Problem 265. Show that

$$U \subset U^{\perp R \perp L},$$
$$U \subset U^{\perp L \perp R}.$$

Proof. First, notice that

$$U^{\perp R \perp L} = \{x \in V \ : \ B(x, y) = 0 \text{ for all } y \in U^{\perp R}\}.$$

By definition,

$$U^{\perp R} = \{y \in V \ : \ B(x, y) = 0 \text{ for all } y \in U\},$$

so we have that if $x \in U$, then for all $y \in U^{\perp R}$, $B(x, y) = 0$, so $x \in U^{\perp R \perp L}$. Hence, $U \subset U^{\perp R \perp L}$. The same goes for the other direction. □

Problem 266. If $U_1 \subset U_2$ for subspaces U_1 and U_2, then

$$U_2^{\perp L} \subset U_1^{\perp L},$$
$$U_2^{\perp R} \subset U_1^{\perp R}.$$

Proof. Let $x \in U_2^{\perp L} = \{x \in V \ : \ B(x, y) = 0 \text{ for all } y \in U_2\}$. In particular, if $B(x, y) = 0$ for all $y \in U_2$, then this means that $B(x, y) = 0$ for all $y \in U_1 \subset U_2$, so we have $x \in U_1^{\perp L}$. Hence, $U_2^{\perp L} \subset U_1^{\perp L}$. The argument is analogous for $\perp R$. □

Problem 267 (Section 6.1, Exercise 1)**.** Show that if B is any bilinear form on V, then

$$(U_1 + U_2)^{\perp L} = U_1^{\perp L} \cap U_2^{\perp L},$$

and

$$(U_1 + U_2)^{\perp R} = U_1^{\perp R} \cap U_2^{\perp R}$$

for any two subspaces U_1, U_2. Show also that if B is non-degenerate, then

$$(U_1 \cap U_2)^{\perp L} = U_1^{\perp L} + U_2^{\perp L},$$
$$(U_1 \cap U_2)^{\perp R} = U_1^{\perp R} + U_2^{\perp R},$$

Proof. By definition,

$$(U_1 + U_2)^{\perp L} = \{x \in V \ : \ B(x, y) = 0 \text{ for all } y \in U_1 + U_2\}.$$

Since these are subspaces, we see immediately by restricting to elements in U_1 or U_2 that

$$(U_1 + U_2)^{\perp L} \subset U_1^{\perp L},$$
$$(U_1 + U_2)^{\perp L} \subset U_2^{\perp L},$$

so

$$(U_1 + U_2)^{\perp L} \subset U_1^{\perp L} \cap U_2^{\perp L}.$$

For the other direction, we have

$$U_1^{\perp L} \cap U_2^{\perp L} = \{x \in V \ : \ B(x, y) = 0 \text{ for all } y \in U_1 \text{ and for all } y \in U_2\}.$$

So taking $x \in U_1^{\perp L} \cap U_2^{\perp L}$, $y \in U_1 + U_2$, we get that $y = z_1 + z_2$, $z_1 \in U_1$, $z_2 \in U_2$, so $B(x, y) = B(x, z_1 + z_2) = B(x, z_1) + B(x, z_2) = 0 + 0 = 0$. Hence, $B(x, y) = 0$ for all $y \in U_1 + U_2$, and so $x \in (U_1 + U_2)^{\perp L}$. We have equality.

The argument is the same for R instead of L.

Now assume that B is non-degenerate. Since B is non-degenerate, we have

$$U^{\perp L \perp R} = U^{\perp R \perp L} = U$$

for all subspaces U. Hence, using the prior result, we have

$$(U_1^{\perp L} + U_2^{\perp L})^{\perp R} = U_1^{\perp L \perp R} \cap U_2^{\perp L \perp R} = U_1 \cap U_2,$$

so taking $\perp L$ of both sides gives

$$(U_1^{\perp L} + U_2^{\perp L}) = (U_1 \cap U_2)^{\perp L}.$$

It's a similar argument for $\perp R$. □

Problem 268 (Section 6.1, Exercise 2)**.** Let B be an arbitrary bilinear form on V and assume U is a subspace such that the restriction of B to U is non-degenerate. Show that $V = U \oplus U^{\perp L}$.

