Exercises in Group Theory

Arpon Basu

January 26, 2024

1 Group Axioms

Exercise 1.1. *Suppose G is a group and H, K are two subgroups. Define the subset $HK := \{hk \in G : h \in H, k \in K\}$. Similarly define KH. Prove that HK is a subgroup iff $KH = HK$.*

Proof. If $KH = HK$, then for any $h_1, h_2 \in H$ and $k_1, k_2 \in K$, if we consider $(h_1k_1)^{-1}(h_2k_2)$, we get

$$(h_1k_1)^{-1}(h_2k_2) = k_1^{-1}h_1^{-1}h_2k_2 = k_1^{-1}hk_2 = k_1^{-1}k_2'h' = kh' \in KH = HK$$

where $hk_2 = k_2'h'$ since $HK = KH$. Consequently, since HK is closed under "$^{-1}\cdot$", it's a group.
Conversely, if HK is a group, then $kh = (h^{-1}k^{-1})^{-1} \in HK \; \forall h \in H, k \in K$, ie:- $KH \subseteq HK$. Moreover, if $hk \in HK$, then $KH \ni k^{-1}h^{-1} = (hk)^{-1} \in HK$, so $HK \subseteq KH$, and thus $HK = KH$.

1. **Important trick I**: To show that a set A is a group under $*$, it suffices to show (given that the existence of an identity $e \in A$ is taken care of) that for any two elements $a_1, a_2 \in A$, $a_1^{-1} * a_2 \in A$.
2. **Important trick II**: Usually when we try to show that $A = B$ for 2 sets A, B, the most common way is to show that every $a \in A$ belongs to B and vice versa. But note that when we're trying to show two groups to be equal, we can also give arguments like "for every $a \in A$, $a^{-1} \in B$", because $G = G^{-1}$ for any group: Further note that when we say $G = G^{-1}$, we are meaning a set equality, not a group isomorphism. Indeed, for infinite groups it's possible that the group is isomorphic to one of it's proper subgroups (take for example $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$).

□

Exercise 1.2. *Suppose G is a group and H is a nonempty finite subset of G. Suppose H is closed under the group operation of G. Prove that H is a subgroup.*

Proof. If $H = \{1_G\}$, then we're done. Otherwise choose $1_G \neq h \in H$, and consider the set $\mathscr{H} := \{h^k : k \geq 1\}$. Clearly $\mathscr{H} \subseteq H$. Since $|H| < \infty$, we have $h^m = h^n$ for some $1 \leq m < n$, and consequently $1_G = h^{n-m} \in H$. Finally, for any $h \in H$ such that $h \neq 1_G$, we have that all elements in $\{hh' : h' \in H\}$ are distinct, and moreover the size of this set is equal to $|H|$. Consequently $\exists h' \in H$ such that $hh' = 1_G$. Thus, the inverse of every element in H also lies in H. Hence H is a group. □

Exercise 1.3. *Prove that a group in which the order of every non-unit element is 2 must be abelian.*

Proof. Let a, b be any two arbitrary elements of our group. Then $baab = ba^2b = b^2 = 1 = (ab)^2 = abab$, and thus $baab = abab$. Post multiply with $b^{-1}a^{-1}$ on both sides to obtain $ba = ab$, as desired. □

Exercise 1.4. *If G is a group in which $(ab)^i = a^i b^i$ for 3 consecutive integers $i > 1$, prove that G is abelian.*

Proof.

$$(ab)^{i-1} = a^{i-1}b^{i-1};\ (ab)^i = a^i b^i \implies a^{i-1}b^{i-1}ab = a^i b^i \implies b^{i-1}a = ab^{i-1}$$

Similarly, $ab^i = b^i a$, and thus $bab^{i-1} = bb^{i-1}a = ab^i \implies ba = ab$, as desired. □

Exercise 1.5. *If G is a group such that $(ab)^3 = a^3b^3$ and $(ab)^5 = a^5b^5$ for all $a, b \in G$, then prove that G is abelian.*

Proof. One notes that

$$(ab)^3 = a(ba)^2 b = a^3b^3 \implies (ba)^2 = a^2b^2 \implies (ab)^4 = ((ab)^2)^2 = (b^2a^2)^2 = a^4b^4$$

Then by the above exercise we're done, since $(ab)^i = a^i b^i$ for $i = 3, 4, 5$. □

2 Homomorphisms

Exercise 2.1. *Let G be any finite group. Show that there exists a monomorphism $f : G \mapsto \mathfrak{S}_n$, where $\mathfrak{S}_n$ is the automorphism group of $[n]$, ie:- the group of all permutations of $[n]$.*

Proof. Let $G = \{g_1, g_2, \ldots, g_n\}$. Then define a function f from G to $\mathfrak{S}_n$ such that

$$f(g_k)(i) = j \text{ if } g_k g_i = g_j$$

Then

1. $f(g)$ is indeed a permutation for all $g \in G$. In fact for any group $G = \{g_1, g_2, \ldots, g_n\}$, $gG = \{gg_1, gg_2, \ldots, gg_n\}$ is a permutation of G. Why? Because since any element $g \in G$ is invertible, $gg_i \neq gg_j$ for $i \neq j$, and thus $\text{im}(f) \subseteq \mathfrak{S}_n$.
2. Also, $(f(g_1) \circ f(g_2))(i) = f(g_1)(f(g_2)(i)) = f(g_1)(i') = j = f(g_1 g_2)(i)$, where $g_2 g_i = g_{i'}$ and $g_1 g_{i'} = g_j$, and thus f is a homomorphism.
3. Furthermore, if $f(g_k)(i) = f(g_{k'})(i)$, then $g_k g_i = g_{k'} g_i \implies g_k = g_{k'}$.

Thus, f maps different elements of g to different permutations [1], and hence is an injective homomorphism.
The above f is known as the *Cayley monomorphism.* □

Exercise 2.2. *Give a counterexample to the following assertion (H and G are finite groups):*

$$|G| > |H| \implies \exists \text{ monomorphism } f : H \mapsto G$$

Proof. Let $G := (\mathbb{Z}_3, +)$ and $H := (\mathbb{Z}_2, +)$. If there existed a monomorphism f from H to G, then by the properties of homomorphisms, we know that $f(0_H) = 0_G$. Since a monomorphism is injective, we then get that $f(1_H) = 1_G$ or 2_G. But then $0_G = f(0_H) = f(1_H + 1_H) = f(1_H) + f(1_H) \neq 0_G$ for $f(1_H) = 1_G$ or 2_G, leading to a contradiction. □

Exercise 2.3. *Give a counterexample to the following assertion:*

$$|G| = |H| \implies \exists \text{ isomorphism } \varphi : H \mapsto G$$

Proof. We give three counterexamples to the following assertion, one when $|G|$ is finite, and the others when it's infinite.

[1] not only are the permutations distinct, they are also derangements w.r.t each other

1. Consider $G = (\mathbb{Z}_4, +)$, and $H = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Note that the square of any element in H is equal to the identity of H [2], while that is not the case in G, and thus they can't be isomorphic.

2. Consider $G = (\mathbb{R}, +)$, and $H = (\mathbb{R}^\times, \cdot)$. Note that the cardinalities of these two groups are equal. If φ is a homomorphism from G to H, then $\varphi(x + y) = \varphi(x)\varphi(y)$, and thus $\varphi(x) = \varphi(x/2)^2 \geq 0$. Consequently, φ isn't surjective. Since an isomorphism is required to be a surjective homomorphism, we conclude that an isomorphism doesn't exist.

3. Consider $G = (\mathbb{C}^\times, \cdot)$, and $H = (\mathbb{C}, +)$. Note that the cardinalities of these two groups are equal. If φ is a homomorphism from G to H, then $\varphi(xy) = \varphi(x) + \varphi(y)$, and thus $0 = \varphi(1) = \varphi((e^{2i\pi/n})^n) = n\varphi(e^{2i\pi/n})$, and thus $\varphi(e^{2i\pi/n}) = 0\ \forall n \in \mathbb{N}$. Consequently, φ isn't injective. Since an isomorphism is required to be a injective homomorphism, we conclude that an isomorphism doesn't exist.

□

Exercise 2.4. *Calculate* $|\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})|$.

Proof. We represent $x + m\mathbb{Z}$ or $x + n\mathbb{Z}$ in this problem simply as x. Whether it's $m\mathbb{Z}$ or $n\mathbb{Z}$ will be clear from the context. Let f be any homomorphism from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$. Then $f(0) = 0$, and we have $f(m \cdot 1) = mf(1)$. But $f(m) = 0$, and thus $mf(1) = 0$. Consequently, $\frac{n}{\gcd(m,n)} \Big| f(1)$. Also remember that for specifying a homomorphism, we only need to map the generators of our domain group (and check that the homomorphism extends consistently to the entire group). Since $\mathbb{Z}/m\mathbb{Z}$ is cyclic, once we have specified $f(1)$, we're done since $f(x) = xf(1) \bmod n$.
Now, if $\frac{n}{\gcd(m,n)} \Big| f(1)$, and since $0 \leq f(1) < n$, we have exactly $\gcd(m, n)$ choices for $f(1)$, and consequently, those many homomorphisms. □

Exercise 2.5. *$x \mapsto x^{-1}$ is an automorphism iff G is abelian.*

Proof. If $x \mapsto x^{-1}$ is an automorphism, then $yx = (x^{-1}y^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1} = xy$, demonstrating abelianity.
If G is abelian, then since $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$, the map is a homomorphism. It's also clear that the map is bijective, and thus is an automorphism. □

Exercise 2.6. *Prove that every group G of order greater than 2 has at least one non-trivial automorphism.*

Proof. If G is not abelian, then $G - Z(G)$ isn't empty. Choose $g_0 \in G - Z(G)$. Then $x \mapsto g_0 x g_0^{-1}$ is a non-trivial automorphism.
If G is abelian, and if there is an $x \in G$ such that $x \neq x^{-1}$, then $x \mapsto x^{-1}$ is a non-trivial automorphism.
Otherwise we have an abelian group in which the order of every element (except 1_G) is 2. Now, we claim that $(\mathbb{F}_2, G)$ is a vector space over $\mathbb{F}_2$, where for any $\alpha \in \mathbb{F}_2$ and $v \in G$, one ***defines*** $\alpha \cdot v := v^\alpha$, and thus $0_{\mathbb{F}_2} \cdot v = 1_G$, and $1_{\mathbb{F}_2} \cdot v = v$.
We must first confirm that the axioms of a vector space are indeed followed: If we refer to the axioms *here*, then it's not hard to verify that G is indeed a vector space over $\mathbb{F}_2$. Moreover, since $|G| > 2$, the dimension d of this vector space is > 1. Then note that if we permute the basis vectors of our vector space, we obtain a non-trivial automorphism of G. □

Exercise 2.7. *Let G be a finite abelian group. Let $p = \prod_{g \in G} g$. Let k be the number of elements in G of order 2. Show that $p = 1_G$ if $k \neq 1$, and $p = t$ if $k = 1$, where t is the unique element of order 2.*

[2] which is (0, 0)

Proof. Let H be the set of all elements in G s.t. $g^2 = 1$. Note that H is a subgroup of G, $|H| = 1 + k$, and H is a vector space over $\mathbb{F}_2$, so $|H|$ is a power of 2. Note that all elements in $G - H$ get canceled by their inverses in $\prod_{g\in G} g$, and thus $\prod_{g\in G} g = \prod_{g\in H} g$. Now, if

- $k = 0$: Then $H = \{1_G\}$, and $\prod_{g\in H} g = 1_G$.
- $k = 1$: Then $H = \{1_G, t\}$, and $\prod_{g\in H} g = t$.
- $k \geq 2$: Since $H \cong \mathbb{F}_2^d$ for some $d \geq 2$,

$$\prod_{g\in H} g \sim \bigoplus_{f\in\mathbb{F}_2^d} (f_1, f_2, \ldots, f_d) = \left(\sum_{f\in\mathbb{F}_2^d} f_1, \sum_{f\in\mathbb{F}_2^d} f_2, \ldots, \sum_{f\in\mathbb{F}_2^d} f_d\right)$$

Since exactly half of $\mathbb{F}_2^d$'s are 1s (and the other 0s), we have that $\sum_{f\in\mathbb{F}_2^d} f_i = 2^{d-1} = 0 \bmod 2$, and thus $\prod_{g\in H} g \sim 0_{\mathbb{F}_2} \sim 1_G$. □

Exercise 2.8. *Let G, H, K be 3 groups and let K be abelian. Endow $\mathrm{Hom}(\cdot, K)$ with the pointwise addition operation to make it an abelian group. Prove that $\mathrm{Hom}(G \times H, K)$ is isomorphic as a group to $\mathrm{Hom}(G, K) \times \mathrm{Hom}(H, K)$.*

Proof. We refer to the proof here.
Let G, H, K be three groups with K abelian and consider two homomorphisms:

$$j_G : G \mapsto G \times H$$
$$j_G(g) = (g, 1)$$
$$j_H : H \mapsto G \times H$$
$$j_H(h) = (1, h)$$

Define

$$\Phi : \mathrm{Hom}(G \times H, K) \mapsto \mathrm{Hom}(G, K) \times \mathrm{Hom}(H, K)$$
$$\Phi(\lambda) = (\lambda \circ j_G, \lambda \circ j_H)$$

We treat each Hom as a group via pointwise addition. Then note that Φ is a group isomorphism. Indeed,

1. Φ is a homomorphism:
$$\Phi(\lambda + \beta) = ((\lambda + \beta) \circ j_G, (\lambda + \beta) \circ j_H)$$
WLOG lets consider the first coordinate only:
$$((\lambda + \beta) \circ j_G)(g) = (\lambda + \beta)(g, 1) = \lambda(g, 1) + \beta(g, 1) = \lambda \circ j_G(g) + \beta \circ j_G(g)$$
In other words
$$(\lambda + \beta) \circ j_G = \lambda \circ j_G + \beta \circ j_G$$
Analogously $(\lambda + \beta) \circ j_H = \lambda \circ j_H + \beta \circ j_H$ showing that
$$\Phi(\lambda + \beta) = \Phi(\lambda) + \Phi(\beta)$$

2. Φ is invertible: Indeed, consider the function

$$\Theta : \mathrm{Hom}(G,K) \times \mathrm{Hom}(H,K) \mapsto \mathrm{Hom}(G \times H, K)$$
$$\Theta(\lambda,\beta) : G \times H \mapsto K$$
$$\Theta(\lambda,\beta)(g,h) = \lambda(g) + \beta(h)$$

It's easy to see that Θ is the inverse of Φ, and thus Φ is an isomorphism.

□

3 Linear Representations

Exercise 3.1. *Let G be a finite subgroup of $\mathrm{GL}(n,\mathbb{R})$. Prove that there exists $x \in \mathrm{GL}(n,\mathbb{R})$ such that xGx^{-1} is a subgroup of $\mathrm{O}(n,\mathbb{R})$.*

Proof. Define the matrix

$$B := \sum_{g \in G} g^{\mathsf{T}} g$$

It's easy to see that B is a symmetric positive definite matrix [3]. On the other hand, also note that for any $h \in G$, we have

$$h^{\mathsf{T}} B h = \sum_{g \in G} h^{\mathsf{T}} g^{\mathsf{T}} g h = \sum_{g \in G} (gh)^{\mathsf{T}} (gh)$$

But as we saw above, pre- or post-multiplication by any element of a finite group merely permutes it's elements, and thus

$$\sum_{g \in G} (gh)^{\mathsf{T}} (gh) = \sum_{g \in G} g^{\mathsf{T}} g \implies h^{\mathsf{T}} B h = B \; \forall h \in G$$

Now, since B is a real symmetric (strictly) positive definite matrix, it can be written as $x^T x$ for some $x \in \mathrm{GL}(n,\mathbb{R})$[4]. Thus

$$h^{\mathsf{T}} B h = B \iff h^{\mathsf{T}} x^{\mathsf{T}} x h = x^{\mathsf{T}} x \iff (x^{-1})^{\mathsf{T}} h^{\mathsf{T}} x^{\mathsf{T}} x h x^{-1} = I$$
$$\iff (xhx^{-1})^{\mathsf{T}} (xhx^{-1}) = I \; \forall h \in G$$

Thus we have explicitly constructed a $x \in \mathrm{GL}(n,\mathbb{R})$ which demonstrates $xGx^{-1} < \mathrm{O}(n,\mathbb{R})$. □

Exercise 3.2. *Let G be any finite group. Show that there exists a monomorphism $f : G \mapsto \mathrm{GL}(n,\mathbb{R})$.*

Proof. We construct an *inclusion* $\mathfrak{S}_n \overset{\psi}{\hookrightarrow} \mathrm{GL}(n,\mathbb{R})$ such that for any $\sigma \in \mathfrak{S}_n$,

$$\psi(\sigma)(e_i) = e_{\sigma(i)}$$

where $\{e_1, e_2, \ldots, e_n\}$ is the canonical basis of $\mathbb{R}^n$, and consequently for any vector $\mathbb{R}^n \ni v = \sum_{i=1}^n \alpha_i e_i$,

$$\psi(\sigma)(v) = \sum_{i=1}^n \alpha_i e_{\sigma(i)}$$

[3] Since $g^{\mathsf{T}} g$'s are symmetric, B is symmetric too, and since $g^{\mathsf{T}} g$'s are strictly positive definite (since g is invertible, $g^{\mathsf{T}} g$ is strictly positive definite), B is strictly positive definite too

[4] B being real symmetric implies it can be written as $O^{\mathsf{T}} D O$ (where O is an orthogonal matrix), and B being positive definite implies $D \succ 0$, and thus we can choose $x = \sqrt{D} O$

Basically, ψ maps each permutation in $\mathfrak{S}_n$ to the corresponding *permutation matrix* in $\mathrm{GL}(n,\mathbb{R})$[5], and it's easy to see that this is a monomorphism. Since the composition of monomorphisms form a monomorphism, and since we already know a monomorphism b/w G and $\mathfrak{S}_n$, there exists a monomorphism from G to $\mathrm{GL}(n,\mathbb{R})$ too. □

Exercise 3.3. *Define* $\mathcal{M} : \mathbb{C} \mapsto \mathrm{M}(2,\mathbb{R})$, $\mathcal{M}(x+iy) = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$. *For any matrix* $A \in \mathrm{M}(n,\mathbb{C})$, *replace every entry* z *of* A *by the* 2×2 *block* $\mathcal{M}(z)$ *to form a* $2n\times 2n$ *real matrix* $A' \in \mathrm{M}(2n,\mathbb{R})$. *Show that* $\det(A') = |\det_{\mathbb{C}} A|^2$.

