DUMMIT AND FOOTE NOTES

BRANDON GONTMACHER

Contents

1. Chapter 1: Intro to groups

1.1. Axioms and examples.

Proposition 1.1. Let G be a group. Then

(1) The identity is unique.
(2) For each $g \in G$, g^{-1} is unique.
(3) $(g^{-1})^{-1} = g$.
(4) $(ab)^{-1} = b^{-1}a^{-1}$
(5) The value of $\prod_{i=1}^{n} a_i$ is independent of how we arrange parentheses.

Proof.

(1) Let f and g both be identites, so $fg = f = g$.
(2) Let c and c both be inverses to a and $e \in G$ the identity. Then $ab = e = ca$. Thus $c = ce = c(ab) = (ca)b = eb = b$.
(3) Clear.
(4) Let $c = (ab)^{-1}$ so that $(ab)c = e$, which gives $bc = a^{-1}$ and $c = b^{-1}a^{-1}$ by multiplying on the left.
(5) The result is trivial for $n = 1, 2, 3$. For all $k < n$ assume that any $\prod_{i=1}^{k} b_i$ is independent of parentheses. Then
$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{k} a_i \prod_{i=k+1}^{n} a_i.$$
Then by assumption both are independent of parentheses since $k, n-k < n$ so by induction we are done.

■

Proposition 1.2. Let $a, b \in G$. Then the equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, we can cancel on the left and right.

Proof. That $x = a^{-1}b$ is unique follows from the uniqueness of a^{-1} and the same for $y = ba^{-1}$. ■

1.2. **Dihedral groups.** Letr r be a rotation clockwise about the origin by $2\pi/n$ radians and let s be reflection about the line of symmetry through the first labelled vertex and the origin.

Proposition 1.3.

(1) $|r| = n$
(2) $|s| = 2$
(3) $s \neq r^i$ for all i
(4) $sr^i \neq sr^j$ for all $i \neq j$. Thus
$$D_{2n} = \{1, r, \ldots, r^{n-1}, s, sr, \ldots sr^{n-1}\}$$
and we see that $|D_{2n}| = 2n$.
(5) $rs = sr^{-1}$
(6) $r^i s = sr^{-i}$.

Proof.

(1) This is clear.
(2) So is this.
(3) And this.
(4) Just cancel on the left and use the fact that $|r| = n$. We assume that i is not congruent to $j \mod n$.
(5) Omitted.
(6) By (5), this is true for $i = 1$. Assume it holds for $k < n$. Then $r^{k+1}s = r(r^k s) = rsr^{-k}$. Then $rs = sr^{-1}$ so $rsr^{-k} = sr^{-1}r^{-k} = sr^{-k-1}$ so we are done.

■

A presentation for the dihedral group with $2n$ elements is
$$D_{2n} = \langle r, s : r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

Example 1.4. The group
$$X_{2n} = \langle x, y : x^n = y^2 = 1, xy = yx^2 \rangle$$
does *not* have order $2n$. In fact, $x = xy^2 = yx^2y = yxyx^2 = yyx^2x^2 = x^4$, so $x^3 = 1$. Thus $|X_{2n}| \leq 6$. Once can show that $|X_{2n}| = 6$ if $n = 3k$ and $|X_{2n}| = 2$ if $(3, n) = 1$ (in the latter case, it can be shown that $x = 1$).

Example 1.5. The group
$$Y = \langle u, v : u^4 = v^3 = 1, uv = v^2u^2 \rangle$$
is actually trivial!

1.3. **Symmetric groups.** Let Ω be a nonempty set and S_Ω the set of bijections from Ω to itself, which is a group under function composition called the *symmetric group on* Ω. The elements of Ω are permutations of Ω. If $\Omega = \{1, 2, \ldots, n\}$, then $|S_\Omega| = n!$.

Proposition 1.6. S_n is nonabelian for $n \geq 3$.

1.4. **Matrix groups.** Useless.

1.5. **The Quaternion group.** Useless.

1.6. **Homomorphisms and isomorphisms.**

Definition 1.7. A map $\varphi : G \to H$ between groups is a *homomorphism* if

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

If φ is also a bijection, then it is an *isomorphism*.

Example 1.8. The exponential map $\mathbb{R} \to \mathbb{R}^+$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \cdot)$.

Example 1.9. Let A and B be nonempty sets. Then the symmetric groups S_A and S_B are isomorphic if and only if $|A| = |B|$. To show this, let $\sigma \in S_A$ such that $\sigma(x) = y$ and for each $x \in A$ let $\theta(x) \in B$.Define $\varphi : S_A \to S_B$ by

$$\varphi(\sigma)(\theta(x)) = \theta(y).$$

Since θ is some bijection, it has an inverse, so this map is an isomorphism.

We only prove the converse when A and B are finite. If $S_A \cong S_B$ then they must have the same order, say $n!$. Then it immediately follows that $|A| = |B|$.

Say we are given groups only in terms of generators and relations; e.g. let G be a group with generators $\{s_1, \ldots, s_m\}$ and H a group with generators $\{r_1, \ldots, r_m\}$. If any relation in G satisfied by the s_i is also satisfied in H by the r_i then there is a unique homomorphism $\varphi : G \to H$ given by $s_i \mapsto r_i$. Thus φ is uniquely determined by its action on the generators.

1.7. **Group actions.**

Definition 1.10. A *group action* of a group G on a set A is a map $G \times A \to A$, written $g \cdot a$, such that

(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$.
(2) $1 \cdot a = a$.

Each $g \in G$ induces a map $\sigma_g : A \to A$ given by $\sigma_g(a) = g \cdot a$, which is in fact a permutation of A. Moreover, the map $G \to S_A$ given by $g \mapsto \sigma_g$ is a homomorphism. This is the *permutation representation* associated to a given action. If $\varphi : G \to S_A$ is any homomorphism, then the map $G \times A \to A$ defined by $g \cdot a = \varphi(g)(a)$ is an action of G on A.

Definition 1.11. If the action of G on a set A and each $g \in G$ induces a distinct permutation of A, then the action is *faithful*. Equivalently, a faithful action is one in which the permutation representation is injective. The *kernel* of a group action is

$$\{g \in G : ga = a \text{ for all } g \in G\}$$

is the set of elements of G which fix all elements $a \in A$.

2. Subgroups

2.1. **Definition and examples.**

Definition 2.1. A subset H of a group G is a *subgroup* if H is nonempty and $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$. We write $H \leq G$.

Proposition 2.2 (Subgroup criterion)**.** A subset $H \subseteq G$ is a subgroup if and only if

(1) H is nonempty
(2) $x, y \in H$ implies $xy^{-1} \in H$.

If H is finite, it suffices to check only that H is closed under multiplication.

Proof. If $H \leq G$, then it is obvious.

Conversely, let $x \in H$ (by assumption, H is nonempty) and $y = x$. Then $1 = xx^{-1} \in H$ so H has the identity. Also, $1x^{-1} \in H$, so H has inverses. Since $xy^{-1} \in H$, then since $y^{-1} \in H$ we see that $x(y^{-1})^{-1} = xy \in H$ so H is closed under multiplication.

Now let H be finite and closed under multiplication. Then there are only finitely many x^n which are distinct, say $x^a = x^b$ for some integers $a < b$. Let $m = b - a$ so that $x^m = 1$. Thus all elements have finite order. Then $1 \in H$ and $x^{m-1} = x^{-1} \in H$ so it has identity and inverses. ■

2.2. **Centralizers and normalizers, stabilizers, and kernels.** Let G be a group acting on a subset $A \subseteq G$.

Definition 2.3. The *centralizer* of A in G is the set

$$C_G(A) = \{g \in G : gag^{-1} = a \text{ for all } a \in A\},$$

i.e. $C_G(A)$ is the set of all $g \in G$ which commute with all elements of A.

Immediately we see that $1 \in C_G(A)$. Let $x, y \in C_G(A)$. Then $xax^{-1} = a$ implies that $x^{-1}ax = a$, so $C_G(A)$ is closed under inverses. Now

$$\begin{aligned}(xy)a(xy)^{-1} &= (xy)a(y^{-1}x^{-1}) \\ &= x(yay^{-1})x^{-1} \\ &= xax^{-1} = a\end{aligned}$$

so $xy \in C_G(A)$. Thus the centralizer is a subgroup of G.

Example 2.4. If $A = \{a\}$ then we see that $a^n \in C_G(a)$.

Corollary 2.5. If G is abelian, then $C_G(A) = G$ for all subsets $A \subseteq G$.

Definition 2.6. The *center* of G is

$$Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\},$$

the set of elements in G which commute with all other elements in G.

By definition, $Z(G) = C_G(G)$ so it is immediately a subgroup.

Definition 2.7. The *normalizer* of A in G is the set

$$N_G(A) = \{g \in G : gAg^{-1} = A\}.$$

This is the elements in G which act as permutations on the set A by conjugation.

Fixing the set A pointwise is a special case of this, so we see that $C_G(A) \leq N_G(A)$. The normalizer is also a subgroup of G.

Definition 2.8. Let G be a group acting on an arbitrary set S (so not necessarily a subset of G) and let $s \in S$. The *stabilizer* of s in G is the set

$$G_s := \{g \in G : g \cdot s = s\}$$

of elements which fix s under the given action of G.

It is immediate that $1 \in G_s$. Let $y \in G_s$. Then

$$\begin{aligned}s = 1 \cdot s &= (y^{-1}y) \cdot s \\ &= y^{-1} \cdot (y \cdot s) \\ &= y^{-1} \cdot s\end{aligned}$$

So the stabilizer contains inverses. Similarly, it is closed under products as well, so it is a subgroup of G.

Let $S = \mathcal{P}(G)$ be the set of all subsets of G and let G act on S by conjugation, i.e.

$$g : B \to gBg^{-1} \text{ for all } B \in S.$$

Under this action, the normalizer $N_G(A)$ is exactly the stabilizer of A in G, i.e. $N_G(A) = G_A$ for $A \in \mathcal{P}(G)$.

Now let $N_G(A)$ act on A by conjugation. Then the kernel of this action is just $C_G(A)$. Finally, $Z(G)$ is the kernel of G acting on itself by conjugation.

2.3. **Cyclic groups and cyclic subgroups.**

Definition 2.9. A group is *cyclic* if it's generated by a single element, i.e. $G = \{x^n : n \in \mathbb{Z}\}$. We write $G = \langle x \rangle$

Note that all cylic groups are abelian.

Proposition 2.10. If $G = \langle x \rangle$ then $|G| = |x|$.

Proof. First assume $|x| = n < \infty$. Then $1, x, \ldots, x^{n-1}$ are all distinct. Thus $|G| \geq n$. However, by the division algorithm, we see that any x^k with $k \geq n$ is equal to x^{k-n}, which we reduce until $k - Nn < n$. So we only have n distinct elements.

Now assume the order of x is infinite. Thus no power of x is the identity: if $x^a = x^b$, then $x^{a-b} = 1$, a contradiction. Since all powers are distinct, we see that G contains infinitely many distinct elements. ■

Proposition 2.11. Let G be any group, $x \in G$, $m, n \in \mathbb{Z}$. If $x^n = x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $|x| = n$ and $x^m = 1$, then $n \mid m$.

Proof. We can write $d = mn + rs$ by the Euclidean algorithm. Then $x^d = x^{mn+rs} = (x^m)^r (x^n)^s = 1$.

Let $x^m = 1$ and $|x| = n$. If $m = 0$, then $n \mid m$; assume $m \neq 0$. Note that $n < \infty$. Since $0 < d \leq n$ and n is the smallest power of x giving the identity, we see that $d = n$ so that $n \mid m$. ■

Theorem 2.12. Any two cyclic groups of the same order are isomorphic. More specifically, if $\langle x \rangle$ and $\langle y \rangle$ have order n then the isomorphism is given by $x^k \mapsto y^k$. If $\langle x \rangle$ is infinite cyclic, then the map is actually $\mathbb{Z} \to \langle x \rangle$ given by $k \mapsto x^k$.

Proposition 2.13. Let G be a group, $x \in G$, and a a nonzero integer.

(1) if $|x|$ is infinite, then $|x^a| = \infty$
(2) if $|x| = n < \infty$ then $|x^a| = \frac{n}{(n,a)}$

Proposition 2.14. Let $G = \langle x \rangle$.

(1) If the order of x is infinite, then $G = \langle x^a \rangle$ if and only if $a = \pm 1$.
(2) If $|x| = n < \infty$ then $G = \langle x^a \rangle$ if and only if $(a, n) = 1$.

In particular, the number of generators of G is $\varphi(n)$, Euler's φ-function.

Example 2.15. The generators of $\mathbb{Z}/12\mathbb{Z}$ are $1, 5, 7$, and 11. These are the only ones since $\varphi(12) = 4$.

Theorem 2.16. Let $G = \langle x \rangle$.

(1) Every subgroup of G is cyclic.
(2) If $|G| = \infty$ then $\langle x^a \rangle \neq \langle x^b \rangle$ if $a \neq b$ (assuming $a, b > 0$). In general, this is true if $b = -a$.
(3) If $|G| = n < \infty$ then for each positive integer a dividing n there is a unique subgroup of G of order a which is exactly $\langle x^d \rangle$ for $d = \frac{n}{a}$. Moreover, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$.

Example 2.17. An element $g \in G$ commutes with powers of $x \in G$ if and only if it commutes with x; thus $C_G(\langle x \rangle) = C_G(x)$.

2.4. **Subgroups generated by subsets of a group.**

Proposition 2.18. The intersection of arbitrarily many subgroups is a subgroup.

Definition 2.19. If $A \subseteq G$ then we define

$$\langle A \rangle \bigcap_{A \subseteq H H \leq G} H$$

to be the subgroup of G generated by A.

It is just the intersection of all subgroups of G containing A.

On the other hand, for the same susbet A we can define $\bar{A} = \{a_1^{e_1} \cdots a_n^{e_n} : a_i \in A, e_i = \pm 1\}$ where $\bar{A} = \{1\}$ if A is empty. It's just the set of all finite products (*words*) of elements of A and their inverses.

Proposition 2.20. $\bar{A} = \langle A \rangle$

The "top-down" approach is good to prove existence and uniqueness and other such generalities, but this way we can actually see what elements of $\langle A \rangle$.

2.5. **The lattice of subgroups of a group.** Omitted.

3. Quotient groups and homomorphisms

3.1. **Definitions and examples.** The idea of a quotient group is that we want a natural way to multiply the fibers of a homomorphism, i.e. turn them into a group.

Example 3.1. Let $\mathbb{Z}/n\mathbb{Z} = \langle x \rangle$ and define $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\varphi(a) = x^a$. Then φ is a surjective homomorphism and the fiber over x^a is $\varphi^{-1}(x^a) = \bar{a}$ since $\varphi(m) = \varphi(a)$ whenever $m \equiv a \mod n$. Thus each fiber is a residue class modulo n.

Proposition 3.2. Let $\varphi : G \to H$ be a homomorphism.

(1) $\varphi(1_G) = 1_H$
(2) $\varphi(g^n) = \varphi(g)^n$ for all $g \in G$ and $n \in \mathbb{Z}$
(3) $\ker \varphi \leq G$
(4) $\mathrm{im}\varphi \leq H$

Proof. Easy. ∎

Definition 3.3. Let $\varphi : G \to H$ be a homomorphism with kernel K. The *quotient group* G/K has elements which are fibers of φ and if X_a, X_b are the fibers above a and b then $X_a X_b = X_{ab}$ is the fiber above ab.

Thus the kernel is a single element in G/K and the other elements are "translates" of it, i.e. elements in G/K have the form $a + K$ (or aK in multiplicative notation) for some $a \in G$.

Definition 3.4. For $N \leq G$ and $g \in G$, the *left coset* of N in G is the set $gN = \{gn : n \in N\}$. An element of a coset is a *representative* of it.

Note that if $h \in gN$ then $gN = hN$.

Theorem 3.5. Let G be a group and K the kernel of some homomorphism $\varphi : G \to H$. Then the operation $uK \cdot vK := (uv)K$ is a well-defined operation in G/K. In particular, multiplication of cosets doesn't depend on the representatives chosen.

In the example, each fiber is a copy of $n\mathbb{Z}$ shifted by some a; thus the cosets are $a + n\mathbb{Z}$ and we find the quotient group is just the familiar $\mathbb{Z}/n\mathbb{Z}$.

In general, taking the quotient G/K for an arbitrary $K \leq G$ does not lead to a quotient group with a well-defined operation.

Proposition 3.6. The left cosets of $N \leq G$ partition G and $uN = vN$ if and only if $v^{-1}u \in N$.

Proposition 3.7. Let $N \leq G$.

(1) The operation on left cosets is well-defined if and only if $gng^{-1} \in N$ for all $g \in G$, $n \in N$.
(2) If the above operation is well-defined, then it makes the left cosets of N in G into a group G/N.

Definition 3.8. A subgroup $N \leq G$ is *normal* if every element of G normalizes N, i.e. $N_G(N) = G$, so that $gNg^{-1} = N$ for all $g \in G$. We write $N \trianglelefteq G$.

To summarize:

Theorem 3.9. Let $N \leq G$. The following are equivalent:

(1) $N \trianglelefteq G$
(2) $N_G(N) = N$
(3) $gN = Ng$ for all $g \in G$
(4) the left cosets of N in G form a group
(5) $gNg^{-1} \subseteq N$ for all $g \in G$

The only surprising one is the last one, which is left as an exercise.