Proof. Let $T : U \to U^*$ be the map defined by $T(x) = x_L = B(x, \cdot)$. This is surjective, and so extending this in the obvious way to all of V, we get that this is a surjective map onto U^*. Notice that

$$\ker(\hat{T}) = \{x \in V \ : \ \hat{T}(x) = 0\} = \{x \in V \ : \ B(x, y) = 0 \text{ for all } y \in U\} = U^{\perp L}.$$

Hence, taking the natural injection $U \hookrightarrow V$ and using the fact that $U \cong U^*$ by T, we have

$$0 \to U \to V \to U^{\perp L} \to 0$$

is an exact sequence, and so we get

$$V = U \oplus U^{\perp L}$$

□

Problem 269. Let F be a field of characteristic 2. Show that $F^2 = \{a^2 \ : \ a \in F\} \subset F$ is a subfield.

Proof. Let $a^2, b^2 \in F^2$. We have

$$a^2 + b^2 = (a + b)^2 \in F^2.$$

Notice that for all $a^2 \in F^2$, we have $-a^2 \in F^2$. Furthermore, $0^2 = 0$, so $0 \in F^2$. Next, take $a^2, b^2 \in F^2$. We have

$$a^2 \cdot b^2 = (ab)^2 \in F^2.$$

For all $a^2 \in F^2$, we have $(a^{-1})^2 \in F^2$. Furthermore, $1^2 = 1$, so $1 \in F^2$. Inheriting the commutativity from F, we have that this is a subfield. □

Remark. We implicitly used the Freshman dream, which states that

$$(a+b)^2 = a^2 + b^2$$

so long as the characteristic of the field is 2.

Problem 270. Let V be a vector space over $\mathbb{C}$. Suppose $v_1, \ldots, v_r$ are linearly independent vectors of V, and let $w \in \bigwedge^p(V)$. Prove that w is expressible as $w = \sum_1^r v_i \wedge \psi_i$ for some $\psi_1, \ldots, \psi_r \in \bigwedge^{p-1}(V)$ iff $v_1 \wedge \cdots \wedge v_r \wedge w = 0$.

Proof. ($\Longrightarrow$) Assume w is expressible as $\sum_1^r v_i \wedge \psi_i$. Then we have that

$$\begin{aligned} v_1 \wedge \cdots \wedge v_r \wedge w &= v_1 \wedge \cdots \wedge v_r \wedge \left(\sum_1^r v_i \wedge \psi_i \right) \\ &= \sum_1^r v_1 \wedge \cdots \wedge v_r \wedge v_i \wedge \psi_i = 0 \end{aligned}$$

by properties of the wedge product.
($\Longleftarrow$) Since $w \in \bigwedge^p(V)$, we have that it can be written as

$$w = \sum_1^n a_i(\alpha_{i_1} \wedge \cdots \wedge \alpha_{i_p}).$$

Furthermore,

$$\begin{aligned} & v_1 \wedge \cdots \wedge v_r \wedge w \\ &= v_1 \wedge \cdots \wedge v_r \wedge \left(\sum_1^n a_i(\alpha_{i_1} \wedge \cdots \wedge \alpha_{i_p}) \right) \\ &= \sum_1^n a_i v_1 \wedge \cdots \wedge v_r \wedge \alpha_{i_1} \wedge \cdots \wedge \alpha_{i_p} = 0. \end{aligned}$$

We see this can happen if and only if v_i is among the α_{i_j} for all i, and so we have the representation desired. $\square$

James Marshall Reber, ID: 500409166 Math 6111, Homework Misc 2: Data not in Jacobson

---

We define a ring to be Noetherian if it satisfies the **ascending chain condition**; that is, if we have a chain of ideals

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots,$$

then there exists an N such that, for all $n \geq N$, we have

$$I_N = I_n.$$

In other words, the chain eventually terminates/stabilizes.

For the most part, we consider Noetherian rings to be commutative rings. For non-commutative rings, place the appropriate adjectives for left and right ideals for left and right Noetherian.