Proof. Consider the map $f : \mathrm{M}(n,\mathbb{C}) \mapsto \mathrm{M}(2n,\mathbb{R})$. We shall show that it is a homomorphism: Indeed, if one takes two matrices $A_1, A_2 \in \mathrm{M}(n,\mathbb{C})$, then by expanding their product it's not hard to see that $f(A_1)f(A_2) = f(A_1A_2)$, ie:- f is a homomorphism. Now by Schur's triangularization, we have that every matrix in $\mathrm{M}(n,\mathbb{C})$ is similar[6] to some upper triangular matrix. Since homomorphisms preserve relations and inverses, we obtain that *it is enough to verify the given assertion for upper triangular matrices* $A \in \mathrm{M}(n,\mathbb{C})$. *In fact, since for upper triangular matrices the determinant is determined entirely by diagonal entries, it is enough to verify the above assertion for only diagonal matrices in* $\mathrm{M}(n,\mathbb{C})$. But that follows easily through directly expanding the matrices. □

4 Dihedral Groups

Exercise 4.1. *Produce a group isomorphism* $\mathfrak{S}_3 \cong D_3$, *where* D_3 *is the dihedral group.*

Proof. Let $r \in D_3$ denote anticlockwise rotation by $2\pi/3$, and let $\sigma \in D_3$ denote reflection along x-axis. Then $D_3 = \{1, r, r^2, \sigma, \sigma r, \sigma r^2\}$. Let φ be our isomorphism. Then:

- $\varphi(\mathrm{id}) = 1$
- $\varphi\left(\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\right) = r$
- $\varphi\left(\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\right) = \sigma$

On **extending** φ to other elements of $\mathfrak{S}_3$, one can verify this is an isomorphism.
Note: Let G_1 and G_2 be two groups, and let S be a generating set of G_1. If there is a homomorphism $f : S \mapsto G_2$, then there can be *atmost one* extension of f to a homomorphism between $G_1 \mapsto G_2$. □

Exercise 4.2. *Show that* $\mathfrak{S}_3$ *is generated by a 2-cycle and a 3-cycle.*

Proof. Immediately follows from the previous exercise: One notes that $\sigma \in D_3$ is (equivalent, in the sense of our isomorphism, to) the 2-cycle $(2,3)$, while $r \in D_3$ is the 3-cycle $(1,2,3)$. Thus $\mathfrak{S}_3$ is generated by a 2-cycle and a 3-cycle. □

Exercise 4.3. *Calculate* $Z(D_n)$ *for* $n > 2$.

Proof. We use the presentation $D_n = \{r^i\sigma^j : i \in \{0,1,\ldots,n-1\}, j \in \{0,1\}\}$.
Note that $\sigma \notin Z(D_n)$ for any $n > 2$, since $\sigma r = r^{-1}\sigma \neq r\sigma$. Similarly, $r^i\sigma \notin Z(D_n)$ if $i > 0$ since $r^i\sigma \cdot r = r^{i-1}\sigma$, while $r \cdot r^i\sigma = r^{i+1}\sigma \neq r^{i-1}\sigma$. Finally,

1. If n is odd: Then $r^i \notin Z(D_n)$ for $n/2 > i > 0$, since $r^i\sigma = \sigma r^i \implies r^{2i} = 1$, which is not possible. And if $r^i \in Z(D_n)$ for $i > n/2$, then since $Z(D_n)$ is a group, $r^{-i} = r^j \in Z(D_n), 0 < j < n/2$, which again isn't possible.

[5] it's easy to show that permutation matrices are invertible and hence belong to GL
[6] $A \sim B$ if $A = PBP^{-1}$ for some $P \in \mathrm{GL}(n,\mathbb{C})$

2. If n is even: As above, $r^i \in Z(D_n) \implies r^{2i} = 1 \implies i = n/2$. We further verify that $r^{n/2} \in Z(D_n)$.

Thus $Z(D_n)$ is trivial if n is odd, and $Z(D_n) = \{1, r^{n/2}\}$ if n is even. □

5 Cosets

Exercise 5.1. *Let H be any subgroup of a group G. Prove that the association $G/H \to H\backslash G : gH \mapsto Hg$ is well defined if and only if for all $h \in H$ and for all $g \in G$, $ghg^{-1} \in H$.*

Proof. Note that the association $gH \mapsto Hg$ is **not** well-defined iff there are two elements $g_1, g_2 \in G$ such that the left cosets of g_1 and g_2 are the same but their right cosets aren't [7]. Thus the condition for the association to be well defined is equivalent to $g_1H = g_2H \implies Hg_1 = Hg_2 \ \forall g_1, g_2 \in G$. But $g_1H = g_2H \iff g_1^{-1}g_2 \in H$, and similarly $Hg_1 = Hg_2 \iff g_1g_2^{-1} \in H \iff g_2g_1^{-1} \in H$. Thus $gH \mapsto Hg$ being a well defined function is equivalent to saying

$$g_1^{-1}g_2 \in H \implies g_2g_1^{-1} \in H \ \forall g_1, g_2 \in G$$

Thus for any $g \in G$ and any $h \in H$, we have

$$g^{-1}(gh) \in H \implies ghg^{-1} \in H$$

as desired.
Conversely, $ghg^{-1} \in H \implies gh \in Hg \implies gH \subseteq Hg \ \forall g \in G$. Similarly, $ghg^{-1} \in H \implies hg^{-1} \in g^{-1}H \implies Hg^{-1} \subseteq g^{-1}H \ \forall g \in G$. Applying this conclusion for $g \to g^{-1}$ yields $Hg \subseteq gH$, and thus $gH = Hg \ \forall g \in G$. Consequently, the association $gH \mapsto Hg$ is well defined [8]. □

Exercise 5.2. *For any subgroup H of a group G,*

1. *Produce a bijection $G/H \to H\backslash G$.*
2. *Produce a bijection $G/H \times H \to G$.*

(G and H are not necessarily finite)

Proof. The bijections are as follows:

1. The function $f : gH \mapsto Hg^{-1}$ works. Indeed, if $g_1H = g_2H$, then $g_1^{-1}g_2 \in H \implies Hg_1^{-1} = Hg_2^{-1}$, and conversely, $Hg_1 = Hg_2$, then $g_1^{-1}H = g_2^{-1}H$. Thus the association is well defined and bijective.
2. Let each coset in G/H be represented by any element of the coset (this line requires the *Axiom of Choice*). Then it's easy to see that the function $\varphi : G/H \times H \mapsto G : \varphi((g, h)) = gh$ is indeed a bijection.

□

[7] if that happens, then $g_1H = g_2H$ will get mapped to two different sets Hg_1 and Hg_2 and thus won't be a function.
[8] the association is just the identity function in this case

6 Order

Exercise 6.1. *Let G be any group and assume that $a \in G$, $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$ is finite. Let $o(a) := \min\{n > 0 : a^n = 1_G\}$.*

1. *Prove that $o(a) = |\langle a \rangle|$.*
2. *Describe the kernel and the image of the homomorphism $\mathbb{Z} \to G : n \mapsto a^n$.*

Proof. Since $\langle a \rangle$ is finite, there exist m, n such that $a^m = a^{m+n}$, and thus $a^n = 1_G$. Also, if n is the minimum number such that $a^n = 1_G$, then $1, a, a^2, \ldots, a^{n-1}$ must all be distinct[9], and for any $k \geq n$, $a^k = a^{k \bmod n}$. Thus $\langle a \rangle = \{a^k : n > k \geq 0\}$, and thus $o(a) = |\langle a \rangle|$.
For the second part, as mentioned above, the **image of the homomorphism is $\langle a \rangle$, and the kernel is $o(a) \cdot \mathbb{Z}$**: Why? Clearly, all multiples of $o(a)$ take our homomorphism to 1_G. Moreover, if there exists n' such that $a^{n'} = 1_G$ and $n' \notin o(a) \cdot \mathbb{Z}$, then n' mod $o(a)$ yields a number strictly smaller than $o(a)$ which also takes our homomorphism to 1_G, contradicting the minimality of $o(a)$. □

Exercise 6.2. *Let G be a finite group and let $n = |G|$. Prove that for every element $a \in G, a^n = 1_G$.*

Proof. Since $\langle a \rangle$ is a subgroup of G, $o(a) = |\langle a \rangle| \Big| |G| = n$ [10], and consequently $a^n = 1_G$. □

Exercise 6.3. *If G is a finite group such that 3 does not divide $n = |G|$, and if for all $a, b \in G$, $(ab)^3 = a^3b^3$ then G is abelian.*

Proof.

$$(ab)^3 = a^3b^3 \implies baba = aabb \iff (ba)^2 = a^2b^2$$

Then

$$(ab)^4 = ((ab)^2)^2 = (b^2a^2)^2 = a^4b^4$$

But

$$(ab)^4 = a(ba)^3b = ab^3a^3b$$

Thus

$$ab^3a^3b = a^4b^4 \implies b^3a^3 = a^3b^3$$

Now, since $3 \nmid n$, let n' be the smallest integer greater than n which is divisible by 3. If $a_1^3 = a_2^3$, then $a_1^{n'} = a_2^{n'}$, and thus $a_1^\varepsilon = a_2^\varepsilon$ where $\varepsilon \in \{1, 2\}$. From here it's easy to deduce that $a_1 = a_2$. Thus, the map $x \mapsto x^3$ is injective, and since G is finite, bijective too. Consequently all elements $x, y \in G$ can be written as a^3, b^3 for some $a, b \in G$, and thus $a^3b^3 = b^3a^3$ $\forall a, b \in G$ is equivalent to saying that G is abelian. □

7 Quotients

Exercise 7.1. *Let $k = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Let $V = k^n$, and consider the inner product $g : V \times V \to k$ defined by $g(v, w) = v^*w$, where v^* is the conjugate transpose of v. Let W be any linear k-subspace of V. Define the orthogonal complement by $W^\perp = \{v \in V : \forall w \in W, g(v, w) = 0\}$. Then prove that*

1. *$V \cong W \oplus W^\perp$.*

[9] otherwise there will be an even smaller number n' such that $a^{n'} = 1_G$
[10] Lagrange's Theorem

2. *The composition* $W^\perp \xhookrightarrow{\psi_1} V \xrightarrow{\psi_2} V/W$ *where the first one is the inclusion and the second one is the quotient map, is an isomorphism.*

Proof. The proofs are as follows:

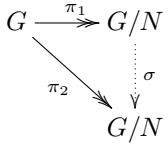
1. Let $\{w_1, w_2, \ldots, w_k\}$ be an orthonormal basis for W. Then for any vector v consider $w = \sum_{i=1}^{k} g(v, w_i)w_i$, and $w' = v - w$. Then $w \in W$, and $w' \in W^\perp$. Moreover it's easy to see that this choice of w is unique. Thus $V \cong W \oplus W^\perp$.

2. Since ψ_1 $(x \mapsto x)$, ψ_2 $(v \mapsto v+w)$ are homomorphisms, so $\psi := \psi_2 \circ \psi_1$ $(x \mapsto x+w)$ is also a homomorphism. Moreover, since $V \cong W \oplus W^\perp$, ψ is an epimorphism. Furthermore, $\ker \psi = \{x \in W^\perp : x+W \in W\} = \{x \in W^\perp : x \in W\} = \{0\}$. Since the kernel of ψ is trivial, it's injective, and thus an isomorphism.

□

Exercise 7.2. *Give examples of a group G, a normal subgroup N and two different epimorphisms $\pi_1, \pi_2 : G \to G'$ such that $\ker \pi_1 = \ker \pi_2$.*

Proof.



Note that if σ is any non trivial automorphism of G/N, and if we[11] have an epimorphism π from G to G/N, then $\sigma \circ \pi$ gives us another distinct epimorphism from G to G/N such that $\ker \pi = \ker \sigma \circ \pi = N$.
Indeed, that's what we do: Choose an abelian group G with a proper subgroup N [12] such that G has atleast one element g such that $g \neq g^{-1}$. Let $G \overset{\pi_1}{\twoheadrightarrow} G/N : \pi_1(g) := gN$ be the usual epimorphism. Let $G/N \overset{\sigma}{\longleftrightarrow} G/N$ be the automorphism $\sigma(gN) := g^{-1}N$ [13]. Then $\pi_2 = \sigma \circ \pi_1$ is another distinct epimorphism from G to G/N with the same kernel N. □

Exercise 7.3. *Let ϕ be an epimorphism from G to G/N (where N is a normal subgroup). Is $\ker \phi$ necessarily isomorphic to N?*

Proof. Let $G = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}$, and let $N = \mathbb{Z}/3\mathbb{Z} \oplus 6\mathbb{Z}$ [14]. Then G/N [15] is isomorphic to $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then $\ker \phi \cong 2\mathbb{Z}$, which **is not** isomorphic to N. □

8 Group Actions

Exercise 8.1. *Let A,B be two abelian groups and let $\phi : B \to \mathrm{Aut}_{\mathrm{gp}}(A)$ be any group homomorphism and let $G = A \rtimes_\phi B$. Prove that G is abelian if and only if ϕ is trivial.*

[11] by the usual quotient construction
[12] since G is abelian, N is normal
[13] it's easy to verify that this is an automorphism given G is abelian
[14] since the groups in question are abelian, any subgroup is normal
[15] note that the coset along the first coordinate is trivial since G and N are same along the first coordinate. Thus the overall coset can be taken to be coset of the second coordinates of G and N.

Proof. If ϕ is trivial (ie:- it's image is just the identity automorphism), then $(a,b)\cdot(c,d) = (a\phi_b(c), bd) = (ac, bd) = (ca, db) = (c,d)\cdot(a,b)$.
If G is abelian, then $(a,b)\cdot(c,d) = (c,d)\cdot(a,b) \implies a\phi_b(c) = c\phi_d(a)\ \forall a,b,c,d \in G$. In particular, let $d = 1_G$, then $\phi_{1_G} =$ id, and thus $a\phi_b(c) = ca = ac \implies \phi_b(c) = c\ \forall b, c$, and thus ϕ is trivial. □

Exercise 8.2. *Let N, H be 2 subgroups of a group G such that $H \leq N_G(N)$, so that $\theta : H \mapsto \text{Aut}(N)$, $\theta_h(n) = hnh^{-1}$, is a homomorphism. Consider the semidirect product $N \rtimes_\theta H$ and the map $f : N \rtimes_\theta H \mapsto G$, defined by $f(n,h) = nh$. Prove that*

1. *f is a homomorphism.*
2. *$ker\ f \cong N \cap H$.*

Proof. The proofs are:

1. $f((n_1,h_1)\cdot(n_2,h_2)) = f(n_1\theta_{h_1}(n_2), h_1h_2) = f(n_1h_1n_2h_1^{-1}, h_1h_2) = n_1h_1n_2h_1^{-1}h_1h_2 = n_1h_1n_2h_2 = f(n_1,h_1)\cdot f(n_2,h_2)$
2. $\ker f = \{(g, g^{-1}) : g \in N \cap H\}$. Consider the map $\alpha : \ker f \mapsto N \cap H$, $\alpha(g, g^{-1}) = g^{-1}$. Clearly α is bijective. Moreover, $\alpha((g_1, g_1^{-1})\cdot(g_2, g_2^{-1})) = \alpha((g_2g_1, g_1^{-1}g_2^{-1})) = g_1^{-1}g_2^{-1} = \alpha(g_1, g_1^{-1})\cdot\alpha(g_2, g_2^{-1})$, and thus α is a homomorphism, and consequently an isomorphism.