Proposition 3.10. $N \leq G$ is normal if and only if it is the kernel of some homomorphism.

Namely, it is the kernel of $\pi : G \to G/N$.

Example 3.11. If G is abelian then every subgroup is normal so G/N is a group for all $N \leq G$.

Example 3.12. Let $G = \langle x \rangle \cong \mathbb{Z}/n\mathbb{Z}$ be cyclic of order n and $N \leq G$. Then $N = \langle x^d \rangle$ where d is the smallest integer such that $x^d \in N$. Then $G/N = \{x^a N : a \in \mathbb{Z}\}$ and since $x^a N - (xN)^a$ it follows that $G/N = \langle xN \rangle$, i.e. quotient groups of a cylic group are cyclic.

3.2. **Cosets and Lagrange's theorem.**

Theorem 3.13 (Lagrange)**.** Let G be finite and $H \leq G$. Then $|H| \mid |G|$ and the number of cosets of H in G is exactly $|G|/|H|$.

Proof. We already proved the first part as an exercise. Note that the cosets partition G. In particular, $|H| = |gH| = n < \infty$. Thus $|G| = kn$ so $k = |G|/n = |G|/|H|$. ■

Definition 3.14. The number of cosets of H in G is the *index* of H in G and is denoted $|G : H|$. In particular, if G is finite then $|G : H| = |G|/|H|$.

Corollary 3.15. If G is finite and $x \in G$ then $|x| \mid |G|$, so in particular $x^{|G|} = 1$.

Proof. Since $|x| = |\langle x \rangle|$, we are done. ■

Corollary 3.16. If $|G| = p$ is prime, then $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. Let $1 \neq x \in G$. Then $|\langle x \rangle| > 1$ and divides $|G|$. But $|G|$ is prime so it's either 1 or p; it isn't 1 by assumption, so we must have $|\langle x \rangle| = p$ and $\langle x \rangle = G$. ■

Example 3.17. Let $|G : H| = 2$ and let $g \in G \setminus H$. Then $G/H = \{H, gH\}$ and in particular $gH = G \setminus H$. Since right cosets also partition G, we have $Hg = G \setminus H$ as well. Thus $gH = Hg$, so $H \trianglelefteq G$.

The converse to Lagrange's theorem is not true: namely, if G is finite and $n \mid |G|$ then there doesn't need to be an order n subgroup of G. However, the converse is true for finite abelian groups. A weaker version which holds for all finite groups is the following:

Theorem 3.18 (Cauchy)**.** If G is finite and $p \mid |G|$ is prime, then G has an element of order p

Theorem 3.19 (Sylow)**.** If $|G| = p^a m$ where p is prime and $p \nmid m$ then G has a subgroup of order p^a.

Definition 3.20. Let $H, K \leq G$. Then $HK = \{hk : h \in H, k \in K\}$.

Proposition 3.21. If H and K are finite subgroups of G then

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

Proof. Note that $HK = \bigcup_{h \in H} hK$. We need only find the number of distinct cosets. Since $h_1 K = h_2 K$ if and only if $h_2^{-1} h_1 \in K$ and $h_1, h_2 \in H$ by assumption, we see that the two cosets are equal if and only if $h_2^{-1} h_1 \in H \cap K$, which occurs if and only if $h_1(H \cap K) = h_2(H \cap K)$. Thus the number of distinct cosets hK is the number of distinct cosets $h(H \cap K)$. The latter is $|H|/|H \cap K|$ by Lagrange's theorem. Thus HK has $|H|/|H \cap K|$ distinct cosets of K, each of which has $|K|$ elements, so we have the desired formula. ■

Note that we did not assume $HK \leq G$. In fact, this is not always even true.

Proposition 3.22. If $H, K \leq G$, then $HK \leq G$ if and only if $HK = KH$.

Note that $HK = KH$ doesn't imply that elements of H and K commute, only that $hk = k'h'$ for some $h, h' \in H$ and $k, k' \in K$ always holds.

Corollary 3.23. If $H, K \leq G$ and $H \leq N_G(K)$ then $HK \leq G$. In particular, if $K \trianglelefteq G$ then $HK \leq G$ for all $H \leq G$.

3.3. **The isomorphism theorems.**

Theorem 3.24 (First Isomorphism Theorem)**.** If $\varphi : G \to H$ is a homomorphism then $\ker\varphi \trianglelefteq G$ and $G/\ker\varphi \cong \varphi(G)$.

Corollary 3.25. Let $\varphi : G \to H$ be a homomorphism.

(1) φ is injective if and only if $\ker\varphi$ is trivial.
(2) $|G : \ker\varphi| = |\varphi(G)|$

Proof. Exercise. ■

Theorem 3.26 (Second Isomorphism Theorem)**.** Let $A, B \leq G$ with $A \leq N_G(B)$. Then $AB \leq G, B \trianglelefteq AB, A \cap B \trianglelefteq A$, and $AB/B \cong A/A \cap B$.

Proof. We already have that $AB \neq N_G(B)$ and the next two from the previous section.

The quotient AB/B is well-defined. Define $\varphi : A \to AB/B$ by $\varphi(a) = aB$. The kernel consists of those $a \in A$ such that $aB = B$, i.e. $a \in B$. So $\ker\varphi = A \cap B$, so we are done by the first isomorphism theorem. ■

Theorem 3.27 (Third Isomorphism Theorem)**.** Let $H, K \trianglelefteq G$ with $H \leq K$. Then $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K.$$

Proof. We define $\varphi : G/H \to G/K$ by $gH \mapsto gK$. Then $\ker\varphi = K/H$, so by the first isomorphism theorem we are done. ■

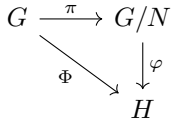
This tells us that we gain no further information from further quotienting a quotient group.

Theorem 3.28 (Fourth Isomorphism Theorem)**.** Let $N \trianglelefteq G$. Then there is a bijection from the set of subgroups $A \leq G$ containing N with the set of subgroups $\bar{A} = A/N \leq G/N$. For all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

(1) $A \leq B$ if and only if $\bar{A} \leq \bar{B}$
(2) if $A \leq B$ then $|B : A| = |\bar{B} : \bar{A}|$
(3) $\overline{A \cap B} = \bar{A} \cap \bar{B}$
(4) $A \trianglelefteq G$ if and only if $\bar{A} \trianglelefteq \bar{G}$

Proof. Tedious. ■

In general, to define a homomorphism on a quotient group G/N by specifying its value at gN, it is necessary to show that φ is well-defined, i.e. is independent of the choice of g (the representative). In effect we are defining a homomorphism Φ on G which is trivial on N, so we actually only need to show that $N \leq \ker\Phi$. In other words, to define a homomorphism on a quotient group, it suffices to check that N is contained in its kernel to show that it is well-defined. In this case, Φ factors through φ, and this is summarized by the following commutative diagram:



3.4. **Composition series and the Hölder program.**

Proposition 3.29. If G is a finite abelian group and $p \mid |G|$ for some prime p then G has an order p element.

Note that this is not Cauchy's theorem, which does not assume G to be abelian.

Proof. We'll do induction on $|G|$. Let $|G| > 1$, so there is a nonidentity $x \in G$. If $|G| = p$ then x has order p, so assume $|G| > p$.

Assume p divides $|x|$ so that $|x| = pn$. Then $|x^n| = p$ so we have an order p element. Thus assume that $p \nmid |x|$.

Let $N = \langle x \rangle$ so that $N \trianglelefteq G$. Then $|G/N| = |G|/|N| < |G|$. Since p doesn't divide N, it must divide $|G/N|$. By the inductive assumption, G/N contains an order p element, say $\bar{y} = yN$. Since $y \notin N$ but $y^p \in N$, we see that $\langle y^p \rangle \neq \langle y \rangle$, so $|y^p| < |y|$. Then $p \mid |y|$, so we are in the situation of the preceding paragraph and are done. ∎

Definition 3.30. A group G is *simple* if $|G| > 1$ and has no nontrivial normal subgroups.

Definition 3.31. A sequence of subgroups of a group G

$$1 = N_0 \leq N_1 \leq \cdots \leq N_{k-1} \leq N_k = G$$

is a *composition series* if $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is simple.

Note that we want each N_i to be normal in N_{i+1}, not necessarily in G.

Theorem 3.32 (Jordan, Hölder)**.** Let G be a nontrivial finite group.

(1) G has a composition series
(2) The composition factors are unique, i.e. if it has two composition series then they must have the same length and the factors must be isomorphic.

Theorem 3.33 (Feit, Thompson)**.** If G is a simple group of odd order then $G \cong \mathbb{Z}/p\mathbb{Z}$.

Definition 3.34. A group G is *solvable* if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$$

such that each G_{i+1}/G_i is abelian.

Theorem 3.35. A finite group G is solvable if and only if for every divisor n of $|G|$ such that $(n, |G|/n) = 1$, G has a subgroup of order n.

Proposition 3.36. Let $N \trianglelefteq G$. If N and G/N are solvable, then G is solvable.

Proof. Let $\bar{G} = G/N$, $1 = N_0 \trianglelefteq \cdots \trianglelefteq N_n = N$ a chain of subgroups with N_{i+1}/N_i abelian, and $\bar{1} = \bar{G}_0 \trianglelefteq \cdots \trianglelefteq \bar{G}_m = \bar{G}$ a similar chain of subgroups. Then there are subgroups $G_i \leq G$ with $N < G_i$ such that $G_i/N = \bar{G}_i$ and $G_i \trianglelefteq G_{i+1}$. Then $\bar{G_{i+1}}/\bar{G}_i \cong G_{i+1}/G$ so

$$1 = N_0 \trianglelefteq \cdots \trianglelefteq N_n = N = G_0 \trianglelefteq \cdots \trianglelefteq G_m = G$$

is the desired chain of subgroups. ∎

3.5. **Transpositions and the alternating group.**

Definition 3.37. A 2-cycle is a *transposition*.

An important observation is that

$$(a_1 a_2 \dots a_m) = (a_1 a_m)(a_1 a_{m_1}) \cdots (a_1 a_2)$$

which shows that every element of S_n is a product of transpositions, or equivalently is generated by transpositions.

We'll now define the alternating group. Let $x_1, \dots, x_n)$ be independent variables and

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j)$$

be a polynomial whose factors are all $x_i - x_j$ for all $i < j$. We let $\sigma \in S_n$ act on Δ by

$$\sigma(\Delta) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

In general, Δ contains one factor $x_i - x_j$ for all $i < j$ and since σ is a bijection on the indices, $\sigma(\Delta)$ contains as a factor $x_i - x_j$ or $x_j - x_i$ but not both. Note that $x_j - x_i = -(x_i - x_j)$. We can rewrite all factors of $\sigma(\Delta)$ in this way so that $\sigma(\Delta) = (-1)^k \Delta = \pm\Delta$ for some k. For each $\sigma \in S_n$ we define

$$e(\sigma) = \begin{cases} +1, & \text{if } \sigma(\Delta) = \Delta \\ -1, & \text{if } \sigma(\Delta) = -\Delta. \end{cases}$$

Definition 3.38. The number $e(\sigma)$ is the *sign* of σ. If $e(\sigma) = 1$ then σ is *even*; otherwise, σ is *odd*.

Proposition 3.39. The map $e : S_n \to \{\pm 1\}$ is a homomorphism.

Proposition 3.40. Transpositions are odd permutations and e is surjective.

Definition 3.41. The *alternating group* is $A_n = \ker e$, i.e. the set of even permutations.

Note that $S_n / A_n \cong e(S_n) = \{\pm 1\}$ so that $|A_n| = |S_n|/2 = n!/2$.

Since we can break down $\sigma \in S_n$ into transpositions and each transposition is odd, we see that since e is a homomorphism that σ is even if it is a product of an even number of transpositions and odd otherwise. Since a k-cycle breaks up into $k - 1$ transpositions, we have the following:

Proposition 3.42. A permutation σ is odd if and only if the number of cycles of even length in its cyclic decomposition is odd.

4. Group actions

4.1. **Group actions and permutation representations.** Recall the following notions: for a group G acting on a set A, we get a map $\sigma_g : A \to A$ given by $\sigma_g(a) = g \cdot a$. This allows us to define a *permutation representation* $\varphi : G \to S_A$ given by $\varphi(g) = \sigma_g$.

Definition 4.1.

(1) The *kernel* of the action is the set of $g \in G$ which act trivially on all $a \in A$.
(2) The *stabilizer* of $a \in A$ is the set of $g \in G$ that fix it.
(3) An action is *faithful* if its kernel is the identity.

The kernel of an action is exactly the same as the kernel of the associated permutation representation. In particular, an action of G on A induces a faithful action of $G/\ker\varphi$ on A, since $g, h \in G$ induce the same permutation on A if and only if they're in the same coset of the kernel. Note that for a given $a \in A$, the kernel of the action must be contained in the stabilizer G_a. In fact, the kernel is exactly $\bigcap_{a \in A} G_a$, as elements here must fix each $a \in A$.

Conversely, given a set A and any homomorphism $\varphi : G \to S_A$, we can define an action of G on A by defining $g \cdot a := \varphi(g)(a)$. The kernel of this action is exactly $\ker\varphi$ as before. Then the permutation representation is exactly given by φ. We have thus shown:

Proposition 4.2. Let G be a group acting on a set A. Then there is a bijection between the actions of G on A and the homomorphisms $\varphi : G \to S_A$.

Proposition 4.3. Let G act on A. Then $a \sim b$ if and only if $a = g \cdot b$ for some $g \in G$ is an equivalence relation. For each $a \in A$, the order of the equivalence class is exactly $|G : G_a|$.

Proof. That $\sim$ is an equivalence relation is obvious. Let C_a be the equivalence class of a, i.e. $C_a = \{g \cdot a : g \in G\}$. Let $b = g \cdot a \in C_a$. Then $gG_a \in G/G_a$. The map $g \cdot a \mapsto gG_a$ gives us a map $C_a \to G/G_a$ which is a bijection, so the two sets have the same order. ∎

Definition 4.4. The equivalence class $\{g \cdot a : g \in G\}$ is the *orbit* of a under G. The action of G is *transitive* if there is only one orbit, i.e. for all $a, b \in A$ there exists $g \in G$ such that $a \cdot g = b$.

4.2. **Groups acting by left multiplication; Cayley's theorem.** Recall that a group G acts on itself by left multiplication, i.e. $g \cdot a = ga$. If $|G| = n < \infty$ we can (arbitrarily) order the elements in G as $g_1, \ldots, g_n$. For each $g \in G$ we can describe $\sigma_g \in S_n$ by $\sigma_g(i) = j$ if and only if $gg_i = g_j$. Of course, labelling the elements differently leads to different descriptions of σ_g.

The action of a group on itself is always transitive: if $x, h \in G$, then $gx = h$ yields $g = hx^{-1} \in G$, which is the desired element such that $g \cdot x = h$. It is also faithful: the only element $g \in G$ such that $g \cdot h = h$ for all $h \in G$ is the identity.

Let $A = G/H$ where $H \leq G$; it does not matter that A is not a group. Then G acts on A by $g \cdot aH = gaH$.

Proposition 4.5. Let $H \leq G$ and G act by left multiplication on $A = G/H$. Let π_H be the associated permutation representation. Then

(1) G acts transitively on A
(2) the stabilizer of $1H \in A$ is H
(3) the kernel of the action ($= \ker \pi_H$) is $\bigcap_{x \in G} xHx^{-1}$ and $\ker \pi_H$ is the largest normal subgroup of G contained in H

Proof.

(1) Let $aH, bH \in A$ and $g = ba^{-1}$. Then $g \cdot aH = bH$.
(2) The stabilizer of $1H$ is just $\{g \in G : gH = H\} = H$.
(3) We have $\ker \pi_H = \{g \in G : gxH = xH \text{ for all } x \in G\} = \{g \in G : x^{-1}gxH = H \text{ for all } x \in G\} = \{g \in G : x^{-1}gx \in H \text{ for all } x \in G\} = \{g \in G : g \in xHx^{-1} \text{ for all } x \in G\} = \bigcap_{x \in G} xHx^{-1}$. Since $\ker \pi_H \trianglelefteq G$ and $\ker \pi_H \leq H$, then if $N \trianglelefteq G$ is contained in H we have $N = xNx^{-1} \leq xHx^{-1}$ for all $x \in G$. Thus $N \leq \bigcap_{x \in G} xHx^{-1} = \ker \pi_H$.

■

Corollary 4.6 (Cayley)**.** Every group is isomorphic to a subgroup of some symmetric group. In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof. Let $H = 1$ and apply the theorem to get a homomorphism $G \to S_G$. The kernel is contained in $H = 1$, so G is isomorphic to its image. ■

Corollary 4.7. If $|G| = n$ and p is the smallest prime dividing $|G|$, then any index p subgroup is normal.