Problem 271. A ring R is Noetherian if and only if all of it's ideals are finitely generated.

Proof. ($\implies$): Assume R is Noetherian; that is, it satisfies the ascending chain condition. Let $I \subset R$ be an ideal; we wish to show that it's finitely generated. Take $0 \neq x_1 \in I$, and examine $(x_1) \subset I$. If $I = (x_1)$, we are done; otherwise, we have that $I - (x) \neq \varnothing$. Take $x_2 \in I - (x_1)$ and examine the ideal $(x_1, x_2) \subset I$. If $I = (x_1, x_2)$, then we win; otherwise, there exists an $x_3 \in I - (x_1, x_2)$. Continue the process. Doing so gives us a chain of ideals:

$$(x_1) \subset (x_1, x_2) \subset \cdots$$

Since we have the ascending chain condition, there exists an n such that $(x_1, \ldots, x_n) = (x_1, \ldots, x_n, x_{n+1})$. In other words, $x_{n+1} \in (x_1, \ldots, x_n)$, and so we have that $I - (x_1, \ldots, x_n) = \varnothing$; that is, I is finitely generated.

($\impliedby$) Assume all ideals are finitely generated. Take a chain

$$I_1 \subset I_2 \subset \cdots.$$

Notice that $I = \bigcup I_n$ is an ideal, and hence finitely generated; that is, we have $I = (x_1, \ldots, x_n)$. Notice that $x_i \in \bigcup I_n$, so there exists an N sufficiently large so that $x_i \in I_N$ for all i. In other words, we have that $I = I_N$, and so we have that the chain stabilizes. □

So we can equivalently say that a Noetherian ring is one where all the ideals are finitely generated.

Problem 272 (Hilbert Basis Theorem)**.** Let R be a Noetherian ring. Then $R[x]$ is Noetherian as well.

Proof. By the equivalence above, it suffices to show that every ideal in $R[x]$ is finitely generated. Let $J \subset R[x]$ be an ideal. Let m be the least degree of a non-zero polynomial in J. For $n \geq m$, define

$$I_n = \{a \in R \ : \ a \text{ is the leading coefficient of an nth degree polynomial in J}\} \cup \{0\}.$$

We first check that the I_n are ideals. Let $a, b \in I_n$. We need to check that $a + b \in I_n$, $-a \in I_n$, and $0 \in I_n$. The latter is clear by construction. Notice that if a is the leading coefficient of an nth degree polynomial in J, we have that

$$ax^n + a_{n-1}x^{n-1} + \cdots + a_0 \in J,$$

and likewise

$$bx^n + b_{n-1}x^{n-1} + \cdots + b_0 \in J.$$

Adding these together gives

$$(a+b)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0) \in J,$$

since J is an ideal, and so $a+b \in J$. Likewise, multiplying the first polynomial by (-1) gives a polynomial in J with leading coefficient -1, using the fact that J is an ideal again. Hence, we have that I_n is a subgroup under addition.

Now, let $r \in R$. We have that

$$r(ax^n + a_{n-1}x^{n-1} + \cdots + a_0) = rax^n + \cdots + ra_0 \in J,$$

so $ra \in I_n$, and likewise for ar. Hence, I_n is an ideal.

Notice as well that $I_n \subset I_{n+1}$. Taking $a \in I_n$, we can multiply the polynomial by x to get a polynomial in J again, and so $a \in I_{n+1}$. Thus, we have a chain of ideals

$$I_1 \subset I_2 \subset \cdots,$$

and these are in R. Since R is Noetherian, there exists an N so that $I_n = I_N$ for all $n \geq N$.

Notice as well that the I_n are finitely generated. For each $m \leq n \leq N$, let A_n be a finite set of polynomials of degree n so that the leading coefficients generate I_n. Let $A = \bigcup A_n$. Then this, too, is a finite set. We will show that A generates J.

Let $p \in J$. If $\deg(p) = m$, then there are $q_i \in A_m$ and $a_i \in R$ so that the leading coefficient of p coincides with the leading coefficient of $\sum a_i q_i$. Hence, $p_i - \sum a_i q_i$ has degree strictly smaller than m, but this implies that it must be 0. So we have that $p \in (A)$.