□

Exercise 8.3 (N/C Theorem)**.** *Let $H \leq G$ be groups. Show that $N_G(H)/C_G(H)$ is isomorphic to some subgroup of* Aut(H).

Proof. Note that $N_G(H)$ acts by conjugation on H, and thus there is a homomorphism $N_G(H) \mapsto \text{Aut}(H) : n \mapsto \theta_n(h \mapsto nhn^{-1})$. Clearly the kernel of this homomorphism is $C_G(H) \leq N_G(H)$. Thus by the first isomorphism theorem $N_G(H)/C_G(H)$ is isomorphic to some subgroup of Aut(H). □

Exercise 8.4. *Let G be a group of order n, and let A be a normal subgroup of order p, which is prime. Suppose $gcd(p-1, n) = 1$. Prove that $A \leq Z(G)$.*

Proof. Note that G acts on A by conjugation, and thus there is a homomorphism $\theta_g(a) := gag^{-1}$ from G to Aut(A). Now, $A \cong \mathbb{Z}/p\mathbb{Z}$, and thus $\text{Aut}(A) \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Since $\gcd(p-1, n) = 1$, this homomorphism must be trivial [16]. Consequently, $\theta_g(a) = a\ \forall a \in A, g \in G$. But that implies $A \leq Z(G)$. □

Aliter. Since $A \trianglelefteq G$, $N_G(A) = G$. Thus by the N/C theorem, $G/C_G(A)$ is isomorphic to some subgroup of $\text{Aut}(A) \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Thus $n/|C_G(A)|\big|(p-1)$, and consequently, if $C_G(A) \neq G$ then we'll have $\gcd(n, p-1) > 1$, leading to a contradiction.
Thus $C_G(A) = G \implies A \leq Z(G)$. □

Exercise 8.5. *In a group of odd order, no nontrivial element is conjugate to its inverse.*

Proof. Let $x^{-1} = g_0xg_0^{-1}$. Now,

$$x^{-1} = g_0xg_0^{-1} \implies g_0 = xg_0x \implies x^kg_0x^k = g_0\ \forall k \in \mathbb{N}$$

Define the map $\theta_g : x \mapsto gxg^{-1}$. Thus θ_{g_0} takes $\langle x\rangle$ to itself. Moreover, note that restricted to $\langle x\rangle$, $\theta_{g_0} \circ \theta_{g_0} = \theta_{g_0}^2$ is identity.

[16] otherwise the order of elements not in the kernel of the homomorphism must divide both $p-1$ and n, leading to a contradiction

Now, note that $H := N_G(\langle x \rangle)$ acts by conjugation on $\langle x \rangle$, and $g_0 \in H$. Thus θ is the conjugation homomorphism from H to $\mathrm{Aut}(\langle x \rangle)$, and by the first isomorphism theorem $H/\ker\theta \cong \mathrm{im}\ \theta$. But

$$|H/\ker\theta| = \frac{|H|}{|\ker\theta|} = \frac{|G|}{|G/H||\ker\theta|}$$

is odd, and thus im θ, being isomorphic to $H/\ker\theta$, doesn't contain elements of even order. However $\theta_{g_0} \in \mathrm{im}\ \theta$ is an element of order two, leading to a contradiction. □

Exercise 8.6. *Let G be a group, and let H and K be subgroups of G. Define the* set $HK := \{hk : h \in H, k \in K\}$. *Prove that*

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Proof. Consider the group action, with the group $H \times K$ acting on the set HK as

$$(h,k) \cdot x := hxk^{-1}, (h,k) \in H \times K, x \in HK$$

This is indeed a group action since for any $(h_1,k_1),(h_2,k_2) \in H \times K$,

$$(h_2,k_2) \cdot ((h_1,k_1) \cdot x) = (h_2,k_2) \cdot (h_1 x k_1^{-1}) = h_2 h_1 x k_1^{-1} k_2^{-1} = (h_2h_1, k_2k_1) \cdot x$$

This action is also easily seen to be transitive. Thus by the Orbit Stabilizer theorem

$$|HK| = \frac{|H \times K|}{|\mathrm{Stab}(s)|} = \frac{|H| \cdot |K|}{|\mathrm{Stab}(s)|}$$

for any $s \in HK$. In particular we may choose $s = 1$ to yield $\mathrm{Stab}(1) = \{(h,h) : h \in H \cap K\} \implies |\mathrm{Stab}(1)| = |H \cap K|$, which yields the desired formula. □

Exercise 8.7. *Any group of order p^2 is abelian.*

Proof. Note that any group G acts on itself by conjugation. By the class formula in that contex, we have

$$|G| = |Z(G)| + \sum_{g_i \notin Z(G), i \in \mathcal{I}} \frac{|G|}{\mathrm{Stab}(g_i)}$$

If G is a p-group, then $|G|$ and $\frac{|G|}{\mathrm{Stab}(g_i)}$ are both divisible by p, and thus $Z(G)$ is also divisible by p.
Thus, if $|G| = p^2$, then $|Z(G)| = p, p^2$. We'll show that $|Z(G)| = p$ can't happen. To that end, note that if $|Z(G)| = p$, then $G/Z(G)$ is a cyclic group of p elements. Now it's well known that if $G/Z(G)$ is cyclic, then G is abelian, contradicting the fact that $|Z(G)| < |G|$. Thus G is abelian. □

9 Sylow Groups

Exercise 9.1. *Let G be a finite group such that $|G| = pqr$, where $p < q < r$ are primes. Prove that the r-Sylow subgroup of G is normal.*

Proof. We first show that some Sylow-subgroup of G must be normal. Assume for the sake of contradiction that the number of p, q, r-Sylow subgroups of G, denoted by n_p, n_q, n_r respectively, are all greater than 1. Also note that all these Sylow-subgroups share no common elements other than 1.

Then since $n_\ell \equiv 1 \bmod \ell$ and $n_\ell \Big| pqr$ for $\ell \in \{p, q, r\}$, we have $n_r = pq, n_q \geq r, n_p \geq q$. Then the total number of non-identity elements contained in these Sylow groups is $\geq pq(r-1) + r(q-1) + q(p-1) = pqr - 1 + (r-1)(q-1) > pqr - 1$, contradicting the fact that there are only $pqr - 1$ non-identity elements in G.

Now, if the Sylow-subgroup which was normal was the r-Sylow subgroup, then we are done. Otherwise $n_r = pq$, and $pq(r-1) = pqr - pq$ elements in G have order r, leaving behind $pq - 1$ non-identity elements to account for.

Let P be the p-Sylow subgroup of G, and say P is the normal Sylow-subgroup of G. Since P is normal, PQ and PR are subgroups of G, where Q, R are any q and r-Sylow subgroups. Then we have $p-1$ elements of order p from P, $q-1$ elements of order q from Q, $(p-1)(q-1)$ elements of order pq from PQ[17], and $(p-1)(r-1)$ elements of order pr from PR, which gives us a total of $pq - 1 + (p-1)(r-1) > pq - 1$ distinct non-identity elements, leading to a contradiction.

If Q is the normal Sylow subgroup of G, a contradiction can be derived as in the above paragraph. □

Exercise 9.2. *Let G be a finite group such that $|G| = p^\alpha$, where p is a prime and $\alpha \in \mathbb{N}$. Then prove that G has normal subgroups of order p^k for all $k \in [\alpha]$.*

Proof. If $\alpha = 1$, the statement is trivially true. We now proceed by induction.

We shall also use a weaker version of the above problem statement in the proof below, which goes as "Every p-group has p-subgroups of every order possible". We're trying to strengthen this statement to add "normal" in it.

By usual class formula arguments, since G is a p-group, we know that $Z(G)$ is not trivial. Thus let $|Z(G)| = p^\beta$, where $0 < \beta < \alpha$[18].

For $\alpha > 1$, for $k \leq \beta$, we can simply take subgroups of $Z(G)$ of order p^k, and be done with [19]. For $k > \beta$, consider the projection epimorphism $\pi : G \longrightarrow G/Z(G) =: H$. Since H is a p-group of order $p^{\alpha-\beta} < p^\alpha$, it has a normal subgroup (say H') of order $p^{k-\beta}$ by our induction hypothesis. Then $\pi^{-1}(H')$ is a normal subgroup of G[20]. But $\pi^{-1}(H')/Z(G) = H' \implies |\pi^{-1}(H')| = |H'| \cdot |Z(G)| = p^{k-\beta} \cdot p^\beta = p^k$, as desired. □

Exercise 9.3. *Let G be a group, $N \trianglelefteq G$ be a normal subgroup of G, and P be a p-Sylow subgroup of G for some prime p dividing $|G|$. Show that $N \cap P$ is a p-Sylow subgroup of N.*

Proof. Since $N \trianglelefteq G$,

$$gN = Ng \; \forall g \in G \implies gN = Ng \; \forall g \in P \implies PN = NP$$

Thus $PN \leq G$. From the product of groups formula proved in the Group Actions exercises, we have

$$|PN| = \frac{|P| \cdot |N|}{|P \cap N|} \implies \frac{|PN|}{|P|} = \frac{|N|}{|P \cap N|}$$

We introduce a notation at this point, which is

$$\nu_p(n) := \ell, \text{ where } p^\ell \big| n, p^{\ell+1} \nmid n, \; n \in \mathbb{N}, \; p \text{ prime}$$

Now, note that $G \geq PN \geq P$, and thus $\nu_p(|G|) \geq \nu_p(|PN|) \geq \nu_p(|P|)$. However, since P is a p-Sylow subgroup, $\nu_p(|P|) = \nu_p(|G|)$, and consequently, $\nu_p(|PN|) = \nu_p(|P|)$, which implies that $\nu_p(|PN|/|P|) = \nu_p(|N|/|P \cap N|) = 0$,

[17] Let $\alpha \in P, \beta \in Q$. Then since $P \trianglelefteq G$, $\beta\alpha\beta^{-1} = \alpha' \in P \implies \beta\alpha = \alpha'\beta \implies (\alpha\beta)^r$ can be written as $\alpha''\beta''$ for $\alpha'' \in P, \beta'' \in Q$, and then $o(\alpha\beta)$ can be deduced to be pq

[18] $\beta = \alpha$ would imply that G is abelian. Now, we already know that p-groups have subgroups of every order $p^k, k \leq \alpha$, and G being abelian would imply that all of them were normal too, and thus we would be done

[19] note that any subgroup of $Z(G)$ is normal in G

[20] by the Third Isomorphism Theorem normal subgroups of a group and it's quotient correspond naturally under the projection map

implying $\nu_p(|N|) = \nu_p(|P \cap N|)$. Now, since $P \cap N \leq P$, $P \cap N$ is a p-group. Thus $P \cap N$ is a p-group, which is also a subgroup of N such that the power of p dividing it's order is equal to the power of p dividing the order of N, and thus $P \cap N$ is a p-Sylow subgroup of N. □

10 Exact Sequences

Exercise 10.1. *Let $1 \to G' \xrightarrow{\alpha} G \xrightarrow{\beta} G'' \to 1$ be a split short exact sequence of groups. Prove that $G \cong G' \rtimes G''$.*

Proof. We know that $N := \ker(\beta)$ is normal in G. We also have $G'/\ker(\alpha) \cong \text{im}(\alpha) = N$. But since α is a monomorphism, $\ker(\alpha)$ is the trivial group, and thus $G'/\ker(\alpha) \cong G'$, and thus $G' \cong N$. Consequently, $G' \rtimes_\theta G'' \cong N \rtimes_\theta G''$.
Note that since we have a split sequence, there exists a homomorphism $s : G'' \mapsto G$ such that $\beta \circ s = \text{id}_{G''}$. Then consider the homomorphism

$$G'' \xrightarrow{\theta} \text{Aut}(N)$$
$$\theta_{g''}(n) := s(g'')ns(g'')^{-1}$$

Then

- $\theta_{g''}$ is an automorphism:
  1. $\theta_{g''}(n_1n_2) = s(g'')n_1n_2s(g'')^{-1} = s(g'')n_1s(g'')^{-1} \cdot s(g'')n_2s(g'')^{-1} = \theta_{g''}(n_1) \cdot \theta_{g''}(n_2)$. Thus $\theta_{g''}$ is an homomorphism.
  2. $\theta_{g''}(n_1) = \theta_{g''}(n_2) \iff s(g'')n_1s(g'')^{-1} = s(g'')n_2s(g'')^{-1} \iff n_1 = n_2$. Thus $\theta_{g''}$ is injective.
  3. $n = \theta_{g''}(s(g'')^{-1}ns(g''))$ for all $n \in N$. Thus $\theta_{g''}$ is surjective, and thus an automorphism.
- θ is a homomorphism:
  1. $\theta_{g_1''} \circ \theta_{g_2''}(n) = s(g_1'')(s(g_2'')ns(g_2'')^{-1})s(g_1'')^{-1} = \theta_{g_1''g_2''}(n)$. Thus θ is a homomorphism. Here we used the fact that s is a homomorphism.

To establish the isomorphism $N \rtimes_\theta G'' \cong G$, consider the map

$$\varphi : N \rtimes_\theta G'' \mapsto G : (n, g'') \mapsto ns(g'')$$

Then

1. $\varphi((n_1, g_1'') \cdot (n_2, g_2'')) = \varphi(n_1\theta_{g_1''}(n_2), g_1''g_2'') = n_1s(g_1'')n_2s(g_1'')^{-1} \cdot s(g_1''g_2'') = n_1s(g_1'')n_2s(g_1'')^{-1}s(g_1'')s(g_2'') = n_1s(g_1'')n_2s(g_2'') = \varphi(n_1, g_1'') \cdot \varphi(n_2, g_2'')$. Thus φ is an homomorphism.
2. $n_1s(g_1'') = n_2s(g_2'') \iff n_2^{-1}n_1 = s(g_2''(g_1'')^{-1}) \iff \beta(n_2^{-1}n_1) = \beta(s(g_2''(g_1'')^{-1})) \iff 1 = g_2''(g_1'')^{-1} \iff g_1'' = g_2'', n_1 = n_2$. Thus φ is injective.
3. Given $g \in G$, consider $g'' := \beta(g)$, $n := gs(g'')^{-1}$. Then $g = \varphi(n, g'')$, and thus φ is surjective.

Thus φ is an isomorphism, as desired. □

Exercise 10.2. *Prove that $Z(\text{GL}_n(\mathbb{C})) = \{aI_n : a \in \mathbb{C}^\times\}$.*

Proof. Consider a diagonal matrix $D \in \mathrm{GL}_n(\mathbb{C})$ such that all the diagonal entries of D are distinct complex numbers. Consider $A \in Z(\mathrm{GL}_n(\mathbb{C}))$. Then $AD = DA$, and we have

$$(AD)_{ij} = \sum_{k=1}^{n} a_{ik}d_{kj} = a_{ij}d_{jj}$$

$$(DA)_{ij} = \sum_{k=1}^{n} d_{ik}a_{kj} = a_{ij}d_{ii}$$

If $i \neq j$, then $a_{ij}d_{jj} = a_{ij}d_{ii}$ implies $a_{ij} = 0$, since $d_{ii} \neq d_{jj}$. Thus A is a diagonal matrix.
Now if we have $a_{ii} \neq a_{jj}$ for some $i < j$, then note that choosing[21] $M \in \mathrm{GL}_n(\mathbb{C})$ such that $m_{ij} \neq 0$ yields, on equating the $(ij)^{\text{th}}$ positions of AM and MA, $a_{ii}m_{ij} = a_{jj}m_{ij}$, leading to a contradiction.
Thus $a_{ii} = a_{jj}$ for all i, j, and thus A is a scalar matrix, as desired.
Note: The above proof verbatim, with GL_n replaced by $\mathbb{B}_n$, also shows that $Z(\mathbb{B}_n) = \{aI_n : a \in \mathbb{C}^\times\}$. □

Exercise 10.3. *Prove that the extension* $1 \to \mathrm{SL}_n(\mathbb{C}) \hookrightarrow \mathrm{GL}_n(\mathbb{C}) \xrightarrow{\det} \mathbb{G}_m(\mathbb{C}) \to 1$ *is split.*

Proof. Let

$$s : \mathbb{G}_m(\mathbb{C}) \mapsto \mathrm{GL}_n(\mathbb{C}) : z \mapsto \begin{bmatrix} z & \mathbf{0}^\mathsf{T} \\ \mathbf{0} & I_{n-1} \end{bmatrix}$$

s is obviously a homomorphism, and $\beta \circ s = \mathrm{id}_{\mathbb{G}_m(\mathbb{C})}$. □

Exercise 10.4. *For* $a \in \mathbb{C}^\times, b \in \mathbb{C}$, *write* $f(a,b) := \begin{bmatrix} a & b \\ 0 & 1/a \end{bmatrix}$. *Let* $B = \{f(a,b) : a \in \mathbb{C}^\times, b \in \mathbb{C}\}$. *Prove that*

1. *B is not commutative.*
2. *If $\alpha(b) = f(1,b)$ and $\beta(f(a,b)) = a$, then $1 \to \mathbb{G}_a(\mathbb{C}) \xrightarrow{\alpha} B \xrightarrow{\beta} \mathbb{G}_m(\mathbb{C}) \to 1$ is a split short exact sequence.*

Proof. We can see that

1. $\begin{bmatrix} 2 & 1 \\ 0 & 1/2 \end{bmatrix} \cdot \begin{bmatrix} 3 & 1 \\ 0 & 1/3 \end{bmatrix} = \begin{bmatrix} 6 & 7/3 \\ 0 & 1/6 \end{bmatrix} \neq \begin{bmatrix} 6 & 7/2 \\ 0 & 1/6 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 0 & 1/3 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 0 & 1/2 \end{bmatrix}$
2. α is injective, β is surjective, and both are clearly homomorphisms. Also, $\mathrm{im}(\alpha) = \ker(\beta) = \mathbb{U}_2(\mathbb{C})$, and thus this is a short exact sequence. Finally $s : \mathbb{G}_m(\mathbb{C}) \mapsto B : a \mapsto f(a,0)$ is a homomorphism, and we also have $\beta \circ s = \mathrm{id}_{\mathbb{G}_m(\mathbb{C})}$, and thus this is a split short exact sequence.