Proof. Let $H \leq G$ and $|G : H| = p$, and let π_H be the permutation representation induced by multiplication on G/H. Denote $K = \ker \pi_H$ and let $|H : K| = k$. Then $|G : K| = pk$. Since H has p left cosets, G/K is isomorphic to a subgroup of S_p by the first isomorphism theorem (the image of G under π_H). Then pk divides $p!$ by Lagrange's theorem. Thus $k \mid (p-1)!$. But every prime divisor of $(p-1)!$ is less than p, but by the minimality of p every prime divisor of k is greater than or equal to p. Thus $k = 1$ and we see that $H = K \trianglelefteq G$. ■

4.3. **Groups acting by conjugation; the class equation.** Let G act on itself by conjugation, so $g \cdot a = gag^{-1}$. Two elements $a, b \in G$ are *conjugate* if there is some $g \in G$ such that $b = gag^{-1} = g \cdot a$. The orbits of G under this action are called *conjugacy classes*. Similarly, two subsets $S, T \subseteq G$ are conjugate if there is some $g \in G$ such that $T = gSg^{-1}$.

Remark. If G is nontrivial then conjugation is not a transitive action; $\{1\}$ is always a conjugacy class. In general, $\{a\}$ is a conjugacy class if and only if $a \in Z(G)$.

The number of conjugates of a subset $S \subseteq G$ is $|G : G_s|$. In particular, we have $G_s = N_G(S)$. If $S = \{s\}$ is a one-element set, then $N_G(S) = C_G(s)$, which shows that the number of conjugates of a single element is $|G : C_G(s)|$. Note that this doesn't tell us how many conjugacy classes there are; this tells us the order of each conjugacy class.

Theorem 4.8 (Class equation)**.** Let G be finite and $g_1, \ldots, g_r$ representatives of the distinct conjugacy classes of G such that $g_i \notin Z(G)$. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

Proof. Recall that $\{x\}$ is a one-element conjugacy class if and only if $x \in Z(G)$. Let $Z(G) = \{1, z_2, \ldots, z_m\}$ and $K_1, \ldots, K_r$ the conjugacy classes of G not contained in the center with each g_i a representative for each K_i. Then the set of conjugacy classes of G is given by $\{1\}, \{z_1, \}, \ldots, \{z_m\}, K_1, \ldots, K_r$. In particular, these partition G, so we have

$$|G| = \sum_{i=1}^{m} 1 + \sum_{i=1}^{r} |K_i| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

as desired. ∎

Example 4.9. Note that $\langle g \rangle \leq C_G(g)$. In the quaternion group Q_8 we have $\langle i \rangle C_{Q_8}(i) \leq Q_8$. Since $i \notin Z(Q_8)$ and $|Q_8 : \langle i \rangle| = 2$, we must have $C_{Q_8}(i) = \langle i \rangle$, so i has exactly 2 conjugates, namely i and $-i = kik^{-1}$. The other conjugacy classes are similarly found; the full list is $\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}$. Thus we have $|Q_8| = 8$ as expected.

Theorem 4.10. If p is prime and $|P| = p^a$ for $a \geq 1$ then $Z(P) \neq 1$.

Proof. We have $|P| = |Z(P)| + \sum_{i=1}^{r} |P : C_G(g_i)|$ by the class equation. Since $C_P(g_i) \neq P$ (otherwise P is abelian and we are immediately done), we must have that p divides $|P : C_P(g_i)|$. Since p also divides P, it must divide $|Z(P)|$ as well. ∎

Corollary 4.11. If $|P| = p^2$, then P is abelian. In particular, P is isomorphic to either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof. By the above theorem, $Z(P) \neq 1$, so $P/Z(P)$ is cyclic and thus P must be abelian. If P has an order p^2 element, then P is cyclic, so let every nonidentity element have order p. Let $1 \neq x \in P$ and $y \in P \setminus \langle x \rangle$. Since $|\langle x, y \rangle| > |\langle x \rangle| = p$, we must have $P = \langle x, y \rangle$. Since x and y both have order p, $\langle x \rangle \times \langle y \rangle = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. The map $(x^a, y^b) \mapsto x^a y^b$ is the desired isomorphism $\langle x \rangle \times \langle x \rangle \cong P$. ∎

Proposition 4.12. Let $\sigma, \tau \in S_n$ and let $\sigma = (a_1 \ldots a_{k_1})(b_1 \ldots b_{k_2}) \ldots$ be its cycle decomposition. Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1) \ldots \tau(a_{k_1})(\tau(b_1) \ldots \tau(b_{k_2}).$$

Proof. If $\sigma(i) = j$ then $\tau\sigma\tau^{-1}(\tau(i)) - \tau(j)$. Thus if the pair i, j appears in the cycle decomposition of σ, then $\tau(i), \tau(j)$ appears in the cycle decomposition of $\tau\sigma\tau^{-1}$. ∎

Proposition 4.13. Two elements in S_n are conjugate if and only if they have the same cycle type. The number of conjugacy classes of S_n is the number of partitions of n.

If $\sigma \in S_n$ is an m-cycle, then the number of conjugates (the number of m-cycles) is $\frac{n(n-1)\cdots(n-m+1)}{m} = \binom{n}{m}$. This is the index of the centralizer of σ : $\frac{|S_n|}{|C_{S_n}(\sigma)|}$. Since $|S_n| = n!$ we get $|C_{S_n}(\sigma) = m(n-m)!$. Since σ commutes with any disjoint cycles and with all σ^i, we can explicitly write $C_{S_n}(\sigma) = \{\sigma^i \tau : \tau \in S_{n-m}\}$.

Proposition 4.14. A_5 is simple.

Proof. We first begin with a necessary lemma:

Lemma 4.15. If $H \trianglelefteq G$ then for each conjugacy class $K \subset G$ either $K \subseteq H$ or $K \cap H$ is empty.

Proof. If $x \in K \cap H$ then $gxg^{-1} \in gHg^{-1} = H$, so H contains all conjugates of x, i.e. $K \subseteq H$. ■

The proof is just by explicitly finding the conjugacy classes of A_5 and their orders; we'll just sketch it. The cycle types of even permutations are $1, (123), (12345), (12)(34)$. It can be shown that $C_{A_5}((123)) = \langle (123) \rangle$ and $C_{A_5}((12345)) = \langle (12345) \rangle$. These groups have orders 3 and 5, so index 20 and 12. Ther are 20 3-cycles in S_5 and they all lie in A_5. But there are 24 5-cycles in A_5 and only 12 distinct conjugates of (12345). Thus there is some 5-cycle which is not conjugate, e.g. $\sigma = (13524)$. Thus A_5 has two conjugacy classes of 5-cycles with 12 elements each. Finally, (12)(34) has 14 distinct conjugates in A_5, so all 15 order 2 elements in A_5 are conjugate to it. Thus the conjugacy classes have orders $1, 15, 20, 12, 12$.

Let $H \trianglelefteq A_5$. Then H is a union of conjugacy classes of A_5. Since $1 \in H$, its order must be 1 plus some combination of the other orders. But such a sum does not divide $|A_5| = 60$, so we have a contradiction. ■

4.4. **Automorphisms.** Note that $\mathrm{Aut}(G) \leq S_G$.

Proposition 4.16. Let $H \trianglelefteq G$. Then G acts on H (by automorphisms of H) by conjugation. In particular, for each $g \in G$ we get an element in $\mathrm{Aut}(H)$. The induced permutation representation is a homomorphism $G \to \mathrm{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Corollary 4.17. If $K \leq G$ and $g \in G$ then $K \cong gKg^{-1}$. Conjugate elements and subgroups have the same order.

Corollary 4.18. For any $H \leq G$, $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular, for $H = G$ this is just $G/Z(G)$.

Proof. Since $H \trianglelefteq N_G(H)$, $N_G(H)$ acts by automorphisms on H so we get the first statement. ■

Definition 4.19. Conjugation by g is an *inner automorphism* of G.

By the above corollary, $\mathrm{Inn}(G) \cong G/Z(G)$. If G is abelian, then every inner automorphism is trivial.

Definition 4.20. A subgroup $H \leq G$ is *characteristic* in G, written $H \mathrm{char} G$, if $\sigma(H) = H$ for all $\sigma \in \mathrm{Aut}(G)$.

Proposition 4.21.

(1) Characteristic subgroups are normal
(2) If H is the unique subgroup of G of a given order, then it is characteristic in G
(3) If $K \mathrm{char} H$ and $H \trianglelefteq G$ then $K \trianglelefteq G$.

Proposition 4.22. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$

Example 4.23. Let $|G| = pq$, where p and q are not necessarily distinct primes with $p \leq q$. Assume $p \nmid q-1$. We show that G is abelian.

If $Z(G) \neq 1$, then by Lagrange's theorem $G/Z(G)$ is cyclic to G is abelian. Thus assume $Z(G) = 1$.

If every nonidentity element has order p then the centralizer of each element has order q and by the class equation we have $pq = 1 + kq$. But this is impossible since $q \mid pq$ and $q \mid kq$ but $q \nmid 1$. Thus G contains an order q element, say x.

Let $H = \langle x \rangle$. Since H has index p, which is the smallest prime dividing $|G|$, H is normal. As $Z(G) = 1$, $C_G(H) = H$. Thus $G/H = N_G(H)/C_G(H)$ is an order p group isomorphic to a subgroup of $\mathrm{Aut}(H)$, which has order $\varphi(q) = q - 1$. But then $p \mid q - 1$, which is impossible. Thus G must be abelian.

Furthermore, it can actually be shown that if $|G| = pq$ with $p < q$ and $p \nmid q - 1$ then G must be *cyclic*.

Example 4.24. Let $|G| = 45 = 3^2 5$. If there is a subgroup $P \trianglelefteq G$ with $|P| = 3^2$ then G is abelian.

We know that $G/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$ and $\mathrm{Aut}(P)$ has order $3(3-1)$ or $3(3-1)^2(3+1)$ depending on if P is isomorphic to $\mathbb{Z}/3^2\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. In either case, $|P|$ is the square of a prime so P is abelian and $P \leq C_G(P)$. Thus $9 \mid |C_G(P)|$, so $|C_G(P)/P|$ is 1 or 5. Since $C_G(P) = G$ and $P \leq Z(G)$, we have $|G/Z_G(P)| = 1$, so $G/Z(G)$ is cyclic and thus G is abelian.

4.5. **The Sylow theorems.**

Definition 4.25.

(1) A group of order $p^a, a \geq 1$, is a *p-group.*
(2) If $|G| = p^a m$ with $p \nmid m$ then an order p^a subgroup is a *Sylow p-subgroup* of G.
(3) The set of Sylow p-subgroups of G is $\mathrm{Syl}_p(G)$ and the number of them is $n_p(G) = \mathrm{Syl}_p(G)$.

Theorem 4.26 (Sylow)**.** Let $|G| = p^a m$ with p, m as above.

(1) $\mathrm{Syl}_p(G)$ is always nonempty
(2) If $P \in \mathrm{Syl}_p(G)$ and Q is any p-subgroup of G then there is some $g \in G$ such that $Q \leq gPg^{-1}$. In particular, any two $P, Q \in \mathrm{Syl}_p(G)$ are conjugate.
(3) $n_p \equiv 1 \mod p$. Furthermore, $n_p = |G : N_G(P)|$ for any $P \in \mathrm{Syl}_p(G)$, so also $n_p \mid m$.

To prove this, we prove the following lemma first:

Lemma 4.27. Let $P \in \mathrm{Syl}_p(G)$. If Q is any p-subgroup of G then $Q \cap N_G(P) = Q \cap P$.

Proof. Let $H = N_G(P) \cap Q$. Since $P \leq N_G(P)$, we have $P \cap Q \leq H$. We just need to prove the reverse inclusion. By definition, $H \leq Q$, so we just need to show $H \leq P$. Since $H \leq N_G(P)$, PH is a subgroup of G. Then $|PH| = |P||H|/|P \cap H|$. All these quantities are powers of p, so PH is a p-group. Since $P \leq PH$, $p^a \mid |PH|$. This is the largest power of p dividing $|G|$, so we must have $|PH| = p^a = |P|$. But then $P = PH$ so $H \leq P$. ■

Proof.

(1) We proceed by induction on $|G|$. When $|G| = 1$, there is nothing to prove, so assume the existence of Sylow p-subgroups for all $k < |G|$.

If $p \mid |Z(G)|$ then by Cauchy's theorem $Z(G)$ has a an order p subgroup $N \leq Z(G)$. Then $|G/N| = |\bar{G}| = p^{a-1}m$. By induction, $\bar{G}$ has a subgroup $\bar{P}$ of order p^{a-1}. Let P be the subgroup of G containing N such that $P/N = \bar{P}$ so that $|P| = p^a$. Thus assume $p \nmid |Z(G)|$.

Let $g_1, \ldots, g_r$ be the representatives of noncentral conjugacy classes of G. If $p \mid |G : C_G(g_i)|$ for all i then since $p \mid |G|$ we would need to have $p \mid |Z(G)|$ by the class equation, which reduces to the above case. Thus for some i, $p \nmid |G : C_G(g_i)|$. Thus $|C_G(g_i)| - |H| = p^a k$ with $p \nmid k$. Since $g_i \notin Z(G)$, $|H| < |G|$. Then H has a Sylow p-subgroup P by induction. Since $|P| = p^a$ and $P \leq G$ as well, P is also a Sylow p-subgroup of G.
(2) This, as well as the third part, use some combinatorial arguments which we omit.

■

In particular, since any Sylow p-subgroups are conjugate, which is an automorphism, they are actually *isomorphic.*

Corollary 4.28. Let $P \leq G$ be a Sylow p-subgroup. Then the following are equivalent:

(1) $n_p = 1$, i.e. P is the unique Sylow p-subgroup
(2) $P \trianglelefteq G$
(3) $P \mathrm{char} G$

Proof. If (1) holds, then $gPg^{-1} = P$ for all g, so P is clearly normal. Conversely, if $P \trianglelefteq G$ and $Q \in \mathrm{Syl}_p(G)$ then $Q = gPg^{-1}$ for some $g \in G$ by Sylow's theorem, but then $Q = P$ so $\mathrm{Syl}_p(G) = \{P\}$.

Since characteristic subgroups are normal, (3) implies (2). Conversely, if $P \trianglelefteq G$ then P is the unique subgroup of order p^a so thus $P \mathrm{char} G$. ■

Example 4.29. A finite abelian group has a unique Sylow p-subgroup for all primes p. It consists of all elements x whose order is a power of p.

Example 4.30.

(1) S_3 has three Sylow 2-subgroups: $\langle(12)\rangle, \langle(23)\rangle, \langle(13)\rangle$. It has a unique Sylow 3-subgroup $\langle(123)\rangle = A_3$.
(2) A_4 has a unique Sylow 2-subgroup: $\langle(12)(34), (13)(24)\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It has four Sylow 3-subgroups: $\langle(123)\rangle, \langle(124)\rangle, \langle(134)\rangle, \langle(234)\rangle$.

Example 4.31. Let $|G| = pq$ for primes p, q with $p < q$. Let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. We know that $n_q = 1 + kq$, $n_q | p$, and $p < q$. Thus we must have $k = 0$, so $n_q = 1$ and $Q \trianglelefteq G$. Since $n_p \mid q$, we either have $n_p = 1$ or $n_p = q$.

In particular, if $p \nmid q - 1$ then $n_p \neq q$ so we would have $P \trianglelefteq G$. Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. If $P \trianglelefteq G$ then since $G/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ which has order $p - 1$ we would have that since $p, q \nmid p - 1$ it must be the case that $G = C_G(P)$. In this case, $x \in P \leq Z(G)$ so x and y commute. Thus $|xy| = pq$ so $G \cong \mathbb{Z}_{pq}$ is cyclic!

Now let $p \mid q - 1$ and Q the Sylow q-subgroup of S_q. We have $|N_{S_q}(Q)| = q(q - 1)$ by an earlier exercise. Since $p \mid q - 1$, by Cauchy's theorem $N_{S_q}(Q)$ has an order p subgroup P. Then PQ is an order pq group. Since $C_{S_q}(Q) = Q$, PQ is nonabelian. In fact, PQ is the *unique* such group.

Example 4.32. Let $|G| = 12$. Assume $n_3 \neq 1$ and let $P \in \mathrm{Syl}_3(G)$. Since $n_3 \mid 4$ and $n_3 \equiv 1 \mod 3$, we must have $n_3 = 4$. Distinct Sylow 3-subgroups intersect only in the identity and each contains two elements of order 3, G contains $2 \cdot 4 = 8$ elements of order 3. Since $|G : N_G(P)| = n_3 = 4$, we have $N_G(P) = P$. G acts by conjugation on the Sylow 3-subgroups, so we get a permutation representation $\varphi : G \to S_4$. The kernel K of the action is the subgroup of G normalizing all the Sylow 3-subgroups. In particular, $K \leq N_G(P) = P$. But P is not normal by assumption, so $K = 1$ and thus φ is injective, so $G \cong \varphi(G) \leq S_4$. Since G contains 8 elements of order 3 and there are exactly 8 elements of order 3 in S_4, all of which are in A_4, it follows that $|\varphi(G) \cap A_4| \geq 8$. But both groups have order 12, so we actually have $\varphi(G) = A_4$ and thus $G \equiv A_4$.

Let V be a Sylow 2-subgroup of A_4. Since $|V| = A_4$, it contains the remaining elements of A_4; in particular, there are no other Sylow 2-subgroups. Thus $n_2(A_4) = 1$ so $V \trianglelefteq A_4$.

The only other case is when $n_3 = 1$, in which case G has a normal Sylow 3-subgroup.