Assume that for all $m \leq j \leq n-1$, we have that $p \in J$ with $\deg(p) = j$ is generated by elements in A. We will then check it for $k = n$. Let $p \in J$ be such that $\deg(p) = n$. If $n \leq N$, then we have that there are polynomials of degree n, $q_i \in (A)$ and $a_i \in R$, so that the leading coefficient of p is the leading coefficient of $\sum q_i a_i$. Hence, $p - \sum a_i q_i$ has degree less than n, and so by the induction hypothesis we can write this polynomial as a sum of elements in (A).

If $n > N$, then we can find polynomials with degree $n-1$, q_i in J and $a_i \in R$, so that the leading coefficient of p agrees with $\sum q_i a_i$. Hence, $p - x\sum a_i q_i$ has degree less than n, and so applying the induction hypothesis to the q_i and to $p - x\sum a_i q_i$, we get that $p \in (A)$. Hence, J is finitely generated. Since J was chosen arbitrarily, we get that $R[x]$ is Noetherian. $\square$

Notice that by induction, if R is Noetherian, so is $R[x_1, \ldots, x_n]$.

We define a *left module over* R ${}_RM$ to be an abelian group (written additively) such that we have

$$\begin{aligned} a(x+y) &= ax + ay, \\ (a+b)x &= ax + bx, \\ a(bx) &= (ab)x, \\ 1x &= x, \end{aligned}$$

where $a, b \in R$, $x \in M$.

Analogously, we define a *right module over* R M_R to be an abelian group (written additively) such that we have

$$\begin{aligned} (x+y)a &= xa + ya, \\ x(a+b) &= xa + xb, \\ (xa)b &= x(ab), \\ x1 &= x. \end{aligned}$$

We define a *balanced product* of two modules M_R and ${}_RN$ to be an abelian group P coupled with a function $f : M \times N \to P$ such that

$$\begin{aligned} f(x+x', y) &= f(x,y) + f(x',y), \\ f(x, y+y') &= f(x,y) + f(x,y'), \\ f(xa, y) &= f(x, ay). \end{aligned}$$

We define a *morphism* between balanced products (P, f) and (Q, g) to be a function $\eta : P \to Q$ which is a group homomorphism and which satisfies

$$g(x, y) = \eta f(x, y).$$

Throughout, M and N will be left and right modules, respectively. Hence, we will drop the subscripts for notational simplicity.

We define the *tensor product of M and N* to be a balanced product $(M \otimes_R N, \otimes)$ (here, we will drop the R subscript if it's implicitly understood) such that if (P, f) is any balanced product of M and N, then there exists a unique morphism $\Phi : M \otimes N \to P$. In other words, it satisfies a universal property.

Remark. This definition establishes that *if* a tensor product exists, it is unique. We see this in the following problem.

Problem 273. Prove that if $((M \otimes N)_1, \otimes_1)$ and $((M \otimes N)_2, \otimes_2)$ are the tensor product, then they are isomorphic.

Proof. This follows by the universal property. We have the maps $\otimes_1 : M \times N \to (M \otimes N)_1$ and $\otimes_2 : M \times N \to (M \otimes N)_2$. Hence, by the universal property of tensor products, there exists unique maps f, g such that $f : (M \otimes N)_1 \to (M \otimes N)_2$ and $g : (M \otimes N)_2 \to (M \otimes N)_1$. Notice that uniqueness forces $f \circ g = 1$ and $g \circ f = 1$, so these are invertible morphisms. Hence, they are isomorphisms. □

Notice as well that, assuming the tensor product exists, we have a nice way of writing it in terms of elements from M and N.