□

Exercise 10.5. *Let for* $a, b, c \in \mathbb{C}, u(a,b,c) := \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$. *Let* $G = \mathbb{U}_3(\mathbb{C}) := \{u(a,b,c) : a, b, c \in \mathbb{C}\}$. *Let* $\beta : G \to \mathbb{G}_a(\mathbb{C})^2 : u(a,b,c) \mapsto (a,c)$. *Prove that β is a group homomorphism and there is a central short exact sequence as follows, where* $\alpha(b) = u(0,b,0)$:

$$1 \to \mathbb{G}_a(\mathbb{C}) \xrightarrow{\alpha} \mathbb{U}_3(\mathbb{C}) \xrightarrow{\beta} \mathbb{G}_a(\mathbb{C})^2 \to 1$$

[21] we can choose the permutation matrix of $\sigma = (i\ j)$. It has $m_{ij} = 1$, and is invertible.

Proof.

$$u(a,b,c)\cdot u(a',b',c') = u(a+a', b+b'+ac', c+c')$$

Thus β is an epimorphism.
Also α is clearly a monomorphism, and $\mathrm{im}(\alpha) = \{u(0,b,0) : b \in \mathbb{C}\} = \ker(\beta)$. But note that

$$u(a,b,c)\cdot u(0,b',0) = u(a,b+b',c) = u(0,b',0)\cdot u(a,b,c)$$

Thus $\mathrm{im}(\alpha) \leq Z(G)$, and thus the sequence is central. □

Exercise 10.6. *Which of the following properties do extensions preserve? Provide proofs or counterexamples. Note that when we enquire if extensions preserve a property $\mathcal{P}$, we mean that in the short exact sequence $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$, if **both** A and C possess the property $\mathcal{P}$, then does B also necessarily possess $\mathcal{P}$?*

1. *Cyclicity*
2. *Abelianity*
3. *"finitely-generated"ness*
4. *Finiteness*
5. *"p-group"ness*
6. *Periodicity (A group G is called periodic of every element in G has finite order)*
7. *Torsion-freeness (A group G is called torsion-free if every element in G other than 1 has infinite order)*

Proof. The proofs and counterexamples are as follows:

1. **False**: Every semi-direct product can be realized as an extension, and since $\mathfrak{S}_3 \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ is not cyclic, we have a counterexample. Since $\mathfrak{S}_3$ isn't abelian either, we have another counterexmaple for the next part.
2. **False**: A counter example is given by the abelian groups $G' = \mathbb{G}_a(\mathbb{C})$, $G'' = \mathbb{G}_a(\mathbb{C})^2$, whose group extension given in the previous exercise generated a **non-abelian** group $(\mathbb{U}_3(\mathbb{C}), \cdot)$.
3. **True**: Indeed, $C \cong B/\ker(\beta) = B/\mathrm{im}(\alpha)$. Since A is f.g., $\mathrm{im}(\alpha)$ is f.g. too. Thus, we shall now prove that if $G/N = H$, with N, H being f.g., then G is a f.g. too.
   To that end, for any $g \in G$, we have $g = y_g n \in y_g N \in H$. Since H is finitely generated, and if $\overline{Y}$ is a finite generating set of H, then y_g is a word on elements of $Y := \pi^*(\overline{Y})$ [22], and since N is f.g. too, n is a word on the generators of N (let X be a finite generating set of N), and thus a word for g can be formed by concatenating the Y-word for y_g and the X-word for n, leading to $g \in \langle X \cup Y\rangle \implies G \subseteq \langle X \cup Y\rangle$.
   Conversely, one notes that since $N \trianglelefteq G$[23], we have that for any $y \in G, x \in N\ \exists x' \in N$ such that $yx = x'y$, and thus for any word in $w \in \langle X \cup Y\rangle$, if any member of X immediately precedes a member of Y in w, one can swap them. Consequently, every word in $\langle X \cup Y\rangle$ is equal to the concatenation of a Y-word and a X-word[24]. But from our above discussion such a word generates a member of G, and thus $\langle X \cup Y\rangle \subseteq G$. Hence $G = \langle X \cup Y\rangle$, and thus is f.g.

[22] $\pi^*(\overline{Y})$ is the set comprised of $y \in G$ such that for every $\overline{y} \in \overline{Y}$ there is a **unique** $y \in \pi^*(\overline{Y})$ such that $\overline{y} = \pi(y) = yN$. Note that we can't simply set $Y = \pi^{-1}(\overline{Y})$ since if N is infinite, then Y becomes infinite

[23] this symbol denotes that N is normal in G. Also, N is indeed normal in G since we're talking of the quotient G/N as a group

[24] either of them possibly empty

4. **True**: Since we have $C \cong B/\text{im}(\alpha)$ and $|\text{im}(\alpha)| = |A|$, we have that $|B| = |C| \cdot |A|$.

5. **True**: $|B| = |C| \cdot |A|$.

6. **True**: For any $b \in B$, $\beta(b) \in C \implies \exists n\ \beta(b)^n = 1 \implies b^n \in \ker(\beta) \implies b^n \in \text{im}(\alpha) \implies \exists a \in A\ \alpha(a) = b^n$. Since $a \in A$, $\exists n'\ a^{n'} = 1 \implies \alpha(a^{n'}) = b^{nn'} \implies 1 = b^{nn'}$, and thus b has finite order.

7. **True**: If we have $b^n = 1_B$ for some $b \in B$, then $\beta(b)^n = 1_C \implies \beta(b) = 1_C$ since C is torsion-free. But that implies $b \in \ker(\beta) \implies b \in \text{im}(\alpha) \implies \exists a \in A\ \alpha(a) = b \implies \alpha(a^n) = 1 \implies a^n = 1 \implies a = 1 \implies b = 1$, and thus B is torsion-free.

□

Exercise 10.7. *Let N be the set of strictly upper triangular matrices with coefficients in $\mathbb{C}$. Let $\mathbb{U}_n(\mathbb{C}) = I_n + N$. Prove that*

1. *$N^n = 0$ that is, for $g_1, \ldots, g_n \in N, g_1 \cdots g_n = 0$.*
2. *$\mathbb{U}_n(\mathbb{C})$ is a subgroup of $\text{GL}_n(\mathbb{C})$.*
3. *For $a \in N^i, b \in N^j, [1+a, 1+b] = (1+a)(1+b)(1+a)^{-1}(1+b)^{-1} \in I_n + N^{i+j}$.*

Proof. The proofs are as follows:

1. We claim that if $M \in N^k$, $k \in [n]$, then $M_{i,t} = 0$ for $i \in [n], t \in [\min(i+k-1, n)]$. That automatically shows $N^n = 0$.
   The claim is true for $k = 1$ by the definition of N. If the claim is true for $k \in [r-1]$, then by induction $(M = M'N, M' \in N^{k-1})$

$$M_{i,t} = \sum_{l=1}^{n} M'_{i,l} N_{l,t} = \sum_{l=i+r-1}^{n} M'_{i,l} N_{l,t} = 0,\ t \in [\min(i+r-1, n)]$$

   as desired.

2. Note that I_n is the identity of $I_n + N$[25]. Also, note that N is a semi-group under multiplication (thus $N^k \subseteq N$ for any $k \in \mathbb{N}$) and group under addition. Moreover, for any $M \in N$ it's easy to verify that

$$(I_n + M)^{-1} = I_n + \sum_{k=1}^{n-1} (-M)^k \in I_n + N$$

   Also

$$(I_n + M_1) \cdot (I_n + M_2) = I_n + M_1 + M_2 + M_1 M_2 \in I_n + N$$

   Thus $I_n + N$ is a group.

3. Continuing from the above, we make the following observations:

   - $N^i \subseteq N^j$ for $i \geq j$
   - If $a \in N^i$, $b \in N^j$ then $a + b \in N^{\min(i,j)}$

[25] under multiplication

- If $a \in N$, then $(1-a)^{-1} = 1 + \sum_{k=1}^{\infty} a^k = 1 + \sum_{k=1}^{n-1} a^k$

Also, since $(N, +)$ is a group, we replace a, b by $-a, -b$ in the expression for convenience, to get

$$(1-a)(1-b)(1-a)^{-1}(1-b)^{-1} = (1-a-b+ab)\left(1 + \sum_{\ell_1+\ell_2 \geq 1} a^{\ell_1} b^{\ell_2}\right)$$

Now, it's easy to see that when the above expression is opened, we'll get something of the form $1 + f(a,b)$, where $f(a,b)$ is a sum of product of a's and b's, such that there is atleast one a and one b in every product. Then note that every term in $f(a,b)$ must belong to N^{i+j}, and thus $f(a,b) \in N^{i+j}$, thus finishing the proof.

□

11 Nilpotent and Solvable Groups

Exercise 11.1. *Let Q, N be two abelian groups. Let $\theta : Q \to \mathrm{Aut}_{\mathrm{gr}}(N)$ be a group homomorphism and $G = N \rtimes_\theta Q$ the corresponding semidirect product. Prove that G is solvable.*

Proof. Consider the subnormal series

$$\{1\} \trianglelefteq N' \trianglelefteq G$$

where $N' := \{(n, 1) : n \in N\} \trianglelefteq G$ is the normal subgroup of G induced by N. Moreover, $N'/\{1\} \cong N$ is abelian, $G/N' \cong Q$ is abelian. Thus G is solvable. □

Exercise 11.2. *Prove the following statements:*

1. *The dihedral groups D_n are all solvable.*
2. *The dihedral group D_n is nilpotent if and only if it is a 2-group. [This gives a class of nilpotent groups which are non-abelian and semidirect product of cyclic subgroups.]*

Proof. The proofs are as follows:

1. Since $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$, by the previous result we're done.
2. If D_n is a 2-group, then it's nilpotent since any p-group is nilpotent.
   The statement is true for $n = 2$, so assume $n > 2$. If D_n is nilpotent, then by the classification of finite nilpotent groups we have that it is the product of its Sylow subgroups, all of which are normal. Thus, let

$$D_n = P_1 \times P_2 \times \cdots \times P_r \implies Z(D_n) = \bigotimes_{i=1}^{r} Z(P_i)$$

   But $|Z(D_n)| = 1, 2$ as shown in the Dihedral Groups exercises. Thus, if $p \big| n$, where p is an odd prime, then $p \big| |Z(P)| \implies p \big| |Z(D_n)|$[26], which is a contradiction.

□

Exercise 11.3. *Prove that any group G of order pq, where $p < q$ are primes, is solvable.*

[26] Since P is a p-Sylow subgroup, the size of it's center is divisible by p by class equation arguments

Proof. Consider the subnormal series

$$\{1\} \trianglelefteq Q \trianglelefteq G$$

where Q is the q-Sylow subgroup of G. Then the normality relation "$\{1\} \trianglelefteq Q$" is obvious, and the normality relation "$Q \trianglelefteq G$" holds because $|G : Q| = p$ is the smallest prime divisor of $|G|$. Also note that $Q/\{1\}$ has order q, and thus is abelian, and similarly, G/Q has order p, and thus is abelian.
Consequently, G is solvable. □

Exercise 11.4. *Prove that any group G of order pqr, where $p < q < r$ are primes, is solvable.*

Proof. Consider the subnormal series

$$\{1\} \trianglelefteq R \trianglelefteq RQ \trianglelefteq G$$

where R, Q are r, q-Sylow subgroups of G respectively.
From the Sylow theory exercises, we know that $R \triangleleft G$. Since R is normal, RQ is a subgroup of G. Also, since $|G : RQ| = p$ is the smallest prime divisor of G, $RQ \triangleleft G$. Finally, note that the the order of every quotient of consecutive members of this series is a prime, and thus all the quotient groups are abelian. Consequently, G is solvable. □

Exercise 11.5. *Show that the alternating group $\mathfrak{A}_4$ is solvable.*

Proof. One can note that $(1,2,3)$, $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(2,3,4)$, $(2,4,3)$, $(1,3,4)$, $(1,4,3)$ are 8 members of $\mathfrak{A}_4$ with order 3. That leaves us with exactly 4 elements which don't have an order of 3, and we recognize these elements to be part of the unique 2-Sylow subgroup (let's call it P) of $\mathfrak{A}_4$. Since the Sylow subgroup is unique, it's normal, and we thus have the following subnormal series:

$$1 \trianglelefteq P \trianglelefteq \mathfrak{A}_4$$

The normalities are obvious, and one notes that $|P : 1| = 4, |\mathfrak{A}_4 : P| = 3$. Since any group of size 3 or 4 is abelian, we get that the quotients are abelian too, and thus $\mathfrak{A}_4$ is solvable. □

Exercise 11.6. *Calculate the derived series of $\mathfrak{S}_4$.*

Proof. Let $G := \mathfrak{S}_4$, and let $A := \mathfrak{A}_4$. Note that $A \triangleleft G$.
Since $G/A \cong \mathbb{Z}_2$ is abelian, $G^{(1)} \leq A$. Further note that since $(a,b,c) = [(a,b),(a,c)]$, $G^{(1)}$ contains all 8 3-cycles. Consequently, $G^{(1)} = A$. Now, let P be the 2-Sylow subgroup of A. We have seen that P is normal, and moreover $A/P \cong \mathbb{Z}_3$ is abelian. Thus $G^{(2)} = A^{(1)} \leq P$, and thus $|G^{(2)}| = 1, 2, 4$. Since A isn't abelian, $|G^{(2)}| \neq 1$. But note that $[(a,b,c),(a,b,d)] = (a,b)(c,d)$, and thus $G^{(2)}$ contains $(1,3)(2,4)$, $(1,4)(2,3)$ and $(1,2)(3,4) = \mathrm{id}$, and thus $|G^{(2)}| > 2$, and thus $G^{(2)} = P$. Since P is abelian, $G^{(3)} = 1$. Also note that $P \cong \mathbb{Z}_2^2 =: K_4$
Thus the derived series of $\mathfrak{S}_4$ is

$$\mathfrak{S}_4 \triangleright \mathfrak{A}_4 \triangleright K_4 \triangleright 1$$

□

Exercise 11.7. *Let G be a finite group. Prove that G is nilpotent if and only if for every divisor d of $n := |G|$, G has a normal subgroup of order d.*

Proof. If G has normal subgroups of the order of every divisor of n, then all Sylow subgroups of G must be normal. Consequently G is a direct product of its Sylow subgroups and thus is nilpotent.
If G is nilpotent, then all Sylow subgroups of G are normal. Let p be any prime divisor of n. From the Sylow theory exercises we know that the p-Sylow subgroup of G has normal subgroups of order p^α for all $\alpha \in [\nu_p(n)]$. Thus for any divisor $d = \prod_{i=1}^r p_i^{k_i}$ of $n = \prod_{i=1}^r p_i^{\ell_i}$, choose normal subgroups N_i of order $p_i^{k_i}$ from the p_i-Sylow subgroups. Since all the N_i's are normal, $N_1 \times N_2 \times \cdots N_r \trianglelefteq P_1 \times P_2 \times \cdots P_r = G$ is a normal subgroup of G of order d, as desired. □