Example 4.33. Let $|G| = p^2 q$ for p, q distinct primes. Let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$.

First consider $p > q$. Since $n_p \mid q$ and $n_p = 1 + kp$, we must have $n_p = 1$ so then $P \trianglelefteq G$.

Now let $p < q$. If $n_q = 1$ then $Q \trianglelefteq G$ so assume $n_q > 1$, say $n_q = 1 + tq$. Since $n_q \mid p^2$ we must have $n_q = p$ or $= p^2$. Since $q > p$ this forces $n_q = p^2$. Thus $tq = p^2 - 1 = (p - 1)(p + 1)$. But q is prime so either $q \mid p - 1$ or $q \mid p + 1$. The first one is impossible since $q > p$ so we must have $q \mid p + 1$. This forces $p = 2$ and $q = 3$, so $|G| = 12$, which reduces to the previous example.

In all cases, G always has a normal Sylow subgroup.

Proposition 4.34. If $|G| = 60$ has has more than one Sylow 5-subgroup, then G is simple.

Proof. Let $|G| = 60$ and $n_5 > 1$ but there exists $H \trianglelefteq G$ with $H \neq 1, G$. Sylow's theorem implies that the only possibility is then $n_5 = 6$. Let $P \in \mathrm{Syl}_5(G)$ so $|N_G(P)| = 10$ (its index is n_5).

If $5 \mid |H|$ then H contains a Sylow 5-subgroup of G, and since H is normal it must contain all 6 conjugates. In particular, this means $|H| \geq 1 + 6 \cdot 4 = 25$, which means we must have $|H| = 30$. But order 30 groups have a normal, thus unique, Sylow 5-subgroup. Thus $5 \nmid |H|$.

If $|H| = 6$ or 12, then H has a normal, thus characteristic, Sylow subgroup. Thus it's also normal in G. Replacing H by this subgroup if necessary, assume $|H| = 2, 3$, or 4. Let $\bar{G} = G/H$ so $|\bar{G}| = 30, 20$, or 15. In each case, $\bar{G}$ has a normal subgroup $\bar{P}$ of order 5. Letting H_1 be the inverse image of $\bar{P}$ in G, we see that $H_1 \trianglelefteq G$ with $H_1 \neq G$ and $5 \mid |H_1|$. But this is impossible by the above, so we are done. ∎

Corollary 4.35. A_5 is simple.

Proof. The subgroups $\langle (12345) \rangle$ and $\langle (13245) \rangle$ are distinct Sylow 5-subgroups. ∎

Proposition 4.36. If G is a simple group of order 60, then $G \cong A_5$.

Proof. Icky. ∎

4.6. **The simplicity of A_n.** We just want to prove the following:

Theorem 4.37. *A_n is simple for all $n \geq 5$.*

Proof. We induct on n. We have seen two proofs already of the case $n = 5$, so assume $n \geq 6$. Let $H \trianglelefteq G$ with $H \neq 1, G$. For each $1 \leq i \leq n$ let G_i be the stabilizer of i in the natural action of A_n on $\{1, \ldots, n\}$ so that $G_i \leq A_n$ and $G_i \cong A_{n-1}$. By induction, G_i is simple for $1 \leq i \leq n$.

First assume there exists $\tau \in H$ with $\tau \neq 1$ but $\tau(i) = i$ for some i. Then $\tau \in H \cap G_i$. Since $H \cap G_i \trianglelefteq G_i$ and G_i is simple, we must have $H \cap G_i = G_i$. Thus $G_i \leq H$. Since $\sigma G_i \sigma^{-1} - G_{\sigma(i)}$, for all i we see that $\sigma G_i \sigma^{-1} \leq \sigma H \sigma^{-1} = H$. Thus $G_j \leq H$ for all j. Now any $\lambda \in A_n$ can be written as a product of an even number of transpositions, so write $\lambda = \lambda_1 \cdots \lambda_t$ where each λ_k is a product of two transpositions. Since $n > 4$ we have $\lambda_k \in G_j$ for some j, so $A_n := \langle G_1, \ldots, G_n \rangle \leq H$, a contradiction. Thus if τ is a nonidentity element in H then it does not fix *any* element. We then see that if $\tau_1, \tau_2 \in H$ with $\tau_1(i) = \tau_2(i)$ for any i then $\tau_1 = \tau_2$ since $\tau_2^{-1}\tau - 1(i) = i$.

Now assume there is some $\tau \in H$ whose cycle decomposition contains a cycle of length ≥ 3, say $\tau = (a_1 a_2 a_4 \ldots)(b_1 b_2 \ldots) \ldots$ and let $\sigma \in A_n$ be such that $\sigma(a_1) = a_1, \sigma(a_2) = a_2$, but $\sigma(a_3) \neq a_3$. Then

$$\tau_1 = \sigma\tau\sigma^{-1} = (a_1 a_2 \sigma(a_3) \ldots)(\sigma(b_1)\sigma(b_2) \ldots) \ldots$$

so that τ and τ_1 are distinct elements with $\tau(a_1) = \tau_1(a_1) = a_2$, a contradiction. Thus we can only have 2-cycles in the cycle decomposition of nonidentity elements in H.

Let $\tau \in H$ be a nonidentity element so now we have $\tau = (a_1 a_2)(a_3 a_4)(a_5 a_6) \ldots$ and let $\sigma = (a_1 a_2)(a_3 a_5) \in A_n$. Then $\tau_1 = \sigma\tau\sigma^{-1} = (a_1 a_2)(a_5 a_4)(a_3 a_6) \ldots$ so τ and τ_1 are distinct elements of H both sending a_1 to a_2. This is again a contradiction, so we are done. ∎

5. Direct and semidirect products and abelian groups

5.1. **Direct products.**

Proposition 5.1. $|G_1 \times \ldots \times G_n| = |G_1| \cdot \ldots \cdot |G_n|$

Each factor G_i is isomorphic to the subgroup $\{(1, 1, \ldots, g_i, 1, \ldots, 1) : g_i \in G_i\}$ where g_i is in the i^{th} position. Identifying G_i with this subgroup, we have that $G_i \trianglelefteq G$, where G is the product of all the G_i, and $G/G_i \cong G_1 \times \ldots \times G_{i-1} \times G_{i+1} \times \ldots \times G_n$. Moreover, this is exactly the kernel of the projection $\pi_i : G \to G_i$.

Example 5.2. Let p prime and consider $E_{p^n} = \mathbb{Z}/p\mathbb{Z} \times \ldots \mathbb{Z}/p\mathbb{Z}$ with n factors. This is the *elementary abelian group* of order p^n, which has the property that $x^p = 1$ for all $x \in E_{p^n}$.

Let $E = E_{p^2}$. Each nonidentity element has order p, so they each generate a cyclic order p subgroup. By Lagrange's theorem, they all intersect trivially. Thus the $p^2 - 1$ nonidentity elements are partitioned into subsets of order $p-1$ because each one consists of nonidetntiy elements of some order p subgroup. Therefore there are $(p^2 - 1)/(p - 1) = p + 1$ order p subgroups.

5.2. **Fundamental theorem of finitely generated abelian groups.** Note that any finite group is obviously finitely generated—we can just take the entire group to be the set of generators.

Theorem 5.3 (Fundamental theorem of finitely generated abelian groups)**.** Let G be a finitely generated abelian group. Then

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

for integers $r, n_1, \ldots, n_s$ such that $r \geq 0, n_i \geq 2$ for all i, and $n_{i+1} \mid n_i$ for all i. Moreover, such an expression is unique.

Definition 5.4. The number r above is the *rank* of G and the integers n_i are the *invariant factors*. The above description is called the *invariant factor decomposition*.

Note that a finitely generated abelian group is finite if and only if its rank is 0. Moreover, the order of a finite abelian group is just the product of its invariant factors. By the divisibility condition on the n_i, we see that if $|G| = n$ then every prime divisor of $|G|$ must divide n_1.

Corollary 5.5. If n is a squarefree product of primes, then the only cyclic group of order n is $\mathbb{Z}/n\mathbb{Z}$.

Example 5.6. Let $n = 180 = 2^2 \cdot 3^2 \cdot 5$. Then $2 \cdot 3 \cdot 5 \mid n_1$, so the possible values of n_1 are $2^2 \cdot 3^2 \cdot 5, 2^2 \cdot 3 \cdot 5, 2 \cdot 3^2 \cdot 5$, or $2 \cdot 3 \cdot 5$.

If $n_1 = 2 \cdot 3^2 \cdot 5$, then the only number n_2 that divides n_1 such that $n_1 n_2 \mid n$ as well is $n_2 = 2$. In this case we actually have $n_1 n_2 = n$, so that is the end.

If $n_1 = 2 \cdot 3 \cdot 5$ then we can have $n_2 = 2, 3$, or 6. If $n_2 = 2$ or 3 then since $n_3 \mid n_2$ we would need to have $n_2 = n_3$, but then $n_1 n_2 n_3$ would either be divisible by 2^3 or 3^3. Thus the second factor must be $2 \cdot 3$, which is the end of the list. The corresponding abelian group is $\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Theorem 5.7. Let $|G| = n > 1$ be an abelian group with $n = p_1^{a_1} \cdots p_k^{a_k}$ its prime factorization. Then

(1) $G \cong A_1 \times \cdots \times A_k$ where $|A_i| = p_i^{a_i}$
(2) For all $A = A_i$ with $|A| = p^a$, $A \cong \mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_t}\mathbb{Z}$ with $b_1 \geq b_2 \geq \ldots \geq b_t \geq 1$ and $\sum b_i = a$.
(3) The decomposition above is unique.

Definition 5.8. The integers p^{b_i} are the *elementary divisors* of G, and the above theorem is the *elementary divisor decomposition*.

The subgroups A_i are in fact the Sylow p_i-subgroups of G. Thus the theorem simply says that G is isomorphic to the direct product of its Sylow subgroups (note that they're normal, as G is abelian, so in particular unique).

Note that $p^a \mid p^b$ if and only if $a \leq b$ and that $\prod_i pa_i = p^a$ if and only if $\sum_i a_i = a$. Thus the elementary divisors of G are actually the invariant factors of the Sylow p-subgroups as p runs over all prime divisors of $|G|$. The conditions on the b_i in the theorem become

(1) $b_i \geq 1$ for all $1 \leq i \leq t$
(2) $b_i \geq b_{i+1}$
(3) $b_1 + \ldots + b_t = b$

Each list of invariant factors is just a partition of b in descending order. For example, the abelian groups of order p^5 can only have invariant factors that partition 5, so we get $5, (4,1), (3,2), (3,1,1), (2,2,1), (2,1,1,1), (1,1,1,1,1)$ and the corresponding abelian groups are the product of $\mathbb{Z}/p^k\mathbb{Z}$ where k runs over the partition.

Proposition 5.9. Integers m and n are coprime if and only if $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$. Furthermore, if $n = p_1^{a_1} \cdots p_k^{a_k}$ then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \mathbb{Z}/p_k^{a_k}\mathbb{Z}$.

5.3. **Groups of small order.** Nothing of note in here except a table for all groups up to order 20.

5.4. **Recognizing direct products.**

Definition 5.10. Let $x, y \in G$ and $A, B \subseteq G$.

(1) $[x, y] = x^{-1}y^{-1}xy$ is the *commutator* of x and y
(2) $[A, B] = \langle [a, b] : a \in A, b \in B \rangle$ is the group generated by commutators of all elements in A and B
(3) $G' = \langle [x, y] : x, y \in G \rangle$ is the *commutator subgroup* of G

Proposition 5.11. Let $x, y \in G$ and $H \leq G$. Then

(1) $xy = yx[x, y]$
(2) $H \trianglelefteq G$ if and only if $[H, G] \leq H$
(3) $\sigma[x, y] = [\sigma(x), \sigma(y)]$ for any $\sigma \in \mathrm{Aut}(G)$. Moreover, $G'\mathrm{char}G$ and G/G' is abelian.
(4) G/G' is the largest abelian quotient: if $H \trianglelefteq G$ and G/H is abelian then $G' \leq H$. Conversely, if $G' \leq H$ then $H \trianglelefteq G$ and G/H is abelian.
(5) If $\varphi : G \to A$ is a homomorphism of G into an abelian group A then φ factors through G', i.e. $G' \ker \varphi$ and the following diagram commutes:

$$\begin{array}{ccc} G & \longrightarrow & G/G' \\ & \searrow^{\varphi} & \downarrow \\ & & A \end{array}$$

Proof.

(1) This is immediate.
(2) $H \trianglelefteq G$ if and only if $g^{-1}hg \in H$ for all $g \in G, h \in H$. For $h \in H$, $g^{-1}hg \in H$ if and only if $h^{-1}g^{-1}hg \in H$ so that $H \trianglelefteq G$ if and only if $[h, g] \in H$ for all $h \in H, g \in G$. Thus $H \trianglelefteq G$ if and only if $[H, G] \leq H$.
(3) That $\sigma([x, y]) = [\sigma(x), \sigma(y)]$ is immediate. Thus for every commutator, its image under an automorphism is also a commutator. Since the commutators generate G', we see that $\sigma(G') = G'$, so $G'\mathrm{char}G$.

    Let $xG'.yG' \in G/G'$. Then $(xG')(yG') = (xy)G' = (yx[x, y]G') = (yx)G' = (yG')(xG')$ since $[x, y] \in G'$.
(4) Let $H \trianglelefteq G$ and G/H be abelian. Then $(xH)(yH) = (yH)(xH)$ so $H = (xH)^{-1}(yH)^{-1}(xH)(yH) = [x, y]H$ so $[x, y] \in H$ and we have $G' \leq H$.

    Conversely, if $G' \leq H$ then since G/G' is abelian we see that every subgroup of G/G' is normal. In particular, $H/G' \trianglelefteq G/G'$. Thus $H \trianglelefteq G$ by the fourth isomorphism theorem. Also, by the third isomorphism theorem we have $G/H \cong (G/G')/(H/G')$ so that G/H is abelian (it's the quotient of the abelian group G/G'). This is exactly (4) phrased in terms of homomorphisms.

■

Proposition 5.12. Let $H, K \leq G$. The number of distinct ways of writing each element in HK in the form hk for some $h \in H, k \in K$ is $|H \cap K|$. In particular, if $|H \cap K| = 1$ then each element has a unique such form.

Theorem 5.13. Let $H, K \leq G$ such that $H, K \trianglelefteq G$ and $H \cap K = 1$. Then $HK \cong H \times K$.

Proof. Note that $HK \leq G$. Let $h \in H$ and $k \in K$. Then $k^{-1}hk \in H$ by normality so $h^{-1}k^{-1}hk \in H$. Similarly, $h^{-1}k^{-1}hk \in K$ so since their intersection is trivial we have $hk = kh$. By the above proposition, this is the only way to write the element $hk \in HK$. Then the map $\varphi : HK \to H \times K$ given by $hk \mapsto (h, k)$ is well-defined, and moreover is actually an isomorphism. ■

Definition 5.14. If $H, K \trianglelefteq G$ and $H \cap K = 1$ then HK is the *internal direct product* of H and K and $H \times K$ is their *external direct product*.

By the theorem above, the distinction is purely aesthetic.

5.5. **Semidirect products.** Assume we already have a group G containing subgroups H and K such that $H \trianglelefteq G$ and $H \cap K = 1$. Note that now we do not require $K \trianglelefteq G$. Then $HK \leq G$ and we can still write every element in HK uniquely, so the bijection $hk \mapsto (h,k)$ still exists. Given $h_1k_1, h_2k_2 \in HK$, their product can be written $(h_1k_1)(h_2k_2) = h_1k_1h_2(k_1^{-1}k_1)k_2 = h_1(k_1h_2k_1^{-1})k_1k_2 = h_3k_3$ where $h_3 = h_1(k_1h_2k_1^{-1})$ and $k_3 = k_1k_2$. Since $H \trianglelefteq G$, $h_3 \in H$. This calculation is assuming there already exists a group G in which H is normal. The idea that follows is to begin with two such groups and define a group G in which H is normal. Since k_3 simply arises from multiplication in K, we can focus on how to get the element $k_1h_2k_1^{-1}$. Then the group HK will have been described entirely in terms of H and K.

Since $H \trianglelefteq G$, K acts on H by conjugation. Thus we can write the above calculation as $(h_1k_1)(h_2k_2) = (h_1(k_1 \cdot h_2))(k_1k_2)$. This action gives a homomorphism $\varphi : K \to \mathrm{Aut}(H)$, so the multiplication in HK depends only on the multiplication in H, the multiplication in K, and φ.

Theorem 5.15. Let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism and $\cdot$ denote the action of K on H determined by φ. Let G be the set of ordered pairs (h,k) with multiplication defined as $(h_1,k_1)(h_2,k_2) := (h_1k_1 \cdot h_2, k_1k_2)$.

(1) G is a group and $|G| = |H||K|$
(2) H and K are naturally subgroups of G
(3) $H \trianglelefteq G$ and $H \cap K = 1$
(4) For all $h \in H$ and $k \in K$, $khk^{-1} = k \cdot h = \varphi(k)(h)$

Proof. (1) That G is a group is just a routine verification. The order of $|G|$ is obvious.
(2) Let $\tilde{H} = \{(h,1) : h \in H\}$ and $\tilde{K} = \{(1,k) : k \in K\}$. Then $(a,1)(b,1) = (a1 \cdot b, 1) = (ab,1)$ and similarly $(1,x)(1,y) = (1,xy)$ so that they are both subgroups. They are canonically identified with H and K.
(3) Under the identifications above, $K \leq N_G(H)$ and since $G = HK$ and $H \leq N_G(H)$ we have $N_G(H) = G$, i.e. $H \trianglelefteq G$.
(4) This follows since $\tilde{H} \cap \tilde{K} = 1$, which is obvious.
(5) This follows since $(1,k)(h,1)(1,k)^{-1} = (k \cdot h, 1)$.