Problem 274. We have

$$M \otimes N = \text{span}\{x \otimes y \ : \ x \in M, y \in N\}.$$

Proof. Let

$$G = \text{span}\{x \otimes y \ : \ x \in M, y \in N\}.$$

Then this is a group, and more importantly is a subgroup of $M \otimes N$. Equipped with the map $\hat{\otimes} : M \times N \to G$, given by $\hat{\otimes}(x, y) = x \otimes y$, we see that G is in fact a balanced product. We check then that G is the tensor product; this will give us that G is in fact $M \otimes N$. This holds, since G is a subgroup, and so any morphism from $M \otimes N$ into a balanced product descends to a morphism from G into the balanced product. The essential uniqueness gives us an isomorphism between G and $M \otimes N$, and since G is a subgroup we have a unique morphism into $M \otimes N$ already, which is given by the natural injection. Hence, they must be isomorphic. □

Problem 275. Construct a tensor product for M and N.

Proof. We start by taking the free abelian group generated by $M \times N$, denoted by F. Elements in this group are of the form

$$n_1(x_1, y_1) + \cdots + n_r(x_r, y_r),$$

$n_i \in \mathbb{Z}$, $x_i \in M$, $y_i \in N$. Take G to be the subgroup generated by

$$(x + x', y) - (x, y) - (x', y),$$
$$(x, y + y') - (x, y) - (x, y'),$$
$$(xa, y) - (x, ay).$$

Define

$$M \otimes N := F/G,$$

and write

$$x \otimes y = (x, y) + G.$$

Going through the motions, we see that we have a balanced product with $\otimes : M \times N \to M \otimes N$ given by $(x, y) \mapsto x \otimes y$. We use the property of free groups to deduce that, given a balanced product (P, f), there is a unique homomorphism $g : F \to P$ given by $(x, y) \mapsto f(x, y)$ and extended linearly. Let K denote the kernel of this homomorphism. We see that $G \subset K$ by the above properties, so we get that the map $x \otimes y \mapsto f(x, y)$ is a unique morphism, using the prior problem. □

Problem 276. Suppose we have module homomorphism $f : M \to M'$, $g : N \to N'$. Show that $f \otimes g : M \otimes N \to M' \otimes N'$ is well-defined.

Proof. We want to use the universal property (since this is all we have). We have $\otimes : M \times N \to M \otimes N$. Notice as well that we can define $\Theta : M \times N \to M' \otimes N'$ via $(x, y) \mapsto f(x) \otimes g(y)$. We show that this gives us a balanced product.

(1) We have

$$\Theta(x+x', y) = f(x+x') \otimes g(y) = [f(x)+f(x')] \otimes g(y) = f(x) \otimes g(y) + f(x') \otimes g(y) = \Theta(x, y) + \Theta(x', y).$$

(2) We similarly have

$$\Theta(x, y + y') = \Theta(x, y) + \Theta(x, y').$$

(3) Finally, we have

$$\Theta(xa, y) = f(xa) \otimes g(y) = f(x)a \otimes g(y) = f(x) \otimes ag(y) = f(x) \otimes g(ay) = \Theta(x, ay).$$

Hence, it's a balanced product with respect to Θ. We get by the universal property a unique morphim

$$f \otimes g : M \otimes N \to M' \otimes N'.$$

Notice that this must factor through, so we have

$$(x, y) \mapsto x \otimes y \mapsto (f \otimes g)(x \otimes y),$$

$$(x, y) \mapsto f(x) \otimes g(y),$$

and these are equal, so we get

$$f(x) \otimes g(y) = (f \otimes g)(x \otimes y).$$

□

Problem 277. Show that for $f : M \to M'$, $f' : M' \to M''$, $g : N \to N'$, $g' : N' \to N''$, we have

$$f'f \otimes g'g = (f' \otimes g')(f \otimes g).$$

Proof. We have $f'f : M \to M''$, $g'g : N \to N''$, so by prior there exists a unique map

$$(f'f \otimes g'g)(x, y) = (f'f)(x) \otimes (g'g)(y).$$

By the prior problems as well, we see that

$$(f'f)(x) \otimes (g'g)(y) = (f' \otimes g')(f(x) \otimes g(y)) = (f' \otimes g')((f \otimes g)(x \otimes y)).$$