Exercise 11.8. *Let $G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \dots$ be the derived series of a group G. Prove that if $G^{(1)}/G^{(2)}$ and $G^{(2)}/G^{(3)}$ are both cyclic, then $G^{(2)} = G^{(3)}$.*

Proof. Consider the projection epimorphism $\pi : G \mapsto G^{(3)}$, and project $G^{(i)}$, $i \leq 3$ by π. Then for any $i, j \leq 3$, by the third isomorphism theorem,

$$\frac{\pi(G^{(i)})}{\pi(G^{(j)})} = \frac{G^{(i)}/G^{(3)}}{G^{(j)}/G^{(3)}} \cong \frac{G^{(i)}}{G^{(j)}}$$

Thus WLOG assume $G^{(3)} = 1$, and thus $G^{(1)}/G^{(2)}$ and $G^{(2)}$ are cyclic groups. Since $G^{(2)} \trianglelefteq G$, $N_G(G^{(2)}) = G$, and thus by the N/C theorem $G/C_G(G^{(2)})$ is isomorphic to some subgroup of $\mathrm{Aut}(G^{(2)})$. Since $G^{(2)}$ is cyclic, $\mathrm{Aut}(G^{(2)})$ is abelian, and thus $G/C_G(G^{(2)})$ is abelian, implying $C_G(G^{(2)}) \geq G^{(1)} \implies G^{(2)} \leq Z(G^{(1)})$. Now exactly similar to the proof of the $G/Z(G)$ theorem, $G^{(1)}/G^{(2)}$ being cyclic with $G^{(2)} \leq Z(G^{(1)})$ implies that $G^{(1)}$ is abelian, which further implies that $G^{(2)} = 1 = G^{(3)}$, as desired. □

Exercise 11.9. *Prove that there doesn't exist a group G such that $[G, G] \cong \mathfrak{S}_4$.*

Proof. If $G^{(1)} = \mathfrak{S}_4$, then $G^{(2)} = \mathfrak{A}_4, G^{(3)} = K_4$, and $G^{(1)}/G^{(2)} \cong \mathbb{Z}_2$ is cyclic, $G^{(2)}/G^{(3)} \cong \mathbb{Z}_3$ is also cyclic, yet $G^{(2)} \neq G^{(3)}$, leading to a contradiction. □

Exercise 11.10. *Give an example of a solvable group which is not a semi-direct product of its subgroups. [Hint: Consider the Quaternion group $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, where $i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik$. Show that this group is solvable but not a semi-direct product. Why does such a group exist? How is this group related to Pauli matrices?]*

Proof. Observe that:

1. $[1, x] = [x, 1] = 1$ for any $x \in H_8$
2. $[x, x] = 1$ for any $x \in H_8$
3. $[-a, b] = [a, b] = [a, -b]$ for any $a, b \in H_8$
4. $[a, b] = (ab)^2 = -1$ for any $a, b \in \{i, j, k\}, a \neq b$

Thus

$$H_8^{(1)} := [H_8, H_8] = \langle \{[a, b] : a, b \in H_8\} \rangle = \langle \{1, -1\} \rangle = \{1, -1\}$$

$$H_8^{(2)} := [H_8^{(1)}, H_8^{(1)}] = \{1\}$$

Since $H_8^{(2)} = \{1\}$, H_8 is solvable.
Assume for the sake of contradiction that H_8 is isomorphic to a semi-direct product of it's non-trivial subgroups. Then one of the subgroups must be of size 2, and the other subgroup must be of size 4. Now, it's not hard to see that all subgroups of H_8 of size 2 are isomorphic to $\mathbb{Z}_2$, and all subgroups of size 4 are isomorphic to $\mathbb{Z}_4$.
Thus our choices from the semi-direct product are $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$, $\mathbb{Z}_2 \rtimes \mathbb{Z}_4$. Furthermore, it's not hard to see that the only groups that these semidirect products yield are (isomorphic to) $\mathbb{Z}_8$, D_4. Clearly $H_8 \neq \mathbb{Z}_8$ since H_8 is non-abelian, while $H_8 \neq D_4$ because H_8 has exactly one element of order 2 (-1), while D_4 has atleast 2 elements of order 2 ($\sigma, r^2\sigma$)[27].
Properties and Significance of the Quaternion Group:

- Every subgroup of H_8 is normal.

[27] $r\sigma = \sigma r^{-1} \implies r^2\sigma = r\sigma r^{-1} \implies (r^2\sigma)^2 = r\sigma r^{-1} \cdot r\sigma r^{-1} = 1$

- Along with D_4, it's the smallest non-abelian nilpotent group.
- $\mathrm{Aut}(H_8) \cong \mathfrak{S}_4$
- The Pauli matrices are $\sigma_1 := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_2 := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_3 := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  Then $H_8 = \langle 1, i\sigma_1, i\sigma_2, i\sigma_3 \rangle$.

□

Exercise 11.11. *Prove that every finite group of order > 2 has a nontrivial automorphism using the structure theorem for finite abelian groups in the proof.*

Proof. The non-trivial automorphism for non-abelian groups is constructed as earlier.
A cyclic group of order > 2 possesses the non-trivial automorphism induced by $x \mapsto x^{-1}$, where x is the generator of the group.
Any non-cyclic finite abelian group G can be expressed as a product of cyclic groups, ie:-

$$G \cong C_1 \times C_2 \times \cdots \times C_r, r > 1$$

[28] Then consider the non-trivial automorphism induced by the mapping of generators

$$(c_1, c_2, \ldots, c_r) \mapsto (c_2, c_1, \ldots, c_r)$$

where c_i is the generator of C_i. □

Exercise 11.12. *Suppose G is a finite abelian group, and let $\widehat{G}$ be the set of all group homomorphisms of $G \to \mathbb{C}^\times$, where $\mathbb{C}^\times$ is the multiplicative group of nonzero complex numbers. For $\phi, \psi \in \widehat{G}$, define their product $\phi\psi$ by $(\phi\psi)(g) = \phi(g)\psi(g)$.*

1. *Prove that $\widehat{G}$ becomes a group.*
2. *Prove that G and $\widehat{G}$ are isomorphic as groups.*

Proof. The proofs are as follows:

1. Let the identity of $\widehat{G}$ be the trivial homomorphism, which maps every element of G to $1_{\mathbb{C}^\times}$. Also, for any $\psi \in \widehat{G}$, define $(\psi)^{-1}(g) := \psi(g)^{-1}$. With this identity and inverse, group axioms (closure, associativity) are easily verified. Note that $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$ is an abelian group.
2. We first prove the theorem for cyclic groups $G = \mathbb{Z}/n\mathbb{Z}$: Consider the isomorphism

   $$\theta : \mathbb{Z}/n\mathbb{Z} \mapsto \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}^\times) : r \mapsto (1 \mapsto e^{2\pi i r/n})$$

   where a homomorphism is specified by mapping the generator 1 of $\mathbb{Z}/n\mathbb{Z}$ to some unit in $\mathbb{C}^\times$.
   Then since $\mathrm{Hom}(\bigotimes_{i=1}^r G_i, K) \cong \bigotimes_{i=1}^r \mathrm{Hom}(G_i, K)$ for any abelian group K, and since for any abelian group G we have $G \cong \bigotimes_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$, we can take the product of the isomorphism of cycles to generate an isomorphism for $G \cong \mathrm{Hom}(G, \mathbb{C}^\times)$.

□

Exercise 11.13. *Does a finite abelian group have elements of every possible order?*

[28] $r > 1$ because G is not cyclic

Proof. No. $\mathbb{Z}_2^2$ doesn't have any element of order 4. Finite abelian groups do have **subgroups** of every possible order though. □

Exercise 11.14. *Let A be an abelian group. Let $a, b \in A$, be two elements of finite order, $m = o(a), n = o(b)$. Prove that there is an element $c \in A$ such that the order of c is the lcm (least common multiple) of m and n.*

Proof. Define $G := \langle a, b\rangle \leq A$. Then G is a finite abelian group. Fix a prime $p \big| \text{lcm}(m, n)$. Then we claim that $\exists g \in G$ such that $\nu_p(o(g)) = \max(\nu_p(m), \nu_p(n)) = \nu_p(\text{lcm}(m, n)) =: k_p$. Indeed, depending on whether $\nu_p(m)$ is $\geq$ or $<$ than $\nu_p(n)$, $g := a$ or b suffices. But since G is a finite abelian group, $G \cong \bigoplus \mathbb{Z}_{p_i^{\ell_i}}$ by the structure theorem. Also, since we have a $g \in G$ with $\nu_p(o(g)) = k_p$, there must be some component $\mathbb{Z}_{p^\ell}$ in $\bigoplus \mathbb{Z}_{p_i^{\ell_i}}$ such that $\ell \geq k_p$. Then, since $\mathbb{Z}_{p^\ell}$ is a p-group, choose an element, say h_p, in it with order p^{k_p}. Now it's easy to see that

$$h := \sum_{p \big| \text{lcm}(m,n)} h_p$$

satisfies $o(h) = \text{lcm}(m, n)$. □

Exercise 11.15. *Let G be a finite nilpotent nonabelian group. Show that there is a prime factor p of $|G|$ such that p^3 divides $|G|$.*

Proof. Since G is a finite nilpotent group, it is isomorphic to the direct product of it's Sylow subgroups. Now, we know that all groups of order p or p^2, where p is a prime, are abelian. Consequently, if there isn't any prime such that $p^3 \big| |G|$, then all Sylow subgroups of G will be abelian, and thus G would be abelian too, leading to a contradiction. □

Exercise 11.16. *Prove that a group of order pq, where $p < q$, is nilpotent if and only if it is abelian.*

Proof. Directly follows from the above exercise. □

Exercise 11.17. *Let G be a finite group. Show that G is nilpotent if and only if $xy = yx$ whenever x, y have relatively prime orders.*

Proof. Let G be a finite group, and let $P_1, P_2, P_3, \ldots, P_r$ be the Sylow subgroups of G corresponding to **different prime divisors** of $|G|$[29]. Then note that $p_1p_2 = p_2p_1$ for any $p_1 \in P_1, p_2 \in P_2$, because they have relatively prime orders, and thus $P_1P_2 = P_2P_1$, implying that P_1P_2 is a subgroup of G. We can similarly extend this to show that $P_1P_2P_3 \cdots P_r \leq G$. But $|P_1P_2P_3 \cdots P_r| = |G|$[30], and thus $P_1P_2P_3 \cdots P_r = G$. From here, it's easy to see that[31]

$$P_1 \times P_2 \times \cdots \times P_r \cong P_1P_2 \cdots P_r = G$$

The P_i's being p-groups are nilpotent, and thus G, being isomorphic to a direct product of nilpotent groups, is nilpotent too.

Conversely, if G is a finite nilpotent group, then it is isomorphic (say, through φ) to the direct product of its Sylow subgroups. Let $\varphi(x) = (x_1, x_2, \ldots, x_r)$ and $\varphi(y) = (y_1, y_2, \ldots, y_r)$ for some $x, y \in G$ respectively, where we have r distinct prime divisors of G, denoted by $\{p_i\}_{1 \leq i \leq r}$. If $\gcd(o(x), o(y)) = 1$, then note that we can't have $x_i \neq 1, y_i \neq 1$ for any index $1 \leq i \leq r$, because otherwise $p_i \big| o(x), p_i \big| o(y)$. Consequently, in the multiplication of the tuples $(x_1, x_2, \ldots, x_r)$ and $(y_1, y_2, \ldots, y_r)$, since for each i one of the multiplicands is always 1, the multiplication of the tuples commute, and thus $xy = yx$ holds when we map back our isomorphism (through φ^{-1}) from tuples to members of G. □

[29] if $|G|$ has only one prime divisor, then it's a p-group and thus nilpotent

[30] Note that since the P_i's have mutually coprime orders, $|P_iP_j| = |P_i| \cdot |P_j|$

[31] one may verify that the group operation for $P_1 \times P_2 \times P_3 \times \cdots \times P_r$ holds due to members from different Sylow subgroups commuting with each other in $P_1P_2P_3 \cdots P_r$

Exercise 11.18. *Prove that a finite group G is nilpotent iff for any $\alpha, \beta \in G$ such that $gcd(o(\alpha), o(\beta)) = 1$, $o(\alpha\beta) = o(\alpha)o(\beta)$.*

Proof. If G is a finite nilpotent group, then similar to the above proof, $o(\alpha\beta) = o(\alpha)o(\beta)$ for elements α, β of co-prime orders.
Conversely, if the order is a multiplicative function for elements of co-prime order, then consider the group $P := P_1P_2 \cdots P_r$, where P_i are Sylow subgroups of G corresponding to different prime divisors. If $P \ni \alpha_1\alpha_2 \dots \alpha_r = \alpha'_1\alpha'_2 \dots \alpha'_r$, then $\alpha_1\alpha_2 \dots \alpha_{r-1} = \alpha'_1\alpha'_2 \dots \alpha'_r\alpha_r^{-1}$. If $\alpha'_r\alpha_r^{-1} \neq 1$, then the RHS has order divisible by p_r, while the LHS doesn't leading to a contradiction. Thus $\alpha_i = \alpha'_i$ for all $i \in [r]$, and thus $|P_1P_2 \dots P_r| = |P_1| \cdot |P_2| \cdots |P_r| \implies G = P_1P_2 \dots P_r$ and we finish as above. □

Exercise 11.19. *Provide an example for a group G and a normal subgroup $N \triangleleft G$ such that N and G/N are nilpotent, but G isn't.*

Proof. Let $G = \mathfrak{S}_3, N = \mathfrak{A}_3$: G clearly isn't nilpotent, while $N \cong \mathbb{Z}_3$ and $G/N \cong \mathbb{Z}_2$ are nilpotent. □

Exercise 11.20. *Any group G is nilpotent if and only if $G/Z(G)$ is nilpotent.*

Proof. We prove the following more general claim:
Let G be a group and let $N \leq Z(G) \leq G$ be a central subgroup of G[32]. Then G is nilpotent if and only if G/N is.
The assertion immediately follows by choosing $N = Z(G)$ in the above claim.
Let G/N be nilpotent, let $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots$ be the lower central series of G, and let π be the projection epimorphism from G to G/N. Then its easy to see that $G'_i := \pi(G_i)$ gives one the lower central series for G/N. In particular, since G/N is nilpotent, $G'_n = 1$ for some n. For that n, $M := G_n \subseteq \pi^{-1}(1) = N$. But note that $G_{n+1} = [G, G_n] = [G, M] = 1$ since M being a subgroup of N is also central, and thus it's commutator with G is 1.
Conversely, if G is nilpotent, then G/N is nilpotent too, since nilpotency is preserved across quotients. □

Exercise 11.21. *Let G be a finite group, M and N two nilpotent normal subgroups such that $G = MN$. Prove that G is nilpotent.*

Proof. We'll show that G is nilpotent by showing all it's Sylow subgroups are unique. To that end, let P be **any** p-Sylow subgroup of G. Define $P_M := P \cap M, P_N := P \cap N$. From the Sylow theory exercises, we know that P_M and P_N are the p-Sylow subgroups of M and N respectively. Furthermore, since M and N are nilpotent, P_M and P_N are the unique p-Sylow subgroups of M and N.
Also note that $M \cap N \trianglelefteq G$: Indeed, let $H := M \cap N$, then $x^{-1}Hx \in x^{-1}Mx = M, x^{-1}Hx \in x^{-1}Nx = N \implies x^{-1}Hx \in M \cap N = H \ \forall x \in G$. Thus $P_H := P \cap H$ is a p-Sylow subgroup of H. Finally, also note that $P_H = P \cap (M \cap N) = (P \cap M) \cap (P \cap N) = P_M \cap P_N$.
Now, from the concatenation of groups formula, we have that

$$|G| = |MN| = \frac{|M| \cdot |N|}{|M \cap N|} \implies \nu_p(|G|) = \nu_p(|M|) + \nu_p(|N|) - \nu_p(|H|)$$

$$\implies \nu_p(|P|) = \nu_p(|P_M|) + \nu_p(|P_N|) - \nu_p(|P_H|)$$

But also

$$|P_MP_N| = \frac{|P_M| \cdot |P_N|}{|P_M \cap P_N|} = \frac{|P_M| \cdot |P_N|}{|P_H|}$$

$$\implies \nu_p(|P_MP_N|) = \nu_p(|P_M|) + \nu_p(|P_N|) - \nu_p(|P_H|)$$

[32] note that any subgroup of $Z(G)$ is automatically normal in G. Since $Z(G)$ is abelian, so is N, and thus N is **nilpotent** too

Thus $\nu_p(|P|) = \nu_p(|P_M P_N|) \implies |P| = |P_M P_N|$, since $|P|$ and $|P_M P_N|$ are just powers of p. But since $P_M, P_N \leq P$, $P_M P_N \subseteq P$, and thus we have that $P_M P_N = P$. But since P_M and P_N were unique, that means P is also unique, since it is uniquely determined by the product $P_M P_N$. □