■

Definition 5.16. Let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. The group described above is the *semidirect product* of H and K with respect to φ. It is denoted $H \rtimes_\varphi K$, or simply $H \rtimes K$ when φ is clear.

Proposition 5.17. Let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then the following are equivalent:

(1) The identity map $H \rtimes K \to H \times K$ is a homomorphism (so is also an isomorphism)
(2) φ is the trivial homomorphism
(3) $K \trianglelefteq H \rtimes K$.

Example 5.18. Let H be an abelian group and $K = \langle x \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Define $\varphi : K \to \mathrm{Aut}(H)$ by mapping x to the automorphism $h \mapsto h^{-1}$. Then $x \cdot h = h^{-1}$. Then $|G : H| = 2$ and $xhx^{-1} = h^{-1}$ for all $h \in H$. If $H = \mathbb{Z}/n\mathbb{Z}$ then $G = D_{2n}$ and if $H = \mathbb{Z}$ then we denote G by D_∞.

Example 5.19. Let $K = \mathrm{Aut}(H)$ with $\varphi : K \to \mathrm{Aut}(H)$ the identity map. Then $H \rtimes \mathrm{Aut}(H)$ is called the *holomorph* of H and we write $\mathrm{Hol}(H)$. For example, $\mathrm{Hol}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_4$.

Example 5.20. Let p, q be primes with $p < q$. We already know that if $p \nmid q-1$ then every group of order pq is cyclic. This can be explained by the fact that if $p \nmid q-1$ then there aren't any nontrivial homomorphisms $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ (which has order $q-1$). Thus assume $p \mid q-1$. By Cauchy's theorem, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ contains an order p subgroup (which is unique!). We thus get a nontrivial homomorphism $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. The associated group $G = \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ has order pq and is nonabelian with $\mathbb{Z}/p\mathbb{Z}$ not a normal subgroup.

Example 5.21. Let $p \neq 2$ be prime. Note that $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{F}_p)$, which has order $(p^2-1)(p^2-p)$. Since $p \mid \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$, by Cauchy's theorem there is an order p automorphism. Thus we get a nontrivial automorphism $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$ so can construct $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$, a nonabelian group of order p^3.

Now consider $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong \mathbb{Z}/p(p-1)\mathbb{Z}$, which has an order p element φ and again gives us a homomorphism $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$. We can again construct the semidirect product to be a nonabelian, order p^3 group. However, this is not isomorphic to the above group since this one has an order p^2 element.

Theorem 5.22. Let $H, K \leq G$ such that $H \trianglelefteq G$ and $\mathbb{H} \cap K = 1$. Let $\varphi : K \to \mathrm{Aut}(H)$ be the homomorphism defined by mapping k to the automorphism given by conjugation. Then $HK \cong H \rtimes K$.

Definition 5.23. Let $H \leq G$. A subgroup $K \leq G$ is a *complement* for H if $G = HK$ and $H \cap K = 1$.

Example 5.24. Let G have order pq for p, q primes with $p < q$ and let $P \in \mathrm{Syl}_p(G), Q \in \mathrm{Syl}_q(G)$. We already showed that $G \cong Q \rtimes P$ for some $\varphi : P \to \mathrm{Aut}(Q)$. Note that P and Q are both cyclic so $\mathrm{Aut}(Q)$ is cyclic with order $q - 1$. If $p \nmid q - 1$ then the only homomorphism is trivial so the semidirect product is the direct product, i.e. G is cylic.

Assume $p \mid q - 1$ and let $P = \langle y \rangle$. Since $\mathrm{Aut}(Q)$ is cyclic it has a unique order p subgroup $\langle \gamma \rangle$ and any homomorphism $\varphi : P \to \mathrm{Aut}(Q)$ must map y to a power of γ. Thus there are p homomorphisms, φ_i for $0 \leq i \leq p - 1$, given by $\varphi_i(y) = \gamma^i$. As φ_0 is trivial, $Q \rtimes_{\varphi_0} P \cong Q \times P$. All other φ_i give order pq nonabelian groups G_i. But these are all isomorphic since for each φ_i there is a generator y_i of P such that $\varphi_i(y_i) = \gamma$.

Example 5.25. Let $|G| = 12$, $V \in \mathrm{Syl}_2(G)$, and $T \in \mathrm{Syl}_3(G)$. Either V or T is normal and by Lagrange's theorem $V \cap T = 1$. Thus G is some sort of semidirect product. In the first case, let $V \trianglelefteq G$. If $V \cong \mathbb{Z}/4\mathbb{Z}$ then $\mathrm{Aut}(V) \cong \mathbb{Z}/2\mathbb{Z}$ and there aren't any nontrivial homomorphisms $T \to \mathrm{Aut}(V)$. Thus the only order 12 group with a normal cyclic Sylow 2-subgroup is $\mathbb{Z}/12\mathbb{Z}$.

Thus let $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $\mathrm{Aut}(V) \cong S_3$ and there is a unique order 3 subgroup, say $\langle \gamma \rangle$. If $T = \langle y \rangle$ then there are three possible homomorphisms $\varphi_i : T \to \mathrm{Aut}(V)$ given by $\varphi_i(y) = \gamma^i$. Again since φ_0 is trivial we just get the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. In the other cases we get isomorphic nonabelian order 12 groups which are isomorphic to A_4.

In the second case, let $T \trianglelefteq G$. Note that $\mathrm{Aut}(T) \cong \mathbb{Z}/2\mathbb{Z} = \langle \lambda \rangle$. If $V \cong \mathbb{Z}/4\mathbb{Z} = \langle x \rangle$ then there are two homomorphisms $V \to \mathrm{Aut}(T)$: the trivial one and the one acting by $x \mapsto \lambda$. The trivial one gives $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$. The nontrivial one is actually not isomorphic to A_4 or D_{12}.

Finally assume $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle a \rangle \times \langle b \rangle$. Then there are three homomorphisms $V \to \mathrm{Aut}(T)$ determined by specifying their kernels as one of the three order 2 subgroups of V. For example, $\varphi_1(a) = \lambda$ and $\varphi_1(b) = \lambda$ has kernel $\langle ab \rangle$—in the semidirect product, a and b invert T and ab centralizes it. If $\ker \varphi_2 = \langle a \rangle$ and $\ker \varphi_3 = \langle b \rangle$ Then the resulting three semidirect products are all isomorphic to $S_3 \times \mathbb{Z}/2\mathbb{Z}$.

6. Further topics about groups

6.1. **p-groups, nilpotent groups, and solvable groups.** We'll first recall some facts about p-groups:

Theorem 6.1. Let $|P| = p^a$.

(1) $Z(P) \neq 1$
(2) If $H \trianglelefteq P$ then $H \cap Z(P) \neq 1$. In particular, every normal subgroup of order p is contained in $Z(P)$
(3) If $H \trianglelefteq P$ then H contains a subgroup of order p^b that's normal in H for each divisor p^b of $|H|$. In particular, P has a normal subgroup of order p^b for all $1 \leq b \leq a$.
(4) If $H < P$ then $H < N_P(H)$.
(5) Every maximal subgroup of P has index p and is normal in P.

Definition 6.2. For any group G, define $Z_0(G) = 1$ and $Z_1(G) = Z(G)$. Then $Z_{i+1}(G)$ is the subgroup of G containing $Z_i(G)$ such that $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. The chain $Z_0(G) \leq Z_1(G) \leq \dots$ is the *upper central series* of G[1]. G is *nilpotent* if $Z_c(G) = G$ for some $c \in \mathbb{Z}$. The smallest such c is the *nilpotence class*.

Remark. If G is abelian then it is nilpotent (of class 1) since $G = Z(G) = Z_1(G)$. In general, the chain of subgroups must stabilize at some point, i.e. $Z_n(G) = Z_{n+1}(G) = \cdots$ for some n.

Proposition 6.3. Let $|P| = p^a$. Then P is nilpotent and its nilpotence class is at most $a - 1$.

Proof. For each $i \geq 0$, $P/Z_i(P)$ is a p-group, so if $|P/Z_i(P)| > 1$ then $Z(P/Z_i(P)) \neq 1$. Thus if $Z_i(P) \neq G$ then $|Z_{i+1}(P)| \geq p|Z_i(P)|$ so $|Z_{i+1}(P)| \geq p^{i+1}$. In particular, $|Z_a(P)| \geq p^a$ so $Z_a(P) = P$. Thus the nilpotent class is $\leq a$. The only way it could be exactly a is if $|Z_i(P)| = p^i$ for all i. Then $Z_{a-2}(P)$ would have index p^2, so $P/Z_{a-2}(P)$ would be abelian. But then it would equal its center and we would have $Z_{a-1}(P) = P$, a contradiction. Thus the class of P is actually $\leq a - 1$. ∎

Theorem 6.4. Let G be a *finite* group and $p_1, \dots, p_s$ the distinct primes dividing its order with $P_i \in \mathrm{Syl}_{p_i}(G)$ for all i. Then the following are equivalent:

(1) G is nilpotent
(2) if $H < G$ then $H < N_G(H)$
(3) $P_i \trianglelefteq G$ for all i
(4) $G \cong P_1 \times \dots \times P_s$

Corollary 6.5. A finite abelian group is the direct product of its Sylow subgroups

Proposition 6.6. If G is a finite group such that for all positive integers $n \mid |G|$, G contains at most n elements x satisfying $x^n = 1$, then G is cyclic.

Proposition 6.7 (Frattini)**.** Let G be finite, $H \trianglelefteq G$, and $P \in \mathrm{Syl}_p(H)$. Then $G = HN_G(P)$ and $|G : H| \mid |N_G(P)|$.

Proposition 6.8. A finite group is nilpotent if and only if every maximal subgroup is normal.

Definition 6.9. Define $G^0 = G$, $G^1 = [G, G]$, and (inductively) $G^{i+1} = [G, G^i]$. The chain of groups $G^0 \geq G^1 \geq \cdots$ is the *lower central series* of G.

Theorem 6.10. A group G is nilpotent if and only if $G^n = 1$ for some $n \geq 0$. More specifically, G is nilpotent of class c if and only if c is the smallest nonnegative integer such that $G^c = 1$. If G has class c then $Z_i(G) \leq G^{c-i-1} \leq Z_{i+1}(G)$ for all $1 \leq i \leq c - 1$.

As with the upper central series, the lower one must also stabilize at some n. The following looks similar to the lower central series, but the commutator which we define inductively is different:

Definition 6.11. Define $G^{(0)} = G$, $G^{(1)} = [G, G]$, and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. This is the *derived* or *commutator* series of G.

We also sometimes write $G^{(1)} = G'$, etc. Note that $G^{(i)} \leq G^i$ for all i.

Theorem 6.12. A group G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 0$.

The smallest such n is the *solvable length* of G.

[1] We use "upper" since because $Z_i(G) \leq Z_{i+1}(G)$.

6.2. **Groups of medium order.** Absolutely not. No way.

6.3. **Free groups.** Let S be an arbitrary set and S^{-1} any set disjoint from S such that there is a bijection between them. Then to each $s \in S$ we can associate $s^{-1} \in S^{-1}$. Let $\{1\}$ be a singleton set not contained in $S \cup S^{-1}$ and let $1^{-1} = 1$. Then a *word* on S is a sequence $(s_1, \ldots)$ where $s_i \in S \cap S^{-1} \cup \{1\}$ and $s_i = 1$ for sufficiently large i. Then a word is just a finite product of elements of S and their inverses. A word is *reduced* if $s_{i+1} \neq s_i^{-1}$ and if $s_k = 1$ then $s_i = 1$ for all $i \geq k$. Then $F(S)$ is the set of reduced words on S and we can embed S into it by $s \mapsto (s, 1, 1, \ldots)$. In particular, if S is the empty set then $F(S) = \{1\}$. Then we can naturally define multiplication of reduced words to turn $F(S)$ into a group.

Theorem 6.13. Let G be a group, S a set, and $\varphi : S \to G$ a set map. Then there is a unique group homomorphism $\Phi : F(S) \to G$ such that the following diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{i} & F(S) \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \Phi} \\ & & G \end{array}$$

Corollary 6.14. $F(S)$ is unique up to a unique isomorphism which is the identity map on S.

Definition 6.15. The group $F(S)$ is the *free group* on S. The cardinality of S, which is the *basis* (or *generators*), is the *rank* of $F(S)$.

Theorem 6.16 (Schreier)**.** Subgroups of a free group are free.

Let G be any group; then it is a homomorphic image of a free group, where we take $S = G$ and $\varphi : G \to G$ the identity. The theorem above produces a homomorphism $F(G) \to G$. We can do this more generally for any subset $S \subseteq G$ such that $G = \langle S \rangle$. This allows us to say that a subset *generates* a group if and only if the map $\pi : F(S) \to G$ extending the identity map $S \to G$ is surjective.

Definition 6.17. Let $S \subseteq G$ such that $G = \langle S \rangle$.

(1) A *presentation* for G is a pair (S, R), where R is a set of words in $F(S)$ such that the normal closure of $\langle R \rangle$ in $F(S)$[2] equals the kernel of the homomorphism $\pi : F(S) \to G$. The elements of S are *generators* and those of R are *relations*.
(2) G is *finitely generated* if there is a presentation (S, R) where S is a finite set and G is *finitely presented* if both S and R are finite.

If G is finitely presented with $S = \{s_1, \ldots, s_n\}, R = \{w_1, \ldots, w_k\}$ we write $G = \langle s_1, \ldots, s_n : w_1 = w_2 = \cdots = w_k = 1 \rangle$. That is to say, if w is the word $w_1 w_2^{-1}$ we write $w_1 = w_2$ instead of $w = 1$.

Example 6.18. We can write $\mathbb{Z} \cong F(\{a\}) = \langle a \rangle$, $\mathbb{Z} \times \mathbb{Z} \cong \langle a, b : [a, b] = 1 \rangle$, and $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \langle a, b : a^n = b^m = [a, b] = 1 \rangle$.

Let G be presented by generators a, b with relations $r_1, \ldots, r_k$. If $a', b' \in H$ are elements of another group satisfying the same relations then we get a homomorphism $G \to H$. Namely, if $\pi : F(\{a, b\}) \to G$ is the presentation homomorphism then we can define $\pi' : F(\{a, b\}) \to H$ by $\pi'(a) = a'$ and $\pi'(b) = b'$. Then $\ker \pi \leq \ker \pi'$ so π' factors through $\ker \pi$ and we get $G \cong F(\{a, b\})/\ker \pi \to H$. In particular, if $\langle a', b' \rangle = H = G$ then this is just an automorphism of G.

On the other hand, any automorphism must send generators to generators satisfying the same relations. Thus, for example, if D_8 is generated by elements a and b, then any pair a', b' of elements where a' is noncentral of order 2 and b' has order 4 satisfies the same relations. Since there are 4 noncentral elements with order 2 and two order 4 elements, D_8 only has 8 automorphisms.

[2]It is the smallest normal subgroup containing $\langle R \rangle$.

7. Intro to rings

7.1. Basic definitions and examples.

Definition 7.1. A ring R with a 1 is a *division ring* if every nonzero element has a multiplicative inverse. If R is furthermore commutative, then it is a *field*.

Example 7.2. Let X be any nonempty set and A a ring. The collection R of (set) functions $f : X \to A$ is a ring under pointwise addition and multiplication. R is commutative if and only if A is and the same is true for having a 1 (in this case, 1_R is the constant function 1 on X).

Example 7.3. A function $f : \mathbb{R} \to \mathbb{R}$ has *compact support* if there exists a, b such that $f(x) = 0$ for all $x \notin [a, b]$. The set of all such functions is a commutative ring *without* an identity.

Definition 7.4.

(1) A nonzero element $a \in R$ is a *zero divisor* if there is some nonzero $b \in R$ such that $ab = 0$ or $ba = 0$.
(2) Assume R has an identity $1 \neq 0$. An element $u \in R$ is a *unit* if there is some $v \in R$ such that $uv = vu = 1$. The set of units in R is R^*.

In fact, R^* is a group. For a field F, we have $F^* = F \setminus \{0\}$. Note that a zero divisor can never be a unit: let $a \in R$ be a unit and $ab = 0$ for $b \neq 0$. Then $va = 1$ for some $v \in R$ so we have $b = 1b = (va)b = v(ab) = v0 = 0$, which is a contradiction. Thus fields don't have any zero divisors.

Example 7.5. Let $a \in \mathbb{Z}/n\mathbb{Z}$ such that $(a, n) = d \neq 1$, so $a \notin (\mathbb{Z}/n\mathbb{Z})^*$, and set $b = n/d$. Then since $d > 1$, we must have $0 < b < n$. Since $n \mid ab$, $ab = 0 \in \mathbb{Z}/n\mathbb{Z}$. But $a, b \neq 0$, so a is a zero divisor. Thus every element in $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor!