Associativity applies, and so we get that this is

$$((f' \otimes g')(f \otimes g))(x \otimes y).$$

We defined it on the generators, and so we have that this holds for the entire map. That is,

$$f'f \otimes g'g = (f' \otimes g')(f \otimes g).$$

□

Problem 278. Use the prior problems to deduce that

$$1_{M \otimes N} = 1_M \otimes 1_N.$$

Proof. We have

$$(1_M \otimes 1_N)(x \otimes y) = x \otimes y,$$

and since this applies on generators we get

$$1_M \otimes 1_N = 1_{M \otimes N}.$$

□

Problem 279. Show that, for $f : M \to M'$, $g : N \to N'$,

$$(f \otimes 1_{N'})(1_M \otimes g) = f \otimes g = (1_{M'} \otimes g)(f \otimes 1_N).$$

Proof. Using the prior problems, we have a big commutative diagram:

$$\begin{array}{ccc} M \otimes N & \xrightarrow{1_M \otimes g} & M \otimes N' \\ \downarrow{\scriptstyle f \otimes 1_N} & \searrow^{f \otimes g} & \downarrow{\scriptstyle f \otimes 1_{N'}} \\ M' \otimes N & \xrightarrow{1_{M'} \otimes g} & M' \otimes N' \end{array}$$

Since the diagram commutes, we get the desired result. □

Problem 280. Prove the distributive laws for tensors; that is, if $f_i : M \to M'$, $g_i : N \to N'$, prove

$$(f_1 + f_2) \otimes g = f_1 \otimes g + f_2 \otimes g,$$
$$f \otimes (g_1 + g_2) = f \otimes g_1 + f \otimes g_2.$$

Proof. Apply these to $x \otimes y$;

$$((f_1 + f_2) \otimes g)(x \otimes y) = (f_1 + f_2)(x) \otimes g(y) = (f_1(x) + f_2(x)) \otimes g(y)$$
$$= f_1(x) \otimes g(y) + f_2(x) \otimes g(y) = (f_1 \otimes g)(x \otimes y) + (f_2 \otimes g)(x \otimes y).$$

Since these are equal on generators, they extend to the whole space. The same argument applies for the second equality. □

Problem 281 (Jacobson 2, Section 3.7, Exercise 1)**.** Prove that the tensor product is commutative for commutative rings (the same argument also gives us for a ring and its opposite). That is, show that

$$M \otimes N \cong N \otimes N.$$

Proof. Define a map

$$\varphi : M \times N \to N \otimes M$$

given by

$$\varphi(x, y) = y \otimes x.$$

We show this gives a balanced product;

$$\varphi(x + x', y) = y \otimes (x + x') = y \otimes x + y \otimes x' = \varphi(x, y) + \varphi(x', y),$$
$$\varphi(x, y + y') = (y + y') \otimes x = y \otimes x + y' \otimes x = \varphi(x, y) + \varphi(x, y'),$$
$$\varphi(xa, y) = y \otimes xa = y \otimes ax = ya \otimes x = ay \otimes x = \varphi(x, ay).$$

So we have an induced map

$$\widehat{\varphi} : M \otimes N \to N \otimes M.$$

An analogous argument gives an induced map

$$\widehat{\theta} : N \otimes M \to M \otimes N,$$

and by the uniqueness we get that the composition of these is the identity; in other words, we have that these are isomorphisms. □

Problem 282. Let M_α be a (finite) collection of left R-modules, N a right R-module. Prove that

$$\left(\bigoplus M_\alpha\right) \otimes N \cong \bigoplus (M_\alpha \otimes N).$$

Proof. We proceed for the case of two left R modules, denoted M_1, M_2. We wish to show that

$$(M_1 \oplus M_2) \otimes N \cong (M_1 \otimes N) \oplus (M_2 \otimes N).$$

Inducting will give our desired result. Let

$$\varphi : (M_1 \oplus M_2) \times N \to (M_1 \otimes N) \oplus (M_2 \otimes N),$$

given by

$$\varphi((x, y), z) = (x \otimes z, y \otimes z).$$

This is a balanced product, since

$$\begin{aligned}
\varphi((x + x', y + y'), z) &= (x + x' \otimes z, y + y' \otimes z) = (x \otimes z, y \otimes z) + (x' \otimes z, y' \otimes z) \\
&= \varphi((x, y), z) + \varphi((x', y'), z), \\
\varphi((x, y), z + z') &= (x \otimes z + z', y \otimes z + z') = (x \otimes z, y \otimes z) + (x \otimes z', y \otimes z') \\
&= \varphi((x, y), z) + \varphi((x, y), z'), \\
\varphi((x, y)a, z) &= \varphi((xa, ya), z) = (xa \otimes z, ya \otimes z) = (x \otimes az, y \otimes az) = \varphi((x, y), az).
\end{aligned}$$