Exercise 11.22. *Let G be a nilpotent group and N any nontrivial normal subgroup of G. Show that $Z(G) \cap N \neq 1$.*

Proof. Consider the lower central series $\{G_i\}$ of G. Since this is a series which decreases to 1, there exists an index k such that $G_k \cap N \neq 1, G_{k+1} \cap N = 1$.
Now, note that showing that $H \leq Z(G)$ for some $H \leq G$ is equivalent to demonstrating that $[H, G] = 1$. To that end,

$$[G_k \cap N, G] \subseteq [G_k, G] \cap [N, G] = G_{k+1} \cap N = 1$$

Thus $1 \neq G_k \cap N \subseteq Z(G)$, showing that $Z(G) \cap N \neq 1$. □

Exercise 11.23. *Suppose that G is a nonabelian finite group and that intersections of distinct maximal subgroups is trivial. Then G is not simple.*

Proof. Assume for the sake of contradiction the contrary. Also define $n := |G|$.
Let M be a maximal subgroup of G[33] of size m. Since G is simple, $N_G(M) = M$. Now note that M has $n/|N_G(M)| = n/m$ conjugate subgroups in G, all of which are also maximal. Since all maximal subgroups intersect trivially, the conjugate subgroups of M (including M) contain among themselves $k := 1 + (m-1) \cdot n/m$ elements. But since $n > m \geq 2$, $n > k \geq 1 + n/2$. Since $k < n$, the conjugate subgroups of M don't cover G, implying $\exists 1_G \neq a \in G$ which doesn't lie in any conjugate of M. Since $\langle a \rangle$ is a proper subgroup of G, a lies in some maximal subgroup of G, say A. Then all conjugates of A too span atleast $1 + n/2$ elements, and none of these elements except 1_G lie in any conjugate of M, since all maximal subgroups intersect trivially. But then together, we then have $2(1 + n/2) - 1 > n$ distinct elements in G, which is impossible. □

Exercise 11.24. *Finite non-nilpotent group G whose every proper subgroup is nilpotent implies G isn't simple.*

Proof. Assume the contrary, ie:- G is a finite non-nilpotent simple group whose every proper subgroup is nilpotent. Let $\mathscr{H}$ be the set of all subgroups of G which are the intersections of maximal subgroups of G. Let $H := L \cap M$ be maximal in $\mathscr{H}$, where L, M are maximal in G. Since normalizers grow in nilpotent groups, $L \geq N_L(H) > H$. But since H was maximal in $\mathscr{H}$, $N_L(H)$ is not contained in any other maximal subgroup of G. Similarly, $N_M(H)$ too is only contained in M. But $N_G(H) \geq N_L(H), N_M(H)$. Thus $N_G(H) = G$, implying that $H = 1$ since G is simple. But that means that every subgroup in $\mathscr{H}$ is 1, which means all maximal subgroups intersect trivially in G. But that is a contradiction. □

Exercise 11.25. *Let G be a finite group whose every proper subgroup is nilpotent. Then G is solvable.*

Proof. If G is nilpotent, then it's obviously solvable. Otherwise, if G is non-nilpotent, then G isn't simple by the previous exercise. Let N be the maximal normal subgroup of G. Then G/N is a simple group, since otherwise a proper normal subgroup of G/N would have corresponded to a strictly larger normal subgroup of G containing N by the third isomorphism theorem. Moreover, since nilpotency is preserved across quotients, every proper subgroup of G/N is nilpotent. Since G/N is a simple group every proper subgroup of which is nilpotent, G/N is itself nilpotent by the previous exercise. Since G/N is a finite nilpotent group, every Sylow subgroup of G/N is normal. Thus G/N has to have a prime order if it is to be simple, and thus G/N is cyclic...(incomplete proof) □

[33] If G has atleast one proper subgroup, then G must have a maximal subgroup since it's finite. If n is divisible by atleast 2 primes, then the Sylow subgroups are proper subgroups. If G is a p-group, then it has a subgroup of size p, which is proper, since $n > p$ since groups of prime size are abelian

12 Rings, Fields and Ideals

Exercise 12.1. *Give a nontrivial example of two rings A, B and a map $f : A \to B$ that is a homomorphism of additive groups, respects multiplications but does not take 1_A to 1_B.*

Proof. Consider the ring $A = \mathbb{Z}^2$. Consider the map $\iota : A \mapsto A : (a, b) \mapsto (a, 0)$. ι clearly preserves operations but doesn't send $(1, 1)$ to $(1, 1)$. □

Exercise 12.2. *Let R be any ring. If $x^2 = x$ for all $x \in R$, show that R is commutative.*

Proof. Let x, y be arbitrary elements of R. Then $x^2 = x$, $y^2 = y$, $(x + y)^2 = x + y$. But

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$$

from which we have $xy + yx = 0$. Thus

$$0 = x(xy + yx) = x^2y + xyx = xy + xyx = xyx + xy$$

$$0 = (xy + yx)x = xyx + yx^2 = xyx + yx$$

This gives us $xy = yx$, as desired. □

Exercise 12.3. *Let p be an odd prime. Let*

$$\frac{a}{b} = \sum_{k=1}^{p-1} \frac{1}{k}$$

be the reduced fraction. Show that:

1. *$p \big| a$.*
2. *If $p > 3$, $p^2 \big| a$.*

Proof. Consider $\ell = a/b \in \mathbb{Q}$. Note that there exists a field epimorphism from $\varphi : \mathbb{Q} \mapsto \mathbb{F}_p : a/b \mapsto ab^{-1}$, where $\ker(\varphi)$ is the set of all rational numbers, whose numerators, in their reduced forms are divisible by p. Thus showing $\varphi(\ell) = 0$ suffices to show the first part, and similarly, we can consider the epimorphism $\psi : \mathbb{Q} \mapsto \mathbb{F}_{p^2}$ to show the second part. Since $\mathbb{F}_p$ is a field, $\{k^{-1} : k \in [p-1]\} = [p-1]$. Thus

$$\varphi(\ell) = \sum_{k=1}^{p-1} \varphi(k^{-1}) = \varphi\left(\sum_{k=1}^{p-1} k\right) = \varphi((p-1)p/2) = 0$$

as desired. Furthermore,

$$\psi\left(\sum_{k=1}^{p-1} k^{-1}\right) = \psi\left(\sum_{k=1}^{(p-1)/2} \left(\frac{1}{k} + \frac{1}{p-k}\right)\right) = \psi\left(p \sum_{k=1}^{(p-1)/2} (k(p-k))^{-1}\right)$$

$$= \psi\left(-p \sum_{k=1}^{(p-1)/2} k^{-2}\right) = \psi\left(-p \sum_{k=1}^{(p-1)/2} k^2\right) = \psi\left(-p^2(p-1)(p-2)/6\right) = 0$$

□

Exercise 12.4. *Let k be a field, and let G be a finite subgroup of $(k^\times, \cdot)$. Prove that G is cyclic.*

Proof. G is a finite abelian group, and we know that finite abelian groups are closed under lcms of orders, ie:- if $x, y \in G$, then $\exists z \in G$ such that $o(z) = \text{lcm}(o(x), o(y))$. Extending this to all elements in G, we get that $\exists g \in G$ such that $o(g) = \text{lcm}_{x \in G}(o(x))$, ie: $x^{o(g)} = 1$ for all $x \in G$, ie:- the polynomial $p(x) := x^{o(g)} - 1$ has n roots in G. Note that $o(g) \big| n \implies o(g) \leq n$.
Now, we know that for any $p(x) \in k[x]$ such that all roots of $p(x)$ are distinct [34], $p(x)$ has atmost $\deg(p)$ roots in k. Thus $x^{o(g)} - 1$ has atmost $o(g)$ roots in G, and thus $n \leq o(g) \implies o(g) = n$. Consequently g is a generator of G, showing that G is cyclic. □

Exercise 12.5. *Let I be a two-sided ideal of a ring A. Prove that there is a natural one-one correspondence between two-sided ideals of A/I and two-sided ideals of A containing I. Here proper ideals correspond to proper ideals.*

Proof. Let $\mathscr{C}$ be the set of ideals of A containing I, and let $\mathscr{D}$ be the set of ideals of A/I. Consider the maps

$$f : \mathscr{C} \mapsto \mathscr{D} : f(J) := \{a + I : a \in J\}$$

$$g : \mathscr{D} \mapsto \mathscr{C} : f(\mathcal{J}) := \{a : a + I \in \mathcal{J}\}$$

For $\mathcal{J} \in \mathscr{D}$,

$$(f \circ g)(\mathcal{J}) = \{a + I : a \in g(\mathcal{J})\} = \{a + I : a + I \in \mathcal{J}\} = \mathcal{J}$$

while for $J \in \mathscr{C}$,

$$(g \circ f)(J) = \{a : a + I \in f(J)\} = \{a : a + I = b + I, b \in J\} = \{a : a \in b + I, b \in J\}$$

But

$$a \in b + I \implies a - b \in I \subseteq J \implies a = b + J, b \in J \implies a \in J$$

Thus $\{a : a \in b + I, b \in J\} = J$, and thus $(g \circ f)(J) = J$. Since f has a both sided inverse g, f is a bijection between $\mathscr{C}$ and $\mathscr{D}$, as desired. That f takes proper ideals to proper ideals is clear. □

Exercise 12.6. *Let k be a field. Prove that 0 is the only two-sided proper ideal of $M_n(k)$, but $M_n(k)$ is not a division ring for $n \geq 2$.*

Proof. $M_n(k)$ isn't a division ring, as is witnessed by the fact that for

$$0 \neq A := (a_{ij})_{n \times n},\ a_{11} = 1,\ a_{ij} = 0 \text{ otherwise},$$
$$0 \neq B := (b_{ij})_{n \times n},\ b_{22} = 1,\ b_{ij} = 0 \text{ otherwise},$$

we have $AB = BA = 0$, and thus $M_n(k)$ has zero divisors for $n \geq 2$.
Let $\mathfrak{m}$ be a non-zero proper maximal ideal of $M_n(k)$. If there is any invertible matrix P in $\mathfrak{m}$, then we're done, since $P^{-1} \cdot P \in \mathfrak{m} \implies 1 \in \mathfrak{m} \implies M_n(k) \in \mathfrak{m}$, violating the properness of $\mathfrak{m}$.
Thus let $x \in \mathfrak{m}$ be a non-zero non-invertible matrix in $M_n(k)$. Note that the following operations can be achieved by left/right multiplication of suitable matrices:

1. Gauss Jordan Elimination to bring matrix to Reduced Row Echelon Form (Note that here we use the fact that k is a field: For RREF to be calculated, it's necessary that every non-zero element has an inverse)
2. Permutation of rows or columns

[34] one can verify, say through the formal derivative, that all roots of $p(x) := x^\ell - 1$ are distinct

Consequently, if $\text{rank}(x) = \ell \in (0, n)$, then by applying Gauss Jordan elimination and the permutation matrix, we've the truncated identity $i_\ell \in \mathfrak{m}$, where i_ℓ is just the $n \times n$ identity matrix whose bottom most $n - \ell$ entries have been set to 0. Now let q be a permutation matrix which swaps the 1^{st} and $(\ell+1)^{\text{th}}$ columns, while c is a matrix whose only non-zero entry is the first entry of the $(\ell+1)^{\text{th}}$ row, which is set to 1. Then $ci_\ell q$ is a matrix in $\mathfrak{m}$ whose only non-zero entry is the $(\ell+1, \ell+1)$ coordinate, which is 1. Then $i_\ell + ci_\ell q = i_{\ell+1} \in \mathfrak{m}$, and similarly, by induction, $i_n = 1 \in \mathfrak{m} \implies \mathfrak{m} = M_n(k)$, thus violating properness once again. □

Exercise 12.7. *Let R be any ring, and let S be an ideal of $M_n(R)$. Show that there exists an ideal J of R such that $S = M_n(J)$. Conclude that there's a natural correspondence between the ideals of R and $M_n(R)$.*

Proof. For any $i, j \in [n]$, define

$$J_{ij} := \{M_{ij} : M \in S\}$$

Then J_{ij} is an ideal. Indeed, define the standard matrix E_{xy} to be the matrix whose $(x,y)^{\text{th}}$ entry is 1, and all other entries are 0. Then $rE_{xy}S \subseteq S$ since S is an ideal. But the $(i,j)^{\text{th}}$ entries of $rE_{xy}S$ are rJ_{ij}, and thus $rJ_{ij} \subseteq J_{ij}$ for any $r \in R$, showing that J_{ij} is an ideal.
We also claim that $J_{ij} = J_{kl}$ for any 4 (not necessarily distinct) $i, j, k, l \in [n]$. Indeed let P_{ik} be the matrix which permutes the i^{th} and k^{th} rows, while let Q_{jl} be the matrix which permutes the j^{th} and l^{th} columns. Then $P_{ik}SQ_{jl} \subseteq S$ implies that $J_{ij} = J_{kl}$.
Then we can drop the subscripts and just define J to be the set of entries of S, and we know that J is an ideal, and moreover, $S = M_n(J)$.
Finally, it's obvious that if $J_1 \neq J_2$ are distinct ideals, then $M_n(J_1) \neq M_n(J_2)$. Consequently, there exists a natural correspondence between the ideals of R and the ideals of $M_n(R)$. Note that this result immediately implies the previous one: Since the only ideals of a field are the zero ideal and itself, the only proper ideal of $M_n(k)$ then must be the zero ideal. □

Exercise 12.8. *Let R be a ring such that it's only left ideals are (0) and R. Show that either R must be a division ring, or $|R| = p$ for some prime p and $R^2 = \{0\}$.*

Proof. If $R^2 = \{0\}$, any subgroup of $(R, +, 0)$ is a left ideal of R[35]. Since R has only the trivial left ideals, it means that $(R, +, 0)$ must be a simple abelian group, and we know that simple abelian groups are finite groups with prime orders, and thus $|R| = p$.
Thus assume $R^2 \neq \{0\}$. Now note that

$$I := \{x : Rx = 0\}$$

is a left ideal of R. Since $R^2 \neq 0 \implies I \neq R$, we have that $I = 0$. But also note that for any $a \in R \setminus \{0\}$, Ra is also a left ideal of R, and thus $Ra = R$. But $Ra = R$ implies that $\exists b \neq 0$ such that $ba = 1$. Similarly, $\exists c \neq 0$ such that $cb = 1$. But

$$cb = 1 \implies (cb)a = a \implies c(ba) = a \implies c = a$$

ie:- a and b are both sided inverses of each other.
Since every element $x \in R \setminus \{0\}$ has a both sided inverse, R must be a division ring. □

Exercise 12.9. *Let X be a compact Hausdorff topological space. Prove that $x \mapsto \mathfrak{m}_x := \ker(\text{ev}_x)$ is a bijection between X and the set of maximal ideals of $C_{\mathbb{R}}(X) = \{\text{continuous } f : X \to \mathbb{R}\}$.*

[35] In fact since $R^2 = 0$, $ab = 0 = ba$ for all $a, b \in R$, implying R is commutative, and thus any left ideal is actually a two-sided ideal

Proof. Let $\mathfrak{m}$ be any proper maximal ideal of $C_{\mathbb{R}}(X)$, and define

$$Z(\mathfrak{m}) := \bigcap_{f \in \mathfrak{m}} f^{-1}(\{0\})$$

Assume for the sake of contradiction that $Z(\mathfrak{m}) = \emptyset$. Then note that

$$\{f^{-1}(\mathbb{R} \setminus \{0\}) : f \in \mathfrak{m}\}$$

is an open cover of X. Since X is compact, there exists a finite subset of $\mathfrak{m}$, say $\mathfrak{n}$, such that $\{f^{-1}(\mathbb{R} \setminus \{0\}) : f \in \mathfrak{n}\}$ is also an open cover of X. Then consider

$$g(x) := \sum_{f \in \mathfrak{n}} f(x)^2$$

Note that g is non-zero everywhere on X, and thus $1/g \in C_{\mathbb{R}}(X)$, which implies $(1/g) \cdot g \in \mathfrak{m} \implies 1 \in \mathfrak{m} \implies \mathfrak{m} = C_{\mathbb{R}}(X)$, thus violating the properness of $\mathfrak{m}$.
Also note that compact + Hausdorff implies normal, which means for any two points $x, y \in X$ one can find disjoint neighborhoods V_x, V_y of those points [36]. Then by Urysohn's lemma, there exists a continuous function f such that $f(x) = 0, f(y) \neq 0$. This function f immediately demonstrates that $\mathfrak{m}_x \neq \mathfrak{m}_y$ for $x \neq y$, and thus given any maximal ideal, we can uniquely identify it as $\mathfrak{m}_x$ for some unique $x \in X$.
Finally, for each $z \in Z(\mathfrak{m})$ we have $\mathfrak{m} \subset \mathfrak{m}_z$. Thus by the maximality, $\mathfrak{m} = \mathfrak{m}_z$ (and, in particular, $Z(\mathfrak{m})$ is a singleton). □

Aliter. We shall give another closely related way of calculating an open cover. Let $\mathfrak{m}$ be a proper maximal ideal which isn't of the form $\mathfrak{m}_x$ for any $x \in X$. Then for every $x \in X$, we have a function $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$. Since f_x is continuous, there exists a neighborhood[37] U_x of x such that $f_x \neq 0$ on U_x. Then $\{U_x : x \in X\}$ is an open cover of X. After this point the rest of the proof is exactly as above. □

Exercise 12.10. *Let A be the set of complex 2×2 matrices of the form $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$. Note that A is the set of all hermitian matrices of order 2 whose trace is real.*

1. *Show that A is a subring of $M_2(\mathbb{C})$.*
2. *Show that A is a division ring.*
3. *Show that this is a quaternion algebra over $\mathbb{R}$ i.e. there are elements $i, j, k \in A$ such that $1, i, j, k$ is a basis of A, and $i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik$. What is the relation with Pauli matrices?*

Proof. The proofs go as follows:

1. The ring axioms are readily verified for A.
2. $$\begin{pmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{pmatrix} \begin{pmatrix} z_2 & w_2 \\ -\overline{w_2} & \overline{z_2} \end{pmatrix} = \begin{pmatrix} z_1 z_2 - w_1 \overline{w_2} & z_1 w_2 + w_1 \overline{z_2} \\ \dots & \dots \end{pmatrix} = 0$$
$$\implies z_1 z_2 - w_1 \overline{w_2} = 0, z_1 w_2 + w_1 \overline{z_2} = 0$$

   If $w_1 = 0$, then $z_1 \neq 0$ since otherwise the left multiplicand matrix will become zero. But then $z_2 = 0, w_2 = 0$. If, $w_1 \neq 0$, then $w_2 = \overline{z_1 z_2}/\overline{w_1}$. Substituting this in the second relation yields $\overline{z_2}(|z_1|^2 + |w_1|^2) = 0 \implies z_2 = 0 \implies w_2 = 0$.
   Thus A has no zero divisors, and is a division ring.