Example 7.6. Let $D \in \mathbb{Q}$ not be a perfect square. Then $\mathbb{Q}(\sqrt{D})$ is a commutative ring with identity. The assumption on D assures that every element can be written uniquely in the fomr $a + b\sqrt{D}$. Moreover, if a and b are not both 0 then $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 \neq 0$ so that $\frac{a-b\sqrt{D}}{a^2-Db^2}$ is the inverse of $a + b\sqrt{D}$. Thus itis actually a field.

We can write $D = f^2D'$ for some $f \in \mathbb{Q}$ and $D' \in \mathbb{Z}$ where D' isn't divisible by the square of any integer (greater than 1), i.e. is ± 1 times the product of distinct primes in $\mathbb{Z}$. D' is the *squarefree* part of D and we have $\sqrt{D} = f\sqrt{D'}$. Then $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'})$ so we can assume that D is a squarefree integer.

Definition 7.7. A commutative ring with identity is an *integral domain* if it has no zero divisors.

Proposition 7.8. Let $a, b, c \in R$ with a not a zero divisor. If $ab = ac$ then either $a = 0$ or $b = c$.

Corollary 7.9. A finite integral domain is a field.

Proof. Let R be a finite integral domain and $0 \neq a \in R$. The map $x \mapsto ax$ is injective since we can cancel on the left (by the above proposition). Since R is finite this is also surjective. In particular there is some $b \in R$ such that $ab = 1$, i.e. a is a unit. Since a was arbitrary, R is a field. ∎

Example 7.10. A subring of a field F that contains the identity is an integral domain. Conversely, one can show that an integral domain is contained in a field.

Example 7.11. Let $D \in \mathbb{Z}$ be squarefree. Then $Z[\sqrt{D}]$ is a subring of $\mathbb{Q}(\sqrt{D})$. If $D \equiv 1 \mod 4$ then $\mathbb{Z}[(1 + \sqrt{D})/2]$ is also a subring. Define $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega]$ where $\omega = \sqrt{D}$ if $D \equiv 2, 3 \mod 4$ and $\omega = (1 + \sqrt{D})/2$ if $D \equiv 1 \mod 4$. This is the *ring of integers* of $\mathbb{Q}(\sqrt{D})$.

We define the norm $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ by $N(z) = z\bar{z} = |z|^2$. It is not hard to see that $N(a)N(b) = N(ab)$. On $\mathcal{O}$, we have $N(a + b\omega) = (a + b\omega)(a - b\bar{\omega})$. It follows that $N(a) \in \mathbb{Z}$ for all $a \in \mathcal{O}$.

If $a \in \mathcal{O}$ has $N(a) = \pm 1$ then $(a + b\omega)^{-1} = \pm(a + b\bar{\omega}) \in \mathcal{O}$ so a is a unit. Conversely, let a be a unit, say $ab = 1$ for some $b \in \mathcal{O}$. Then $N(ab) = N(a)N(b) = N(1) = 1$ so we must have $N(a), N(b) = \pm 1$. Thus the element $a \in \mathcal{O}$ is a unit if and only if $N(a) = \pm 1$.

When $D = -1$, the units of $\mathbb{Z}[i]$ are just $\{\pm 1, \pm i\}$. When $D = -3$, the units are determined by $a^2+ab+b^2 = \pm 1$, so the group of units is $\{\pm 1, \pm p, \pm p^2\}$ where $p = (-1 + \sqrt{-3})/2$. For all other $D < 0$, the only units are ± 1. However, for $D > 0$ the group of units is always infinite!

7.2. **Examples.**

7.2.1. *Polynomial rings.* Let R be commutative with a 1. Then $R[x]$ is also commutative and has a 1; in particular, the 1 comes from R, as R is included in $R[x]$ as the constant polynomials.

Proposition 7.12. Let R be an integral domain and $0 \neq p, q \in R[x]$. Then

(1) $\deg pq = \deg p + \deg q$
(2) $R[x]^* = R$
(3) $R[x]$ is an integral domain.

Proof. If R has no zero divisors then neither does $R[x]$: if p, q have leading terms $a_n x^n$ and $b_m x^m$ then the leading term of pq is $a_n b_m x^{n+m} \neq 0$ since $a_n b_m \neq 0$. This proves the first and third statements. If p is a unit, say $pq = 1$, then $\deg p + \deg q = 0$, so $p, q \in R$. ■

7.2.2. *Matrix rings.* Note that $M_n(R)$ always has zero divisors and is never commutative for $n \geq 2$. There is an isomorphic copy of R in $M_n(R)$ given by the scalar matrices $\{rI : r \in R\}$.

7.2.3. *Group rings.* Fix a commutative ring R with a 1 and let $G = \{g_1, \ldots, g_n\}$ be a finite group. The *group ring* RG is the set of all formal sums $\sum_{i=1}^{n} a_i g_i$. If g_1 is the identity, we write $g_1 a_1$ as a_1. Similarly, we'll write $1g$ as just g. Addition is defined componentwise. Multiplication is given by $(ag_i)(bg_j) = (ab)g_k$ where ab is done in R and $g_k = g_i g_j$ is done in G. We extend this to the whole of RG by setting the coefficient of g_k in the product $(a_1 g_1 + \cdots + a_n g_n) \cdot (b_1 g_1 + \cdots + b_n g_n)$ to be $\sum_{g_i g_j = g_k} a_i b_j$. Note that RG is commutative if and only if G is.

Since G appears in RG just as $1g_i$ and each of these has an inverse, G is a subgroup of the group of units. Also, if $|G| > 1$ then RG always has zero divisors. For example, let $g \in G$ have order $m > 1$. Then $(1 - g)(1 + g + \cdots + g^{m-1}) = 1 - g^m = 1 - 1 = 0$ so $1 - g$ is a zero divisor.

7.3. **Ring homomorphisms and quotient rings.** Note that $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ given by $\varphi_n(x) = nx$ isn't a ring homomorphism since $\varphi_n(xy) = nxy \neq \varphi_n(x)\varphi_n(y) = n^2xy$. But it's always a group homomorphism!

Proposition 7.13. Let $\varphi : R \to S$ be a ring homomorphism. Then $\mathrm{im}\varphi$ is a subring of S and $\ker\varphi$ is a subring of R. Moreover, if $a \in \ker\varphi$ then $ra, ar \in \ker\varphi$ for all $r \in R$.

Proof. Let $s_1 = \varphi(r_1)$ and $s_2 = \varphi(r_2)$ belong to $\mathrm{im}\varphi$. Then $\varphi(r_1 - r_2) = s_1 - s_2$ and $\varphi(r_1r_2) = s_1s_2$. Thus $s_1 - s_2, s_1, s_2 \in \mathrm{im}\varphi$, so it is a subring of S.

Let $\varphi(a) = \varphi(b) = 0$ so that $\varphi(a - b) = \varphi(ab) = 0$ and $\ker\varphi$ is a subring of R. For any $r \in R$, $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$ so $ra \in \ker\varphi$ and the same for $\varphi(ar)$. ∎

Note that a ring homomorphism $\varphi : R \to S$ is in particular a homomorphism of (additive) abelian groups. Let $I = \ker\varphi$. Then the fibers of φ are cosets $r + I$ and these belong to the quotient ring R/I. The additive structure of R/I is the same as the additive structure of the quotient group R/I. When I is the kernel of a ring homomorphism, R/I also inherits a well-defined multiplication turning it into a ring. In general, this happens exactly when I is closed under left and/or right multiplication by all elements of R. As above, we saw that this is true for $\ker\varphi$.

Definition 7.14. A subset $I \subset R$ of a ring is a *left ideal* if it is a subring and is closed under left multiplication by elements of R, i.e. $rI \subseteq I$. A similar definition holds for *right ideals*. A *two-sided ideal*, which we will in general just call an *ideal*, is a left and right ideal.

When R is commutative, all three notions coincide.

Theorem 7.15. Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker\varphi$ and $\mathrm{im}\varphi$ are ideals in R and S, respectively, and $R/\ker\varphi \cong \varphi(R)$. Furthermore, if I is any ideal in R, then the projection $R \to R/I$ is a surjective ring homomorphism with kernel I.

Example 7.16. Let A be a ring, X a nonempty set, and R the ring of all (set) functions $X \to A$. For a fixed $c \in X$ we the *evaluation map* $E_c : R \to A$ given by $E_c(f) = f(c)$ is a ring homomorphism. The kernel consists of those functions which vanish at c. E_c is surjective since the constant functions on X belong to R, i.e. $f(x) = a$ for all $x \in X$ and a given $a \in A$. Thus $R/\ker E_c \cong A$.

Example 7.17. Let R be commutative with a 1 and $G = \{g_1, \ldots, g_n\}$ a finite group. The map $RG \to R$ given by $\sum_{i=1}^n a_ig_i \mapsto \sum_{i=1}^n a_i$ is a homomorphism called *augmentation*. The kernel, called the *augmentation ideal*, consists of elements of RG whose coefficients sum to 0. For example, $g_i - g_j$ belongs to the kernel for all i, j. The augmentation map is surjective, so the quotient ring is isomorphic to R.

Theorem 7.18. Let R be a ring.

(1) Let A be a subring and B an ideal. Then $A + B$ is a subring of R, $A \cap B$ is an ideal of A, and $(A + B)/B \cong A/(A \cap B)$.
(2) Let I, J be ideals in R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.
(3) Let I be an ideal. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between subrings of R containing I and subrings of R/I. Moreover, A is an ideal of R if and only if A/I is an ideal of R/I.

Definition 7.19. Let I, J be ideals of R.

(1) Their *sum* is $I + J := \{i + j : i \in I, j \in J\}$.
(2) Their *product*, IJ, is the set of all finite sums of elements of the form ij with $i \in I$ and $j \in J$.
(3) The n^{th} *power* of I, written I^n, is the set of finite sums of elements of the form $i_1 \cdots i_n$ with $i_k \in I$ for all k.

$I + J$ is the smallest ideal of R containing both I and J and $IJ \subseteq I \cap J$. Note that IJ is a set of finite sums; the set of terms ij is in general not an ideal.

7.4. **Ideals.** Throughout, R is a ring—not necessarily commutative—with a 1.

Definition 7.20. Let $A \subseteq R$.

(1) We denote by (A) the smallest ideal of R containing A; this is the *ideal generated by* A.
(2) $RA = \{r_1a_1 + \cdots + r_na_n : r_i \in R, a_i \in A\}$.
(3) An ideal generated by a single element is a *principal ideal*. If it is generated by a finite set then it is *finitely generated*.

The notion of (A) here is the same as for generating a subgroup by a subset of some group: (A) is the intersection of all ideals I containing A. In fact, RA is exactly the left ideal generated by A (and AR is the right ideal). Of course if R is commutative we then get that $RA = AR = RAR = (A)$. In this case, if $A = \{a\}$ is a singleton set then (a) is just the set of all R-multiples of a. However, if R isn't commutative then $\{ras : r, s \in R\}$ is not necessarily the two-sided ideal generatd by a since it doesn't need to be closed under addition (the ideal we want is RaR, consisting of *finite sums* of elements of the form ras).

In particular, $b \in (a)$ if and only if $b = ra$, i.e. a divides b. This also gives $(b) \subseteq (a)$.

Example 7.21. Consider the ideal $(2, x) \subset \mathbb{Z}[x]$. We want to show that it isn't principal. Explicitly, $(2, x) = \{2p(x) + xq(x) : p(x), q(x) \in \mathbb{Z}[x]\}$. Assume $(2, x) = (a(x))$. Since $2 \in (a(x))$ there must be some $p(x)$ such that $2 = p(x)a(x)$, so $p(x)$ and $a(x)$ must both be constants (by their degrees). Thus $a(x), p(x) \in \{\pm 1, \pm 2\}$. If $a(x) = \pm 1$ then we would have $(a(x)) = \mathbb{Z}[x]$ which contradicts $(a(x))$ being a proper ideal. Thus $a(x) = \pm 2$. But then $x \in (a(x))$ so $x = 2q(x)$ for some $q(x) \in \mathbb{Z}[x]$, which is impossible.

An important observation is that as an ideal of $\mathbb{Q}[x]$, we do indeed have $(2, x) = \mathbb{Q}[x]$ since $\frac{1}{2} \cdot 2 = 1$ so $(2, x) = (1)$.

Example 7.22. For a finite group G and commutative ring R, the augmentation ideal in RG is generated by $\{g - 1 : g \in G\}$ (although we don't necessarily need all such elements).

Proposition 7.23. Let $I \subseteq R$ be an ideal. Then $I = R$ if and only if I contains a unit. Moreover, R is a field if and only if its only ideals are (0) and (1).

Proof. If $I = R$ then of course $1 \in I$. Conversely, let $u \in I$ be a unit with inverse v. Then for $r \in R$, we have $r = r \cdot 1 = r(vu) = (rv)u \in I$ so $R \subseteq I$ and we are done.

If R is a field then every nonzero ideal contains a unit, so by the above R is the only nonzero ideal. Conversely, let 0 and R be the only ideals and $u \in R$ a nonzero element. Then $(u) = R$ so $1 \in (u)$. Thus there exists $v \in R$ with $1 = vu$, i.e. u is a unit. Thus every nonzero element of R is a unit so R is a field. ■

Corollary 7.24. Any nonzero ring homomorphism from a field R into another ring is injective.

Proof. The kernel is an ideal, which is either 0 or the whole ring. The kernel of a nonzero homomorphism is a proper ideal, so must be 0. ■

If R is a ring with a 1 where the only left and right ideals are (0) and (1), then R is a division ring. Conversely, the only ideals (of any kind) in a division ring are (0) and (1).

Definition 7.25. An ideal $M \subseteq R$ is *maximal* if $M \neq R$ and the only ideals containing M are M and R.

In general, these don't even need to exist. For example, a group with no maximal subgroups suffices (such as $\mathbb{Q}$) as we can trivially turn it into a ring by defining $ab = 0$ for all a, b.

Proposition 7.26. If R is a ring with a 1 then every proper ideal is contained in a maximal ideal.

Proposition 7.27. Let R be commutative. Then an ideal M is maximal if and only if R/M is a field.

Proof. M is maximal if and only if there are no ideals I with $M \subset I \subset R$. The ideals of R containing M are in bijection with the ideals of R/M so M is maximal if and only if the only such ideals in R/M are 0 and the whole ring. But then R/M would be a field, so we are done. ■

Example 7.28. The ideal $(2, x)$ is maximal in $\mathbb{Z}[x]$ since the quotient by it is $\mathbb{Z}/2\mathbb{Z}$. However, the ideal (x) isn't maximal since the quotient is just $\mathbb{Z}$, which is of course not a field.

Example 7.29. Let F be a field and G a finite group. Then the augmentation ideal I is maximal in FG since we have $FG/I \cong F$.

Definition 7.30. Let R be commutative. An ideal P is *prime* if $P \neq R$ and if $ab \in P$ then $a \in P$ or $b \in P$.

Proposition 7.31. Let R be commutative. Then P is a prime ideal if and only if R/P is an integral domain.

Proof. The proof is just a matter of translating what it means to be a prime ideal into the language of quotients. Let $\bar{r} = r + P \in R/P$. Then $r \in P$ if and only if $\bar{r} = 0 \in R/P$. Thus P is a prime ideal if and only if $\bar{R} \neq 0$ and whenever $\bar{a}\bar{b} = 0$ we have either $\bar{a} = 0$ or $\bar{b} = 0$, so R/P is an integral domain. ■

Corollary 7.32. If R is commutative then every maximal ideal in it is prime.

7.5. **Rings of fractions.**

Theorem 7.33. Let R be commutative and let $D \subseteq R$ be nonempty and not containing 0 or any zero divisors as well as being closed under multiplication. Then there is a commutative ring Q with 1 such that R is a subring of Q and every element of D is a unit in Q.

(1) Every element of Q has the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R \setminus \{0\}$ then Q is a field.
(2) Let S be any commutative ring with 1 and $\varphi : R \to S$ an injective ring homomorphism such that $\varphi(d)$ is a unit in S for all $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi \mid_R = \varphi$. Thus Q is the minimal ring containing R in which all elements of D become units.

Definition 7.34. The ring Q is called the *ring of fractions* of D with respect to R and we write $Q = D^{-1}R$. If R is an integral domain and $D = R \setminus \{0\}$ then Q is the *field of fractions* of R.

Corollary 7.35. Let R be an integral domain and Q its field of fractions. If a field F contains a subring $R' \cong R$ then the subfield of F generated by R' is isomorphic to Q.

Example 7.36. If R is a commutative ring with 1 and d is neither zero nor a zero divisor then we can form the ring $R[1/d]$ by setting $D = \{d^k : k \geq 0\}$ and defining $R[1/d] := D^{-1}R$. The elements of $R[1/d]$ are polynomials in $1/d$ with coefficients in R.

7.6. **Chinese Remainder Theorem.**

Definition 7.37. Ideals $A, B \subset R$ are *comaximal* if $A + B = R$.

Theorem 7.38 (Chinese remainder theorem)**.** Let $A_1, \ldots, A_k \subset R$ be ideals. The map $R \to R/A_1 \times \cdots \times R/A_k$ given by $r \mapsto (r + A_1, \ldots, r + A_k)$ is a ring homomorphism with kernel $\bigcap_{i=1}^k A_i$. If A_i and A_j are comaximal for all $i \neq j$ then this map is surjective and $\bigcap_{i=1}^k A_i = A_1 A_2 \cdots A_k$ so that $R/(A_1 \cdots A_k) = R/(A_1 \cap \cdots \cap A_k) \cong R/A_1 \times \cdots \times R/A_k$.