Hence, we have an induced map

$$\widehat{\varphi} : (M_1 \oplus M_2) \otimes N \to (M_1 \otimes N) \oplus (M_2 \otimes N).$$

We then want to construct an inverse map, which will then give us an isomorphism. Define

$$i_1 : M_1 \times N \to (M_1 \oplus M_2) \otimes N,$$

defined by

$$i_1(x, y) = ((x, 0), y).$$

This is going to be a balanced product by the same argument above, and so we get an induced map

$$\widehat{i_1} : M_1 \otimes N \to (M_1 \oplus M_2) \otimes N.$$

Similarly, we have an induced map

$$\widehat{i_2} : M_2 \otimes N \to (M_1 \oplus M_2) \otimes N,$$

so we have a map

$$\theta := \widehat{i_1} \oplus \widehat{i_2} : (M_1 \otimes N) \oplus (M_2 \otimes N) \to (M_1 \oplus M_2) \otimes N$$

given by

$$\theta(x \otimes z, y \otimes z) = \widehat{i_1}(x \otimes z) + \widehat{i_2}(y \otimes z).$$

We want to show that $\widehat{\varphi} \circ \theta = \mathrm{Id} = \theta \circ \widehat{\varphi}$. Notice that

$$\begin{aligned}
\theta(x \otimes z, y \otimes z) &= (x, 0) \otimes z + (0, y) \otimes z = ((x, 0) + (y, 0)) \otimes z = (x, y) \otimes z, \\
\widehat{\varphi}((x, y) \otimes z) &= (x \otimes z, y \otimes z).
\end{aligned}$$

So on generators, the compositions will be the identity, and so by extension the compositions are the identity. So we have an isomorphism. □

Remark. By induction, we get

$$\left(\bigoplus_{i=1}^{m} M_i\right) \otimes \left(\bigoplus_{j=1}^{r} N_j\right) \cong \bigoplus_{i,j=1}^{m,r} (M_i \otimes N_j).$$

Problem 283. Prove that

$$R \otimes M \cong M.$$

Proof. Define a map

$$\varphi : R \times M \to M$$

via

$$\varphi(a, m) = am.$$

We see that this is a balanced product;

$$\varphi(a + a', m) = (a + a')m = am + a'm = \varphi(a, m) + \varphi(a', m),$$
$$\varphi(a, m + m') = a(m + m') = am + am' = \varphi(a, m) + \varphi(a, m'),$$
$$\varphi(ar, m) = (ar)m = a(rm) = \varphi(a, rm).$$

So we get an induced linear homomorphism

$$\widehat{\varphi} : R \otimes M \to M$$

given by

$$\widehat{\varphi}(a \otimes m) = am.$$

This is surjective, since

$$\widehat{\varphi}(1 \otimes m) = m.$$

This is injective, since

$$\widehat{\varphi}(a \otimes m) = am = 0$$

implies either a or m is 0, which corresponds to the 0 element in $R \otimes M$. Hence, it's an isomorphism.

Remark. Alternatively, let $\theta : M \to R \otimes M$ be given by $\theta(m) = 1 \otimes m$. Then taking a generator $a \otimes m$, we have

$$\theta(\widehat{\varphi}(a \otimes m)) = \theta(am) = 1 \otimes am = a \otimes m,$$

and likewise

$$\widehat{\varphi}(\theta(m)) = \widehat{\varphi}(1 \otimes m) = m.$$

So these are inverses, and hence we have that $\widehat{\varphi}$ is an isomorphism.