[36] $x \notin V_y, y \notin V_x$
[37] open set

3. Let $a \in A$. Solving for $a^2 = -1$ yields $\beta^2 + \gamma^2 + \delta^2 = 1$, where a is generated by $z = \alpha + \iota\beta, w = \gamma + \iota\delta$. Putting β, γ, δ to be 1 each [38], we get our i, j, k to be

$$i = \begin{pmatrix} \iota & 0 \\ 0 & -\iota \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & \iota \\ \iota & 0 \end{pmatrix}$$

These matrices are ι times the Pauli matrices.
It's easy to see that A is a **real** vector space spanned by the basis $\{1, i, j, k\}$.

□

Henceforward assume all rings are commutative unless otherwise stated.

Exercise 12.11. *Every maximal ideal is a prime ideal.*

Proof. Let I be a maximal ideal of the ring R, and let $ab \in I$. If $a \in I$, we're done. Thus assume $a \notin I$. Then note that $J := I + aR$ is an ideal of R which strictly contains I, since $a \in J$. Since I is maximal, $I + aR = R$. In particular $\exists i \in I, r \in R$ such that $1 = i + ar$. But then

$$1 = i + ar \implies b = bi + bar = bi + abr \in I + I \subseteq I \implies b \in I$$

Thus if $ab \in I$, then either a or b is in I, and thus I is prime. □

Exercise 12.12. *The ideal pR is prime if p is a prime.*

Proof. If p is prime, and $ab \in pR$, then $ab = pr$ for some $r \in R$, implying p divides ab, and thus p divides a or p divides b, since p is a prime. But that means that either a or b is in pR, and thus pR is a prime ideal. □

Exercise 12.13. *An ideal pR in a PID R is prime iff p is.*

Proof. The backward implication is shown by the previous exercise.
If pR is a prime ideal, then

$$p|ab \Leftrightarrow ab \in pR \implies a \in pR \text{ or } b \in pR \Leftrightarrow p|a \text{ or } p|b$$

showing that p is a prime. □

Exercise 12.14. *If A is a PID, show that an ideal is prime if and only if it is maximal.*

Proof. It suffices to show that every prime ideal is maximal, since the converse holds for any ring. Thus assume for the sake of contradiction that there is an ideal pR of a PID R such that pR is prime but not maximal. Then pR is strictly contained in some maximal ideal, say aR. In particular, we have that $p = ar$ for some $r \in R$. Note that since pR is prime, p is a prime. But then

$$p = ar \implies p|ar \implies p|a \text{ or } p|r$$

But $p|r \implies p = apr' \implies ar' = 1 \implies aR = R$. Thus $p|a \implies r$ is a unit. But then $aR = prR = pR$, yielding a contradiction. □

Exercise 12.15. *Show that the additive **group** $\mathbb{Q}$ has no maximal subgroup.*

[38] substituting -1 just yields the negative of these matrices

Proof. We shall show that for any proper subgroup G of $\mathbb{Q}$, we have a larger proper subgroup H which strictly contains G.
Let G be a proper subgroup of $\mathbb{Q}$. Let $x \notin G$ be a rational number, and consider any non-zero y in G [39], and let $x/y = a/b$ be in the reduced form. Define $H := G + \langle x \rangle \leq \mathbb{Q}$. We shall show that $H \neq \mathbb{Q}$ by showing that $x/b \notin H$. Indeed,

$$\frac{x}{b} \in H \implies \frac{x}{b} = g + nx, g \in G \implies x = bg + bnx = bg + nay \in G$$

yields a contradiction. □

Exercise 12.16. *Every nonzero ring A has a maximal ideal. Further show that every proper ideal I is contained in some proper maximal ideal of A.*

Proof. Take the set S of all proper ideals in A. With containment, S is a poset. Every chain in S is bounded above: Indeed, let C be a chain in S and let $\mathfrak{a}$ be the union of all ideals in C. Then $\mathfrak{a}$ is a proper ideal which upper bounds C[40]. By Zorn's lemma, S has a maximal element.
For the second part, take the set S_I of all proper ideals in A containing I. Then S_I has a maximal element M by a similar argument as above, and M is a maximal element of S too, since any ideal greater than M would contain I and hence be a part of S_I, contradicting M's maximality in S_I. Thus M is a maximal ideal containing I. □

Exercise 12.17. *Show that PIDs are UFDs.*

Proof. Note that once we establish factorization, uniqueness follows from results stated in class. Consider any non-unit $a \in R$, where R is a PID. If a isn't prime, then the ideal aR isn't prime, and thus isn't maximal. Consequently, $aR \subseteq pR$ for some prime p. But then $a = pr$ for some $r \in R$. We can then further factorize r, and so on. If the process terminates, then we have obtained a factorization for a. Assume for the sake of contradiction that it doesn't. Then we have an infinite chain of ideals $(a) \subseteq (r) \subseteq (r_1) \subseteq \ldots$. The union of these ideals is also an ideal, and by properties of a PID, it's of the form $(b) \ni b$. But that means some ideal of the chain contained b, and thus (b), and consequently that ideal *was* (b). Since (b) is an upper bound of this chain, it means that the chain terminated after (b), which contradicts it's infiniteness.
Thus every element can be factorized, and thus a PID is a UFD. □

Exercise 12.18. *Every non-zero ring has a minimal prime ideal.*

Proof. Zorn's lemma can be "inverted". Thus take the set of all prime ideals, take the **intersection** of a decreasing chain of prime ideals. It is still a prime ideal and thus by Zorn's lemma there exists a minimal prime ideal. □

Exercise 12.19. *Show that if k is a field, then for $n \geq 2$, $k[X_1, \ldots, X_n]$ is not a principal ideal domain.*

Proof. Consider the ideal $I = (X_1, X_2, \ldots, X_n) := \{\sum_i X_i p_i, p_i \in k[X_1, \ldots, X_n]\}$. If I were principal, ie:- $I = (f) \implies f \in I$. Since $f = \sum_i X_i f_i$ is non-zero, WLOG assume that $f_1 \neq 0$. Since $X_2 \in I$, we have that $X_2 = fp$ for some $p \in k[X_1, \ldots, X_n]$. But note that there exists a natural isomorphism b/w $k[X_1, \ldots, X_n]$ and $k[X_2, \ldots, X_n][X_1]$, and thus interpret X_2, f, p to be elements of $k[X_2, \ldots, X_n][X_1]$. Then $\deg(X_2) = 0$, while $\deg(f) \geq 1 \implies \deg(fp) \geq 1$, leading to a contradiction. □

Exercise 12.20. *Define the derivative $f'(X)$ of a polynomial $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ as $f'(X) = a_1 + 2a_2 X + 3a_3 X^2 + \cdots + n a_n X^{n-1}$. Prove that if $f(X) \in \mathbb{Q}[X]$, then f(X) is divisible by the square of a nonconstant polynomial if and only if $f(X)$ and $f'(X)$ have a gcd $d(X)$ of positive degree.*

[39] if H is the trivial subgroup then the result follows trivially

[40] $\mathfrak{a}$ is a proper ideal: AFTSOC it wasn't. Then $\mathfrak{a} = R \implies 1 \in \mathfrak{a} \implies$ some ideal in our chain contained $1 \implies$ the ideal wasn't proper; contradiction

Exercise 12.21. *Prove that $2x^5 - 4x^3 - 3$ is irreducible over rational numbers.*

Proof. Assume for the sake of contradiction that $f(x) := 2x^5 - 4x^3 - 3$ is reducible in $\mathbb{Q}[x]$, ie:-

$$f(x) = g(x)h(x),\ g, h \in \mathbb{Q}[x]$$

But if $f(x) = g(x)h(x)$, then the same identity holds after replacing x by x^{-1}. Thus inverting x and multiplying x^5 on both sides yields that the polynomial $-3x^5 - 4x^2 + 2$ is reducible in $\mathbb{Q}[x]$ too, which is a contradiction by Eisenstein's criterion. □

Exercise 12.22. *Let R be a commutative ring. Define its* nilradical *to be*

$$\mathfrak{N}_R := \{r : r^n = 0, n \in \mathbb{N}, r \in R\}$$

Prove that the nilradical is an ideal.

Proof. If $\alpha \in \mathfrak{N}$ then $\alpha^n = 0$ for some n, and thus $(\alpha \cdot x)^n = \alpha^n x^n = 0$, ie:- $\alpha \cdot x \in \mathfrak{N}$ for any $x \in R$. Also, if $\alpha, \beta \in \mathfrak{N}$ are such that $\alpha^n = \beta^m = 0$, then note that $(\alpha + \beta)^{n+m-1} = 0$, since every term in it either has atleast n α's or m β's, and thus $\mathfrak{N}$ is closed under addition.
Consequently, $\mathfrak{N}$ is an ideal of R, also known as the nilradical of R. □

Exercise 12.23 (The Nilradical Theorem)**.** *Let R be a commutative ring. Prove that*

$$\mathfrak{N} = \bigcap_{\mathfrak{p} \text{ prime ideal}} \mathfrak{p}$$

Proof. Let $a \in R$ be any element which is not nilpotent. Define $A_a := \{a^n : n \geq 0\}$. Then $1 \in A_a, 0 \notin A_a$. Define the set $\mathcal{J}_a$ of ideals of R to be

$$\mathcal{J}_a := \{I : I \cap A_a = \emptyset\}$$

Then $\mathcal{J}_a$ is a poset under inclusion[41], and by a typical application of Zorn's lemma it has a maximal element, say M_a. We claim that M_a is a prime ideal: Indeed, assume for the sake of contradiction it wasn't. Then $\exists x, y$ such that $xy \in M_a, x, y \notin M_a$. Then note that the ideal $M_a + xR$ strictly contains M_a, and thus

$$M_a + xR \notin \mathcal{J}_a \implies (M_a + xR) \cap A_a \neq \emptyset \implies m + xr = a^j$$

for some $m \in M_a, r \in R$ and j. Similarly, for some m', r' and j' we have $m' + yr' = a^{j'}$, and thus

$$A \ni a^{j+j'} = (m + xr)(m' + yr') = (mm' + xrm' + yr'm + rr'xy) \in M_a$$

leading to a contradiction.
Thus

$$\mathfrak{N} \supseteq \bigcap_{a \text{ not nilpotent}} M_a \supseteq \bigcap_{\mathfrak{p} \text{ prime ideal}} \mathfrak{p}$$

Now let $\alpha \in \mathfrak{N}$ be any arbitrary element such that $\alpha^n = 0$, and let $\mathfrak{p}$ be any prime ideal, and let m be the least exponent such that $\alpha^m \in \mathfrak{p}$[42]. Then if $m > 1$, $\alpha \cdot \alpha^{m-1} \in \mathfrak{p} \implies \alpha \in \mathfrak{p}$ or $\alpha^{m-1} \in \mathfrak{p}$, contradicting minimality of m. Thus

$$\alpha \in \mathfrak{p} \implies \mathfrak{N} \subseteq \mathfrak{p} \implies \mathfrak{N} \subseteq \bigcap_{\mathfrak{p} \text{ prime ideal}} \mathfrak{p}$$

[41] also note that since $1 \in A_a$, every ideal in $\mathcal{J}_a$ is a proper ideal
[42] note that $m \leq n$, since $\alpha^n = 0 \in \mathfrak{p}$

and consequently

$$\mathfrak{N} = \bigcap_{\mathfrak{p} \text{ prime ideal}} \mathfrak{p}$$

□

Exercise 12.24. *Let I be any ideal of a commutative ring. Define*

$$\sqrt{I} := \{r : r^n \in I, r \in R, n \in \mathbb{N}\}$$

Prove that

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p};\ \mathfrak{p} \text{ prime ideal}} \mathfrak{p}$$

Proof. The above proof carries over verbatim. □

Exercise 12.25. *Let R be a commutative ring, and let $\alpha \in \mathfrak{N}$. Then prove that $(u + \alpha) \in R^\times$, for any $u \in R^\times$.*

Proof. Since $u \in R^\times$, let $uv = 1$. Also, let $\alpha^n = 0$. Then it's easy to verify that

$$(u + \alpha) \cdot \left(v \sum_{k=0}^{n-1} (-v\alpha)^k \right) = 1$$

□

Exercise 12.26. *Suppose R is a commutative ring. Prove that a polynomial $a_0 + a_1X + \cdots + a_nX^n \in R[X]$ has an inverse in $R[X]$ (i.e. is a unit in $R[X]$) if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent elements in R. [An element b of a ring R is nilpotent if $b^n = 0$ for some positive integer n.]*

Proof. If a non-constant $f(X)$ is such that a_0 is a unit[43] and $\{a_i\}_{1 \le i \le n}$ are all nilpotent, then so is $\sum_{i \ge 1} a_i X^i$ and consequently $f(X) = a_0 + \sum_{i \ge 1} a_i X^i \in R[X]^\times$ by the previous exercise.
For the converse, let $\mathfrak{p}$ be any prime ideal of R[44]. Let $D = R/\mathfrak{p}$.Then since homomorphisms preserve the identity, $f(X) \in R[X]^\times \implies \overline{f(X)} \in D[X]^\times$. But we know that since $\mathfrak{p}$ is a prime ideal, D is an integral domain, and there are no non-constant invertible polynomials over an integral domain. Thus $\overline{f(X)}$ is constant in $D[X]$, and thus all coefficients of $f(X)$ except for a_0 belong to $\mathfrak{p}$, ie:- $a_i \in \mathfrak{p}$ for all $i \ge 1$. Since $\mathfrak{p}$ was an arbitrarily chosen prime ideal, we thus have that $a_i \in \bigcap_{\mathfrak{p} \text{ prime ideal}} \mathfrak{p}$. Thus, by the nilradical theorem $a_i \in \mathfrak{N}$ for all $i \ge 1$, ie:- all coefficients of $f(X)$ apart from a_0 are nilpotent, as desired.
Note:- The above proof carries over as it is for multivariate polynomials, ie:- $f \in R[X_1, X_2, \ldots, X_n]^\times$ iff the constant term of f is a unit of R and all other coefficients are nilpotent. □

Exercise 12.27. *Suppose R is a commutative ring. Prove that a polynomial is nilpotent in $R[X]$ iff all of it's coefficients are nilpotent.*