This was motivated by the fact that $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ when $(m, n) = 1$.

The above theorem gives an isomorphism of rings, so in particuarly the groups of units on both sides must be isomorphic as well! Thus we also have $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. More generally:

Theorem 7.39. Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be the prime factorization of $n \in \mathbb{Z}$. Then since

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z}$$

as rings, we also have

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^*.$$

Comparing orders on both sides gives the formula

$$\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_k^{a_k})$$

where φ is the usual totient function. Thus φ is determined by its values at prime powers.

8. Euclidean domains, PIDs, and UFDs

8.1. **Euclidean domains.**

Definition 8.1. A function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is a *norm* on the integral domain R.

Definition 8.2. An integral domain R is a *Euclidean domain* if there is a norm N on R such that for any $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that $a = qb + r$ with $r = 0$ or $N(r) < N(b)$.

Equivalently, a Euclidean domain possesses a division algorithm *which terminates*. This allows us to write $a = q_0 b + r_0, b = q_1 r_0 + r_1, \ldots, r_{n-2} = q_n r_{n-1} + r_n, r_{n-1} = q_{n+1} r_n$ such that $N(b) > N(r_0) > \ldots > N(r_n)$.

Remark. Fields are Euclidean domains (with any norm) since we can always write $a = qb + 0$ where $q = ab^{-1}$.

Example 8.3. $\mathbb{Z}$ is a Euclidean domain with $N(a) = |a|$. If F is a field then $F[x]$ is a Euclidean domain with $N(p(x)) = \deg p(x)$. We need F to be a field (and nothing less) since ultimately this is just long division of polynomials and we rely on being able to divide arbitrary nonzero coefficients.

Example 8.4. The integers $\mathcal{O}$ of quadratic fields are integral domains with a norm given by the absolute value of the field norm but in general they are not Euclidean domains with respect to this. However, some are.

Let $x = a+bi, y = c+di \in \mathbb{Z}[i]$. In $\mathbb{Q}(i)$, $x/y = r+si$ with $r = (ac+bd)/(c^2+d^2)$ and $s = (bc-ad)/(c^2+d^2)$ are rational. Let p be the closest integer to r and q the closest integer to s so $|r-p|, |s-q| \leq 1/2$. Then we have a division algorithm if we show that $x = (p+qi)y + z$ for some $z \in \mathbb{Z}[i]$ such that $N(z) \leq \frac{1}{2}N(y)$. Set $t = (r-p) + (s-q)i$ and $z = yt$. Then $z = x - (p+qi)y$ so $z \in \mathbb{Z}[i]$ and $x = (p+qi)y + z$. Since $N(t) = (r-p)^2 + (s-q)^2 \leq 1/2$, $N(z) = N(y)N(t) \leq 1/2N(y)$ as desired.

The above proof also works for $\mathcal{O}$ when $Z[\sqrt{d}]$ for $D = -2, -3, -7, -11$.

Example 8.5. Recall that an integral domain R is a discrete valuation ring if there is a valuation ν on its field of fractions such that R is the valuation ring of ν. A discrete valuation ring is a Euclidean domain with the norm $N(0) = 0$ and $N = \nu$ otherwise: for $a, b \in R$, $N(a) < N(b)$ implies that $a = 0 \cdot b + a$; if $N(a) \geq N(b)$ then $q = ab^{-1} \in R$ so $a = qb + 0$.

Proposition 8.6. Every ideal in a Euclidean domain is principal.

Proof. Of course assume that I is an ideal other than 0. Let $0 \neq d \in I$ have the smallest norm in I. Clearly $(d) \subseteq I$. Let $a \in I$ and write $a = qd + r$. Then $r = a - qd$ and since $a, qd \in I$ we have $r \in I$. By the minimality of d, we must have $r = 0$. Thus $a = qd$ so $a \in (d)$ and we have $I \subseteq (d)$. ∎

Example 8.7. Let $R = \mathbb{Z}[\sqrt{-5}]$ and N the field norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Set $I = (3, 2 + \sqrt{-5})$. Assume $I = (d)$ was principal, say for $d = a + b\sqrt{-5}$. Then we'd have $2 + \sqrt{-5} = x(a + b\sqrt{-5})$ and $3 = y(a + b\sqrt{-5})$. Taking norms we get $9 = N(x)(a^2 + 5b^2)$ and we must have $a^2 + 5b^2 = 1, 3, 9$. If it's 9 then $N(x) = 1$ so $x = \pm 1$ forcing $a + b\sqrt{-5} = \pm 3$, which is impossible since $3 \nmid 2 + \sqrt{-5}$. It can't be 3 either since there are no integer solutions to $a^2 + 5b^2 = 3$. If it's 1 then $a + b\sqrt{-5} = \pm 1$ and we would have $I = R$. But then $1 \in I$ so $3m + (2 + \sqrt{-5})n = 1$ for some $m, n \in R$. Multiplying both sides by $2 - \sqrt{-5}$ would imply $3 \mid 2 - \sqrt{-5}$, which is impossible. Thus I isn't principal so R is not a Euclidean domain.

Proposition 8.8. If $a, b \in R$ are both nonzero such that $(a, b) = (d)$ then d is their greatest common divisor.

Proposition 8.9. Let R be an integral domain. If $d, d' \in R$ are such that $(d) = (d')$ then $d' = ud$ for some unit $u \in R$. In particular, the greatest common divisor is only determined up to multiplication by a unit.

Proof. Assume d, d' are both nonzero. Since $d \in (d')$ we have $d = xd'$ for some x. For the same reason, we have $d' = yd$ for some y. Thus $d = xyd$ so $d(1 - xy) = 0$. Thus $xy = 1$ so x and y are both units. ∎

Theorem 8.10. Let $a, b \in R$ be elements of a Euclidean domain and $d = r_n$ the last remainder of the division algorithm. Then $(a, b) = d$ and we can always write $d = ax + by$ for some $x, y \in R$.

8.2. **PIDs.**

Definition 8.11. A *PID* is an integral domain in which every ideal is principal.

What we proved earlier is that every Euclidean domain is a PID. Not every result can be ported over, but notably anything about greatest common divisors does.

Proposition 8.12. Every nonzero prime ideal in a PID is maximal.

Proof. Let $(p) \subset R$ and $(p) \subset I = (m)$ be a prime ideal contained in a maximal one. Since $p \in (m)$ we have $p = rm$ for some $r \in R$. Thus $r \in (p)$ or $m \in (p)$. If $m \in (p)$ then $(m) \subseteq (p)$ so $(p) = (m)$. If $r \in (p)$ then $r = ps$ for some $s \in R$ so we have $p = rm = psm$ and thus $sm = 1$. Thus m is a unit so $I = R$. We see then that either $I = (p)$ or $I = R$, so (p) is maximal. ■

Corollary 8.13. If R is a commutative ring such that $R[x]$ is a PID then R is a field.

Proof. Let $R[x]$ be a PID. Since R is a subring it must be an integral domain. Then (x) is a nonzero prime ideal. By the above proposition it is maximal, so R is a field. ■

Remark. There are rings in between Euclidean domains and PIDs: $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is a PID but not a Euclidean domain.

8.3. **UFDs.**

Definition 8.14. Let R be an integral domain and let $r \in R$ be nonzero and not a unit. Then r is *irreducible* if whenever $r = ab$ one of a or b is a unit. If $p \in R$ is nonzero then it is *prime* if (p) is a prime ideal. Two elements $a, b \in R$ that differ only by a unit are said to be *associate*.

Proposition 8.15. Primes are irreducible in an integral domain.

Proof. Let (p) be a prime ideal with $p = ab$. Then $ab \in (p)$ so $a \in (p)$ or $b \in (p)$. Thus $a = pr$ for some $r \in R$ so we have $p = ab = prb$ and we get $rb = 1$, showing that b is a unit. Thus p is irreducible. ■

Remark. In general, irreducible elements aren't always prime. In $Z[\sqrt{-5}]$, 3 is irreducible but isn't prime since $3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ with neither factor being divisible by 3.

Proposition 8.16. In a PID a nonzero element is prime if and only if it's irreducible.

Proof. We only need to show one direction, as the other is satisfied by the previous proposition. Let p be irreducible and let $M = (m)$ be an ideal containing (p). Then $p = rm$. Since it's irreducible, either r or m is a unit. If m is a unit, $M = R$. If r is a unit then $(p) = (m)$. Thus (p) is in fact a maximal ideal and since these are prime, (p) is also prime. ■

Definition 8.17. A UFD is an integral domain R such for for any nonzero $r \in R$, the following holds:

(1) r can be written as a finite product of irreducibles $p_i \in R$
(2) The above decomposition is unique up to multiplication by a unit, i.e. if $r = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$ then $m = n$ and $p_i = u_i q_i$ for units u_i for all i.

Example 8.18. $\mathbb{Z}[\sqrt{-5}]$ is not even a UFD since $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ gives distinct factorizations into irreducibles.

Proposition 8.19. In a UFD, a nonzero element is prime if and only if it's irreducible.

Proof. Again, since the proposition from the previous section was for general integral domains, we only need to prove one direction. Let $p \in R$ be irreducible and assume $p \mid ab$. We need to show that $p \mid a$ or $p \mid b$. Write $ab = pc$ for some $c \in R$. We can write a and b each as a product of irreducible elements uniquely, giving a unique factorization of ab. As such, the factorization of p must associate to one of the irreducible elements in the factorization of a or b. Assume this occurs for a so that we can write $a = (up)p_2 \cdots p_n$ for u a unit. But then $p \mid a$ so we are done. ■

Thus we can use the terms prime and irreducible interchangeably in a UFD.

Theorem 8.20. Every PID is a UFD.

Thus we have Euclidean domains $\supset$ PIDs $\supset$ UFDs, all these being proper inclusions.

8.3.1. *Factorization in* $\mathbb{Z}[i]$. Let $\mathcal{O}$ be a quadratic integer ring and N its field norm. Let $a \in \mathcal{O}$ be an element such that $N(a) = p$ is prime. If $a = bc$ then $p = N(a) = N(b)N(c)$ so then one of b or c must be a unit. Thus if $N(a) = \pm p$ it is irreducible in $\mathcal{O}$!

Let $\pi \in \mathcal{O}$ be prime. Since (π) is a prime ideal, also $(\pi) \cap \mathbb{Z}$ is prime: if $ab \in (\pi)$ with $a, b \in \mathbb{Z}$ then either a or b is in (π) since it is prime, so then a or b is in $(\pi) \cap \mathbb{Z}$. Since $N(\pi)$ is a nonzero integer in (π), we must have $(\pi) \cap \mathbb{Z} = (p) \subset \mathbb{Z}$. As $p \in (\pi)$, $\pi \mid p$ so primes of $\mathcal{O}$ can be found by seeing how primes in $\mathbb{Z}$ split. Let $p = \pi\pi'$. Then $N(\pi)N(\pi') = N(p) = p^2$ so as π is not a unit the only possibilites are $N(\pi) = \pm p$ or $N(\pi) = \pm p^2$. In the first case, we would have $N(\pi') = \pm 1$ so π' is a unit and we have $(p) = (\pi) \subset \mathbb{Z}[i]$, showing that π is irreducible. In the latter case, we would just have that p is a product of irreducibles.

The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$. Since $\mathbb{Z}[i]$ is a Euclidean domain, it's also a PID and UFD so its irreducibles are the same as its primes. For a general element $a + bi \in \mathbb{Z}[i]$, $N(a) = a^2 + b^2 = a\bar{a}$. Then by the above, p factors in $\mathbb{Z}[i]$ into two irreducibles if and only if $p = a^2 + b^2$ is the sum of two squares. Since the square of any integer is either 0 or 1 mod 4, an odd prime that is the sum of two squares must be congruent to 1 mod 4. (When $p = 2 = 1^2 + 1^2$, we have $2 = (1+i)(1-i) = -i(1+i)^2$. The irreducibles $1+i$ and $1-i = -i(1+i)$ and this is the only time $a + bi$ and $a - bi$ are associates.) Thus if $p \equiv 3 \mod 4$ it can't be written as a product of two squares so it remains irreducible in $\mathbb{Z}[i]$.

Lemma 8.21. $p \mid n^2+1$ if and only if $p = 2$ or is an odd prime that's 1 mod 4.

Proof. It's trivial for 2 since $2 \mid 1^2+1$ and all other n^2+1 are odd. Let p be an odd prime. Then $p \mid n^2+1$ if and only if $n^2 \equiv -1 \mod p$. Equivalently, n has order 4 in $(\mathbb{Z}/p\mathbb{Z})^*$. By Lagrange's theorem, this can only happen if $4 \mid p-1$, i.e. $p \equiv 1 \mod 4$.

Conversely, let $4 \mid p-1$. If $m^2 \equiv 1 \mod p$ then $m^2-1 = (m-1)(m+1)$ so either $p \mid m-1$ ($m \equiv 1 \mod p$) or $p \mid m+1$ ($m \equiv -1 \mod p$). In either case, we get an order 2 element in $(\mathbb{Z}/p\mathbb{Z})^*$. Since $(\mathbb{Z}/p\mathbb{Z})^*$ is abelian, it contains an order 4 subgroup H (for example, the quotient by $\{\pm 1\}$ has an order 2 subgroup whose preimage has order 4). H can't be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ since it has an order 4 element, so $H \cong \mathbb{Z}/4\mathbb{Z}$. Thus $(\mathbb{Z}/p\mathbb{Z})^*$ has an order 4 element—the generator of H. ■

Now if $p \equiv 1 \mod 4$, we know that $p \mid n^2+1 = (n+i)(n-i)$. If p is irreducible in $\mathbb{Z}[i]$ then p must divide one of the factors. But then p must be a real number so in fact it would divide both of them. However, it would also then divide their difference, $2i$, which clearly cannot be possible. Thus we have the following:

Theorem 8.22 (Fermat)**.** p is a sum of two squares if and only if $p = 2$ or $p \equiv 1 \mod 4$. It's unique up to changing the signs of a and b. Moreover, the irreducible elements in $\mathbb{Z}[i]$ are:

(1) $1+i$ (norm 2)
(2) $p \in \mathbb{Z}$ with $p \equiv 3 \mod 4$ (they have norm p^2)
(3) $a+bi, a-bi$, the distinct irreducible factors of $p = a^2+b^2$ for $p \in \mathbb{Z}$ with $p \equiv 1 \mod 4$

9. Polynomial rings

9.1. **Definitions and basics.**

Proposition 9.1. Let $I \subseteq R$ be an ideal and $(I) = I[x]$ denote the ideal in $R[x]$ generated by I. Then $R[x]/(I) \cong (R/I)[x]$.

Proof. We have a map $\varphi : R[x] \to (R/I)[x]$ just reducing each coefficient of a polynomial modulo I. The kernel is exactly the set of polynomials all of whose coefficients are in I, which is exactly I. By the first isomorphism theorem, we're done. ■

This also shows that if I is a prime ideal then so is (I) since R/I is an integral domain and thus so is $(R/I)[x]$. However, this doesn't hold with maximal ideals, as if I is maximal in R then the ideal generated by I and x is maximal. This can also be seen since if (I) was maximal then $R[x]/(I)$ would be a field. But we'll see later that $(R/I)[x]$ isn't a field even if R/I is.

9.2. **Polynomial rings over fields I.**

Theorem 9.2. Let F be a field. Then $F[x]$ is a Euclidean domain.

Thus it's also a PID and UFD. Recall that the converse also holds whenever $F[x]$ is a PID. However, we'll see that it's more general if we only require $F[x]$ to be a UFD.

Example 9.3. $\mathbb{Q}[x, y]$ isn't a PID since $\mathbb{Q}[x, y] = \mathbb{Q}[x][y]$ and $\mathbb{Q}[x]$ isn't a field (any positive degree polynomial has no inverse). We can see this explicitly since (x, y) isn't principal.

Note that the division algorithm is independent of field extension. If $F \subset E$ is a field extension and $a(x) = Q(x)b(x) + R(x)$ for $a(x), b(x) \in F[x]$ and $Q(x), R(x) \in E[x]$ then since we can write $a(x) = q(x)b(x) + r(x)$ with all polynomials in $F[x]$ it can be seen that $R(x) = r(x)$ and $Q(x) = q(x)$ by the uniqueness of the division algorithm. In particular, $b(x) \mid a(x)$ in $E[x]$ if and only if this is true in $F[x]$.

9.3. **Polynomial rings that are UFDs.**

Proposition 9.4 (Gauss' lemma)**.** Let R be a UFD with fraction field F and let $p \in R[x]$. If p is reducible in $F[x]$ then it's reducible in $R[x]$.

Corollary 9.5. Let R be a UFD, F its fraction field, and $p \in R[x]$. If the coefficients of p are all coprime then p is irreducible in $R[x]$ if and only if it's irreducible in $F[x]$. In particular, the assumption is immediately satisfied if p is monic.