□

Let R and S be two rings. We define a $R - S$ *bimodule*, say N, to be a module which is a left R module and a right S module, with the additional quality that

$$r(ms) = (rm)s$$

for all $r \in R$, $m \in M$, $s \in S$.

Problem 284. Let M $S - R$ bimodule, N a $R - T$ bimodule. Show that

$$M \otimes_R N$$

is a $S - T$ bimodule, where we define

$$sz = (s \otimes 1)z,$$
$$zt = z(1 \otimes t),$$

for $z \in M \otimes_R N$, $s \in S$, $t \in T$.

Proof. We want to first show that it is a left S module. It's clear that it's an abelian group, so we just need to show the following (here, we use the fact that $M \otimes_R N$ is spanned by $x \otimes y$):

(1) Notice that

$$s(z + z') = s\left(\sum (x_i \otimes y_i) + \sum (x'_j \otimes y'_j)\right) = s\left(\sum x''_i \otimes y''_i\right)$$
$$= (s \otimes 1)\left(\sum x''_i \otimes y''_i\right) = \sum sx''_i \otimes y''_i$$
$$= \sum sx_i \otimes y_i + \sum sx'_j \otimes y_j = sz + sz'.$$

(2) We have

$$(r+s)z = (r+s)\left(\sum x_i \otimes y_i\right) = ((r+s)\otimes 1)\left(\sum x_i \otimes y_i\right) = \sum (r+s)x_i \otimes y_i$$
$$= \sum rx_i \otimes y_i + \sum sx_i \otimes y_i = rz + sz.$$

(3) We have

$$1z = 1\left(\sum x_i \otimes y_i\right) = (1\otimes 1)\left(\sum x_i \otimes y_i\right) = \sum x_i \otimes y_i = z.$$

So this is a left S module. The same argument applies to give us that it is a right T module. □

Problem 285. Prove the Prime Avoidance lemma. That is, prove the following statement:
Let R be a commutative ring. Let $I_1, \ldots, I_n$ and J be ideals of R such that $J \subset \bigcup_j I_j$. Then if at most two of the I_js are not prime, then J is contained in one of the I_js.

Remark. Note the contrapositive of the statement:
Let $I_1, \ldots, I_n$, J be ideals of R, $J \not\subset \bigcup_j I_j$. If all but two of the I_j are prime, then there exists an $x \in J$ such that $x \notin I_i$ for all i; in other words, $J \not\subset I_j$ for all j.

Proof. We prove the contrapositive. If $n = 1$, we are clearly done. If $n = 2$, then we have that $R \not\subset I_1 \cup I_2$. Choose $x, y \in J$ such that $x \notin I_1$ and $y \notin I_2$. If $x \notin I_2$ we are done, and if $y \notin I_1$ we are done. So consider the case that $x \notin I_1$, $x \in I_2$, $y \notin I_2$, $y \in I_1$. Then we have that $x + y \notin I_1$ nor I_2. This follows since if $x + y \in I_1$, then we get that $(x + y) - y = x \in I_1$, a contradiction. If $x + y \in I_2$, we get that $(x + y) - x = y \in I_2$, a contradiction.

Now, assume that $n \geq 3$. Assume it holds for $n - 1$. Renumber the ideals so that I_n is a prime ideal. For each j, choose a

$$z_i \in J - \bigcup_{j \neq i} I_j.$$

The inductive hypothesis tells us that the RHS is non-empty, so we can find such a z_i. If $z_i \notin I_i$ for some i we win, so assume that $z_i \in I_i$ for all i. Let

$$z = z_1 \cdots z_{n-1} + z_n.$$

We see that $z \in J$, but $z \notin I_j$ for all j. If $z \in I_j$ for $j \leq n - 1$, then we have

$$z - z_1 \cdots z_{n-1} = z_n \in I_j,$$

a contradiction. Likewise, if $z \in I_n$, we have that

$$z - z_n = z_1 \cdots z_{n-1} \in I_n.$$

Since I_n is a prime ideal, we must have that there is some z_i for $1 \leq i \leq n - 1$ such that $z_i \in I_n$. This, however, gives us a contradiction. Thus, $z \in J$, $z \notin \bigcup I_j$. □