Proof. If all coefficients are nilpotent, then the polynomial too is nilpotent since the inclusion $R \hookrightarrow R[X]$ preserves nilpotency.
To prove the converse direction, we use induction: The result is clear for degree 0 polynomials. Assume the result is true for all nilpotent polynomials of degree atmost $n-1$. Let $f(X)$ be a nilpotent polynomial of degree n, ie:- $f(X)^k = 0$ for some k. If $[X^n]f(X) = a_n$, then $[X^{nk}]f(X) = a_n^k = 0$, and thus a_n is nilpotent. But since $\mathfrak{N}_{R[X]}$ is an ideal, $f(X) - a_nX^n$ is nilpotent too. But $\deg(f(X) - a_nX^n) < n$, and thus all the remaining coefficients are nilpotent by the induction hypothesis. □

[43] a unit of R is also a unit of $R[X]$
[44] R has atleast one prime ideal, since all maximal ideals are prime and every non-zero ring has a maximal ideal by Zorn's lemma

Exercise 12.28. *A polynomial is nilpotent in $R[X_1, X_2, \ldots, X_n]$ iff all of its coefficients are nilpotent.*

Proof. The backward direction is clear.
For the forward direction, note that since $R[X_1, X_2, \ldots, X_n] \cong R[X_2, \ldots, X_n][X_1]$, all coefficients of a polynomial $f \in R[X_1, X_2, \ldots, X_n]$ are nilpotent in $R[X_2, \ldots, X_n]$. Stripping away variables like this, we arrive at our conclusion. □

Exercise 12.29. *Suppose R is a commutative ring and let $f(X) \in \mathfrak{N}_{R[X]} \setminus \{0\}$. Prove that $\exists b \in R \setminus \{0\}$ such that $bf(X) = 0$.*

Proof. Let $f(X) = \sum_{i=0}^{n} a_i X^i$, and let $g(X) = \sum_{j=0}^{m} b_j X^j$ be a polynomial of the minimum degree m such that $f(X)g(X) = 0$. Assume for the sake of contradiction that $m > 0$. Then

$$b_m f(X) \neq 0 \implies \exists i \;\; b_m a_i \neq 0 \implies a_i g(X) \neq 0$$

Let ℓ be the maximum index such that $a_\ell g(X) \neq 0$. Note that

$$g(X) \sum_{i=0}^{\ell} a_i X^i = 0 \implies b_m a_j = 0 \implies \deg(a_\ell g(X)) < \deg(g(X))$$

thus contradicting the minimality of the degree of g. □

Exercise 12.30. *Let I be an ideal of $R[X_1, X_2, \ldots, X_d]$ such that $\exists g \in R[X_1, X_2, \ldots, X_d]$ such that $gI = (0)$. Then $bI = (0)$ for some $b \in R \setminus \{0\}$.*

Proof. See the solution *here*. □

Exercise 12.31 (Universal property of quotient rings)**.** *Let R be a ring and I any two-sided ideal. Let S be another ring and let $f : R \to S$ be any ring homomorphism. Let $\pi : R \to R/I$ be the projection to the quotient ring. Then the following are equivalent.*

1. *$I \subset \ker f$.*
2. *There is a ring homomorphism $\overline{f} : R/I \to S$ such that $f = \overline{f} \circ \pi$.*

In this situation, the homomorphism $\overline{f}$ is unique.

Proof. Done in class. □

Exercise 12.32. *$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ as rings.*

Proof. $\mathbb{R}[X]/(X^2 + 1)$ can be preceived as the ring of all linear polynomials $\{aX + b\}$, with their multiplication being defined after zeroing out $X^2 + 1$, ie:-

$$(aX + b)(a'X + b') = aa'X^2 + (ab' + a'b)X + bb' = (bb' - aa') + (ab' + a'b)X$$

It's now clear that sending $\overline{X} \to \iota, \overline{1} \to 1$ induces an isomorphism between $\mathbb{R}[X]/(X^2 + 1)$ and $\mathbb{C}$. □

Exercise 12.33 (Chinese remainder theorem)**.** *Let R be any ring and let $I_1, \ldots, I_n$ be two-sided ideals. Show that $I = I_1 \cap \cdots \cap I_n$ is a two-sided ideal. Consider the ring homomorphism $f : R/I \to \prod_{i=1}^{n} R/I_i$, defined by $f(a + I) = (a + I_1, \ldots, a + I_n)$. Show that it is injective. Further, show that f is surjective if and only if the ideals I_i are pairwise comaximal i.e. for $i \neq j$, $I_i + I_j = R$.*

Proof. That f is a ring monomorphism is clear. We shall now establish f's surjectivity given pairwise comaximality. Consider indices i, j, k such that $I_i + I_j = R$, $I_i + I_k = R$. Then we have $\alpha_i, \alpha_i' \in I_i, \alpha_j \in I_j, \alpha_k \in I_k$ such that $\alpha_i + \alpha_j = 1, \alpha_i' + \alpha_k = 1$ implying

$$(\alpha_i + \alpha_j)(\alpha_i' + \alpha_k) = 1 \implies \underbrace{\alpha_i\alpha_i' + \alpha_j\alpha_i' + \alpha_i\alpha_k}_{\in I_i} + \underbrace{\alpha_j\alpha_k}_{\in I_j \cap I_k} = 1$$

ie:- $I_i + I_j \cap I_k = R$. Thus we can simplify the pairwise co-maximality condition to $I_i + \bigcap_{j\neq i} I_j = R$ for all i. Consequently, for every i there exists $\alpha_i \in I_i, m_i \in \bigcap_{j\neq i} I_j$ such that $m_i + \alpha_i = 1 \implies m_i \in 1 + I_i$. Now for any $p = (a_1 + I_1, \ldots, a_n + I_n) \in \prod_{i=1}^n R/I_i$, we have that for $a := \sum_i m_i a_i$, $f(a + I) = p$, ie:- f is surjective.
Conversely, if f is surjective, there exists $a \in R$ such that $f(a + I) = (\overline{0}, \ldots, \overline{1}, \ldots, \overline{0})$, where the i^{th} entry is $\overline{1}$, for any i, ie:- $\exists a \in \bigcap_{j\neq i} I_j$, $a + I_i = 1 + I_i \implies \exists \alpha_i \in I_i \; a + \alpha_i = 1 \implies I_i + \bigcap_{j\neq i} I_j = R$, ie:- I_i is pairwise comaximal with all other ideals. □

Exercise 12.34. *$\mathbb{Z}[X]$ is not a pid.*

Proof. Consider the ideal $I := (X - 2, X^2 - 2)$. Note that if $p \in I$, then $2 \big| p(0)$.
If $\mathbb{Z}[X]$ was a PID, then I would be a principal ideal, say (f). Then $f \big| (X - 2)$, $f \big| (X^2 - 2)$. Note that since $\mathbb{Z}$ is a UFD, so is $\mathbb{Z}[X]$, and thus a notion of gcd is consistently defined (upto units). It's easy to see that $\gcd(X - 2, X^2 - 2) \sim 1$[45], and thus f is a unit, and consequently, $(f) = \mathbb{Z}[X]$. But $X + 1 \in \mathbb{Z}[X]$, $X + 1 \notin I$, leading to a contradiction. □

Aliter. We know that X is a prime element in $\mathbb{Z}[X]$. Had $\mathbb{Z}[X]$ been a PID, then (X) would be a prime ideal and hence a maximal ideal, and consequently $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ would have been a field, leading to a contradiction. □

Exercise 12.35. *Let $R = \mathbb{Z}[\sqrt{-n}]$, where $n > 3$ is a square-free integer.*

1. *Prove that $2, \sqrt{-n}, 1 \pm \sqrt{-n}$ are irreducibles in R.*
2. *Prove that R is not a UFD.*
3. *Produce a non-principal ideal in R.*

Proof. For $z = x + y\sqrt{-n} \in R$, define $N(z) = |z|^2 = x^2 + ny^2$.

1. Note that $2 = p_1p_2 \implies 4 = N(p_1)N(p_2)$, and thus $\text{Im}(p_1) = \text{Im}(p_2) = 0$. Thus p_1, p_2 are integral, and the irreducibility of 2 follows then.
   If $\sqrt{-n} = p_1p_2 \implies n = N(p_1)N(p_2)$. If either p_1 or p_2 has an imaginary component, then their norm is atleast n, and then the other must have unit norm (and thus be a unit). If both p_1 and p_2 are real, then p_1p_2 must be real, which isn't possible.
   A similar logic as above holds for $1 \pm \sqrt{-n} = p_1p_2 \implies 1 + n = N(p_1)N(p_2)$. If either p_1 or p_2 have both real and imaginary components, then $N(p_1) \geq n + 1$. If any of them is purely imaginary, then their norm must be n. But $n \nmid (n + 1)$ for $n > 3$. Thus p_1, p_2 are real (integral), which isn't possible because $p_1p_2 \notin \mathbb{R}$.
2. Assume for the sake of contradiction that R is a UFD. Then 2 is a prime since irreducibles and primes are the same in a UFD. If n is even, then $2 \big| -n = (\sqrt{-n})^2$, but $2 \nmid \sqrt{-n}$, and thus 2 is not a prime. If n is odd, then $2 \big| 1 + n = (1 + \sqrt{-n})(1 - \sqrt{-n})$, but $2 \nmid (1 \pm \sqrt{-n})$, and thus 2 isn't a prime again, leading to a contradiction.

[45] We say $a \sim b$ if $a = bu$ for some unit u

3. In general, for any integral domain R, let p be a non-prime irreducible in R, and let $p \mid ab$ be such that $p \nmid a, p \nmid b$, ie:- a, b are witnesses to the non-primality of p. Then consider the ideal $I := (p, a)$. If I is principal, ie;- $I = (x)$, then $x \mid p$. If x is a unit, then $(x) = R \implies (p, a) = R \implies \alpha p + \beta a = 1 \implies b = b\alpha p + ba\beta \implies p \mid b$, leading to a contradiction. Thus x must be an associate of p. But since $(x) = (p, a) \implies x \mid a \implies p \mid a$, once again a contradiction.
   Thus in our context, if n is even, then $(2, \sqrt{-n})$ is a non-principal ideal, while if n is odd, then $(2, 1 + \sqrt{-n})$ is a non-principal ideal.

□

Exercise 12.36. *Let $A_1, \ldots, A_n$ be rings and let $A = \prod_{i=1}^{n} A_i$. Prove that the two-sided ideal of A are precisely the ideals of the form $I_1 \times \cdots \times I_n$ where I_i is an ideal of A_i.*

Proof. The proof is clear enough. □

Exercise 12.37. *If R and S are rings, prove that $R \times S$ can't be a field.*

Proof. $(0) \times S$ is a non-zero proper ideal of $R \times S$. □

Exercise 12.38. *Let k be a commutative ring and let G be a finite group. Prove that $k[G] = \{\sum_{g \in G} a_g g\}$ becomes a k-algebra under operations defined as follows:*

1. $\sum_g a_g g + \sum_g b_g g = \sum_g (a_g + b_g) g$,
2. $(\sum_g a_g g) \star (\sum_g b_g g) = \sum_{g \in G} (\sum_{st=g} a_s b_t) g$,
3. $0 = 0_k 1_G, \;\; 1 = 1_k 1_G$.

Exercise 12.39. *Let k be a commutative ring and let $k[[X_1, \ldots, X_n]]$ be the set of formal (possibly infinite) sums of the form $\sum_I a_I X^I$, where the sum is over all multi-indices $I = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$, and $X^I = x_1^{i_1} \cdots x_n^{i_n}$. Put natural addition and multiplications on this set and show that it becomes a k-algebra in a natural way.*

Exercise 12.40. *Let R be a commutative ring in which every prime ideal is principal. Prove that R is a PID.*

Proof. Assume for the sake of contradiction that R is not a PID. Let S be the set of non-principal ideals. Since R isn't a PID, S is non-empty. By a standard Zorn's lemma argument, S has a maximal element M. Clearly M can't be principal, and hence M is not prime, since all prime ideals are principal in R. Thus there exist $a, b \in R$ such that $ab \in M, a \notin M, b \notin M$. Define $M_a := (M, a)$, $M_b := (M, b), N := \{r \in R : rM_a \subseteq M\}$. Since $M \subsetneq M_a$, M_a is a principal ideal, say (α). Moreover, if $M_b \ni m_b = m + br$, $m \in M$, then $m_b M_a = (m+br)M_a = (m+br)(M + aR) = mM + brM + maR + abrR \in M$. Also it's easy to see that N is an ideal. Thus $M_b \subseteq N$, and thus $N \supsetneq M$, which implies N is also principal, say (β). Also note that by definition $NM_a \subseteq M$, and $NM_a = (\alpha\beta)$.
Now, for any arbitrary $x \in M \subset M_a = (\alpha) \implies x = x'\alpha$. Since $x'\alpha \in M$,

$$x'(\alpha) \subseteq M \implies x' M_a \subseteq M \implies x' \in N \implies x \in NM_a \implies M \subseteq NM_a$$

Thus $M = NM_a = (\alpha\beta)$ is principal, leading to a contradiction. □

Exercise 12.41. *Let k be any field. Prove that $k[x, y]/(y - x^2) \cong k[x]$.*

Proof. Consider the ring homomorphism $\varphi : k[x,y] \twoheadrightarrow k[x,x^2] = k[x] : p(x,y) \mapsto p(x,x^2)$. Clearly φ is an epimorphism since any polynomial $g \in k[x] \subset k[x,y]$ is it's own image under φ. Moreover, note that $y - x^2 \in \ker(\varphi) \implies (y-x^2) \in \ker(\varphi)$. But on the other hand, if we represent a polynomial $f \in \ker(\varphi)$ as a polynomial in y then x^2 is a root of f in $k[x]$, and thus by the factor theorem[46] $(y-x^2)\big|f \implies f \in (y-x^2) \implies \ker(\varphi) \subset (y-x^2) \implies \ker(\varphi) = (y-x^2)$.
Thus by the first isomorphism theorem $k[x,y]/(y-x^2) \cong k[x]$. □

Exercise 12.42. *Let k be any field. Prove that $k[x,y]/(y-x^2) \ncong k[x,y]/(y^2-x^2)$.*

Proof. We note that $k[x,y]/(y-x^2) \cong k[x]$ is an integral domain, while we have $(\overline{y}-\overline{x}), (\overline{y}+\overline{x}) \in k[x,y]/(y^2-x^2)$, and $(\overline{y}-\overline{x}) \cdot (\overline{y}+\overline{x}) = \overline{0}$, and thus $k[x,y]/(y^2-x^2)$ is not an integral domain. □

Exercise 12.43. *Let $R := k[x,y,z]/(xy-z^2)$. Prove that $\overline{P} := (\overline{x},\overline{z})$ is a prime ideal of R.*

Proof. Let φ be the projection ring epimorphism from $k[x,y,z]$ to $k[x,y,z]/(xy-z^2)$. Then note that $\overline{P} = \varphi((x,z)) = (x,z)/(xy-z^2)$. Then

$$\frac{k[x,y,z]/(xy-z^2)}{(\overline{x},\overline{z})} = \frac{k[x,y,z]/(xy-z^2)}{(x,z)/(xy-z^2)} \cong \frac{k[x,y,z]}{(x,z)} \cong k[y]$$

Since $k[y]$ is an integral domain, $\overline{P}$ is a prime ideal.

□

Exercise 12.44. *Let R be an integral domain. Prove that $I := (x^a - y^b)$ is a prime ideal of $R[x,y]$ if $gcd(a,b) = 1$.*

Proof. Consider the ring homomorphism $\varphi : R[x,y] \to R[t]$ induced by $x \to t^b, y \to t^a$. Then clearly $I \subset \ker(\varphi)$. Conversely, let $f \in \ker(\varphi)$. Treating f and $x^a - y^b$ as polynomials over $R[y]$[47], one can write

$$f = (x^a - y^b)g + \sum_{k=0}^{a-1} s_k(y)x^k = (x^a - y^b)g + r(x,y)$$

Now, $f \in \ker(\varphi) \implies f(t^b,t^a) = 0 \implies r(t^b,t^a) = 0$. If we can show that $r = 0$, then we'll be done. AFTSOC not. Then some $s_i(y) \neq 0$. But that means that some $s_j(y)$ is also non-zero.
Now, $s_i(t^a)(t^b)^i$ has terms of the form $t^{a\ell+bi}$, while $s_j(t^a)(t^b)^j$ has terms of the form $t^{a\ell'+bj}$. Now,

$$a\ell + bi = a\ell' + bj \implies a\big|b(i-j) \implies a\big|(i-j)$$

But that's not possible since $0 \leq i-j < a$. Thus every term in r gives rise to different powers of t, and thus the only way for r to be zero is if all the coefficients in it are zero. Thus $f \in \ker(\varphi)$.
Consequently $I = \ker(\varphi)$, and $R[x,y]/I \cong \text{im}(\varphi) \subseteq R[t]$. Since $R[t]$ is a domain, so is $\text{im}(\varphi)$, and thus $R[x,y]/I$ is an integral domain, showing that I is a prime ideal. □

[46] since $k[x,y]$ is UFD, we can talk of the factor theorem
[47] which is an integral domain since R is