Proof. If p is reducible in $F[x]$ then it's reducible in $R[x]$, so we have one direction (contrapositive). Conversely, by the assumption on the coefficients, if $p = ab$ with $a, b \in R[x]$ then neither a nor b are constant polynomials. The same factorization works in $F[x]$, so we're done. ■

Theorem 9.6. R is a UFD if and only if $R[x]$ is a UFD.

Corollary 9.7. If R is a UFD then so is R adjoined with an arbitrary number of variables.

Proof. The finite case follows from $R[x, y] = R[x][y]$. Note that $R[[x]] = \bigcup_{i=0}^{\infty} R[x_1, \ldots, x_i]$, which takes care of the infinite case. ■

9.4. **Irreducibility.**

Proposition 9.8. Let F be a field and $p(x) \in F[x]$. Then $p(x)$ has a linear factor if and only if it has a root in F.

Proof. If $p(x)$ has a linear factor then since F is a field we can assume the factor is monic, say has the form $x - a$. But then $p(a) = 0$. Conversely, let $p(a) = 0$. By the division algorithm, $p(x) = q(x)(x - a) + r$ where r is a constant. Evaluating both sides at a, we must have $r = 0$. ■

Corollary 9.9. A degree 2 or 3 polynomial over a field is reducible if and only if it has a root.

Proposition 9.10. Let $p(x) = a_n x^n + \cdots + a_0$. If $r/s \in \mathbb{Q}$ with $(r, s) = 1$ and $p(r/s) = 0$ then $r \mid a_0$ and $s \mid a_n$.

Proof. Since r/s is a root, we have $a_n(r/s)^n + \cdots + a_0 = 0$, and multiplying through by s^n gives $a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_0 s^n = 0$. Thus $a_n r^n = s(-a_{n-1} r^{n-1} - \cdots - a_0 s^{n-1})$ so $s \mid a_0 r^n$. But $(r, s) = 1$, so $s \mid a_0$. The proof for $r \mid a_n$ is the same. ■

Directly from this we see that monic polynomials cannot have rational roots.

Proposition 9.11. Let I be a proper ideal in an integral domain R and $p(x) \in R[x]$ a nonconstant monic polynomial. If the image of $p(x)$ in $(R/I)[x]$ can't be factored then $p(x)$ is irreducible in $R[x]$.

Proof. Assume $p(x)$ can't be factored in $(R/I)[x]$ but can be in $R[x]$. Then we have $p(x) = a(x)b(x)$ a product of monic polynomials. But then reduction mod I gives a factorization in $(R/I)[x]$ with nonconstant factors, which is a contradiction. ■

Proposition 9.12 (Eisenstein)**.** Let P be a prime ideal of an integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$. Then if $a_i \in P$ for all i but $a_0 \notin P^2$ then $f(x)$ is irreducible.

Proof. Let $f(x) = a(x)b(x)$ be irreducible in $R[x]$. Reducing modulo P gives $x^n = \overline{a(x)b(x)}$ in $(R/P)[x]$. Since P is prime, R/P is an integral domain so $\overline{a(x)}$ and $\overline{b(x)}$ have no constant term. But then the constant a_0 of $f(x)$ would belong to P^2, which is a contradiction. ■

Remark. Let $f(x) = x^4+1$. We can't apply Eisenstein to it, but for $g(x) = f(x+1) = x^4+4x^3+6x^2+4x+2$, we see that it is Eisenstein at 2. Thus $g(x)$ is irreducible, so $f(x)$ is also. Thus we can confirm that a polynomial is irreducible without directly applying Eisenstein's criterion to it.

Example 9.13. Let $\varphi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$. Clearly Eisenstein doesn't apply to it, but it does to $\varphi_p(x + 1) = \frac{(x+1)^p-1}{x} = x^{p-1} + px^{p-2} + \cdots + \frac{p(p-1)}{2}x + p \in \mathbb{Z}[x]$ by the Binomial theorem. Thus $\varphi_p(x)$ is irreducible in $\mathbb{Z}[x]$.

Example 9.14. Let $R = \mathbb{Q}[x]$ and consider $X^n - x \in R[X]$. The ideal (x) is prime in R ($R/(x) \cong Q$ is a field, so (x) is even maximal) so by Eisenstein $X^n - x$ is irreducible.

9.5. **Polynomial rings over fields II.**

Proposition 9.15. The maximal ideals in $F[x]$ are $(f(x))$ where $f(x)$ is an irreducible polynomial.

Note that this implies $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proposition 9.16. Let $g(x) = f_1(x)^{n_1} \cdots f_k(x)^{n_k}$ be its factorization into irreducibles in $F[x]$. Then $F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times \cdots \times F[x]/(f_k(x)^{n_k})$.

Proof. Chinese remainder theorem. ■

Proposition 9.17. Let $f(x)$ have roots $a_1, \ldots, a_k$ in F, not necessarily distinct. Then $(x - a_1) \cdots (x - a_k)$ is a factor of $f(x)$.

Proposition 9.18. A finite subgroup of F^* is cyclic. In particular, if F is finite then F^* is cyclic.

Proof. We can write such a finite subgroup (which of course is abelian) as $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_k\mathbb{Z}$ by the fundamental theorem of finite abelian groups with $n_k \mid n_{k-1} \mid \cdots \mid n_2 \mid n_1$. In general, if G is a cyclic group and $d \mid |G|$ then G has exactly d elements of order dividing d. Since n_k divides the order of each group in the product, it follows that each factor contains n_k elements of order dividing n_k. If $k > 1$ then we would have more than n_k such elements. But then there would be more than n_k roots of $x^{n_k} - 1$ in F, which is impossible. Thus $k = 1$ so the group is cyclic. ■

9.6. **Polynomials in several variables and Gröbner bases.**

Definition 9.19. A commutative ring R with a 1 is *Noetherian* if every ideal is finitely generated.

Theorem 9.20 (Hilbert's basis theorem)**.** If R is Noetherian then so is $R[x]$.

Corollary 9.21. Every ideal in $F[x_1, \ldots, x_n]$ is finitely generated, i.e. it's a Noetherian ring.

10. Intro to modules

10.1. **Basic definitions and examples.** Note that any ring R is an R-module over itself (left or right, doesn't matter) where the action is just multiplication in R. In this case, the R-submodules are the ideals. If R isn't commutative then the left and right R-module structures over itself may induce different submodules!

Example 10.1. Let M be an R-module and I an ideal of R. If $am = 0$ for all $a \in I$ and $m \in M$ then M is *annihilated* by I. Then we can make M into an (R/I)-module by defining $(r + I) \cdot m := rm$. In particular, when I is maximal, R is commutative, and $IM = 0$, then M is a vector space over R/I.

Example 10.2. Let A be any abelian group, finite or infinite, with operation $+$. We make A into a $\mathbb{Z}$-module by defining $na = a + a + \cdots + a$ n times, where it's just 0 if $n = 0$ and we replace $+$ with $-$ if $n < 0$. In fact this is the only way to turn A into a $\mathbb{Z}$-module. Thus every abelian group is a $\mathbb{Z}$-module. Conversely, if M is a $\mathbb{Z}$-module then by definition it is an abelian group. Thus we see that $\mathbb{Z}$-modules are the exact same thing as abelian groups and the submodules are exactly the subgroups. Note that if A has order m then by the above example we can turn it into a $\mathbb{Z}/m\mathbb{Z}$-module.

Example 10.3. Let F be a field, $R = F[x]$, and V a vector space over F with a linear transformation $T : V \to V$. We already know that V is an F-module. Define $T^0 = I$ and T^n to be T composed with itself n times. Let $p(x) = a_n x^n + \cdots + a_0 \in R$. For $v \in V$, we define the action of $p(x)$ on v by $p(x) \cdot v := (a_n T^n + \cdots + a_0)(v)$ which is indeed a linear transformation from V to itself as it is a sum of linear transformation. We are just defining x to act on V by applying T and extending it linearly to all of $F[x]$. Note that this $F[x]$-action extends the action of F on V. We turned V into an $F[x]$-module given only a linear transformation $T : V \to V$, and in general this gives us a bijection between $F[x]$-module structures and such transformations (i.e. different T gives different structure). An $F[x]$-submodule W is first an F-submodule and is also stable under the action of x. Thus the $F[x]$-submodules are exactly the subspaces of V which are invariant under the action of T.

Proposition 10.4. Let M be an R-module. A subset $N \subseteq M$ is a submodule fi and only if N is nonempty and $x + ry \in N$ for all $r \in R$ and $x, y \in N$.

Definition 10.5. Let R be commutative with a 1. An *R-algebra* is a ring A with a ring homomorphism $f : R \to A$ such that $1_R \mapsto 1_A$ and $f(R) \subseteq Z(A)$.

If A is an R-algebra then it has a natural (left or right) R-module structure given by $r \cdot a = a \cdot r = f(r)a$ given by multiplication in A.

Definition 10.6. An *R-algebra homomorphism* is a ring homomorphism $\varphi : A \to B$ such that $1_A \mapsto 1_B$ and $\varphi(r \cdot a) = r \cdot \varphi(a)$ for all $r \in R, a \in A$.

Remark. Every ring with identity is a $\mathbb{Z}$-algebra.

10.2. **Quotient modules and module homomorphisms.**

Example 10.7. If we let R be a module over itself, then R-module homomorphism don't need to be the same as ring homomorphisms and vice versa. When $R = \mathbb{Z}$, $x \mapsto 2x$ is a $\mathbb{Z}$-module homomorphism but not a ring homomorphism since 1 doesn't map to 1. When $R = F[x]$, $f(x) \mapsto f(x^2)$ is a ring homomorphism but not an $F[x]$-module homomorphism since we would ahve $x^2 = \varphi(x) = \varphi(x \cdot 1) = x\varphi(1) = x$.

Note that $\mathrm{Hom}_R(M, N)$ is an R-module by defining $(\varphi + \psi)(m) = \varphi(m) + \psi(m)$ and $(r\varphi)(m) = r(\varphi(m))$. When $M = N$ then $\mathrm{Hom}_R(M, M)$ is a ring with 1 and when R is commutative it is even an R-algebra.

Definition 10.8. $\mathrm{Hom}_R(M, M)$ is the *endomorphism ring* of M and will be written $\mathrm{End}_R(M)$, or just $\mathrm{End}(M)$.

When R is commutative we get a map $R \to \mathrm{End}(M)$ given by $r \mapsto rI$. This turns $\mathrm{End}(M)$ into an R-algebra. However, this doesn't need to be injective since we could have $rm = 0$ for all and $m \in M$ (e.g. $R = \mathbb{Z}, M = \mathbb{Z}/2\mathbb{Z}, r = 2$). We get injectivity when R is a field.

Since modules are first and foremost abelian groups, all subgroups are normal. This allows us to construct the quotient module M/N for any module M and any submodule N. Specifically, if M is an R-module then M/N is an R-module by defining $r(x + N) = (rx) + N$. All of the usual isomorphism theorems then hold for modules as well.

10.3. **Generating modules, direct sums, and free modules.**

Definition 10.9. Let M be an R-module and $N_1, \dots, N_n$ submodules.

- The *sum* of the N_i is the set of all finite sums of their elements: $N_1 + \cdots + N_n := \{a_1 + \cdots + a_n : a_i \in N_i\}$.
- For any $A \subseteq M$ let $RA = \{r_1 a_1 + \cdots + r_m a_m : r_i \in R, a_i \in A\}$ be the set of all finite linear combinations of elements in A. We say that RA is the *submodule of M generated by A*.
- A submodule is *cyclic* if there exists $a \in M$ such that $N = Ra$, i.e. is generated by a single element.

For R a ring with 1 as a module over itself, it is cyclic since $R = R \cdot 1$. The submodules are the ideals of R, so a submodule being cyclic is equivalent to an ideal being principal. However, in general submodules of a finitely generated module don't need to be finitely generated: let $R = F[[x]]$ be a module over itself. Then the submodule generated by all the indeterminates x_i cannot be finitely generated.

Proposition 10.10. Let $N_1, \dots, N_k$ be submodules of an R-module M. The following are equivalent:

(1) $\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$ is an isomorphism.
(2) $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ for all k
(3) Every $x \in N_1 + \cdots + N_k$ can be written uniquely in the form $a_1 + \cdots + a_k$ with $a_i \in N_i$.

Proof. Assume (1). Suppose that for some j (2) fails to hold and let $a_j \in (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) \cap N_j$ be nonzero. Then $a_j = a_1 + \cdots + a_{j-1} + a_{j+1} + a_k$ for $a_i \in N_i$ and $(a_1, \dots, a_{j-1}, -a_j, a_{j+1}, \dots, a_k) \in \ker \pi$ is nonzero, a contradiction.

Now assume (2) Let $a_1 + \cdots + a_k = b_1 + \cdots + b_k$ so that for each j we have $a_j - b_j = (b_1 - a_1) + \cdots + (b_{j-1} - a_{j-1}) + (b_{j+1} - a_{j+1}) + \cdots + (b_k - a_k)$. The LHS is in N_j and the RHS belongs to the sum of all N_i except N_j. Thus $a_j - b_j$ is in the intersection of the sum of these N_i with N_j, so it must be 0 and we have $a_j = b_j$.

Now assume (3). Clearly π is surjective. Then (3) is equivalent to assuming it's injective as well, so we are done. ∎

If an R-module $M = N_1 + \cdots + N_k$ satisfies the above conditions then we write $M = N_1 \oplus \cdots \oplus N_k$ and say it is the *direct sum* of these submodules. This is just saying that we can write every element of M as a unique linear combination of elements from these submodules.

Definition 10.11. An R-module F is *free* on the set $A \subset F$ if for all nonzero $x \in F$ we can write $x = \sum_{i=1}^{n} r_i a_i$ for $r_i \in R$ and $a_i \in A$. Then A is a *basis* for F and if R is commutative then $\#A$ is the *rank*.

Theorem 10.12. For any set A there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following universal property: if M is any R-module and $\varphi : A \to M$ is a set map, then there is a unique R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$ for all $a \in A$, i.e. the following diagram commutes.

$$\begin{array}{ccc} A & \xrightarrow{i} & F(A) \\ & \searrow^{\varphi} & \downarrow \Phi \\ & & M \end{array}$$

When $A = \{a_1, \dots, a_n\}$ is finite, we just have $F(A) = Ra_1 \oplus \cdots \oplus Ra_n \cong R^n$.

This is pretty much the same as for free groups.

10.4. **Tensor product.** We can sort of assume implicitly that any rings mentioned from here on are commutative so will usually make no distinction between left and right modules, ideals, etc. What is written below may not be wholly accurate to the most minute detail, but it is morally accurate.

10.4.1. *Extension of scalars.* Let $R \subseteq S$ be a subring and that $1_R = 1_S$. If N is an S-module then it is naturally an R-module as well. In general, if $f : R \to S$ is a ring homomorphism with $1_R \mapsto 1_S$ (such as inclusion) then N is an R-module with $rn = f(r)n$ for $r \in R$ and $n \in N$. Here, we say that S is an *extension* of the ring R and the resulting R-module is obtained from N by *restriction of scalars* from S to R.

Now assume we have an R-module N and want to put an S-module structure on it ("extending" the scalars). In general this isn't possible (for example, $\mathbb{Z}$ is a $\mathbb{Z}$-module but can't be made into a $\mathbb{Q}$-module). However, we can embed $\mathbb{Z}$ into a $\mathbb{Q}$-module, namely $\mathbb{Q}$ itself. Thus we want to see if we can embed the R-module N as an R-submodule of some S-module, or more generally R-module homomorphisms from N to an S-module. Let N be a nontrivial finite abelian group and consider a $\mathbb{Z}$-module homomorphism of N into a $\mathbb{Q}$-module, which is just a vector space over $\mathbb{Q}$. Every nonzero element in a $\mathbb{Q}$-vector space has infinite (additive) order, but none of the elements in N do so they must all just map to 0. Thus there are no nonzero $\mathbb{Z}$-module homomorphisms from N into any $\mathbb{Q}$-module.

If the R-module N is already an S-module then extending scalars isn't an issue. We need a way to define products sn for $s \in S$ and $n \in N$. Consider the free $\mathbb{Z}$-module (read: abelian group) on the set $S \times N$, i.e. the collection of all finite commuting sums of the form (s_i, n_i). There aren't any relationships between distinct pairs; to make this an S-module, we need to impose some. Thus we quotient this abelian group by the subgroup H generated by elements of the form

$$\begin{gathered}(s_1 + s_2, n) - (s_1, n) - (s_2, n),\\ (s, n_1 + n_2) - (s, n_1) - (s, n_2), \text{ and}\\ (sr, n) - (s, rn).\end{gathered}$$

In other words, we are forcing bilinearity of the operation onto the quotient. In the last relation, rn refers to the R-module structure we assume already exists on N.

The resulting quotient group is denoted $S \otimes_R N$. This is the *tensor product of S and N over R*. Let $s \otimes n$ denote the coset containing (s, n) in $S \otimes N$ so that by definition we have $(s_1 + s_2) \otimes n = s_1 \otimes n + s_2 \otimes n$, etc. These elements are *tensors*. The point of this construction is that $S \otimes N$ is now an S-module. The action is given by

$$s\left(\sum_{\text{finite}} s_i \otimes n_i\right) = \sum_{finite} (ss_i) \otimes n_i.$$

In fact, it is exactly the S-module obtained by extension of scalars from the R-module N.

There's a natural map $i : N \to S \otimes N$ given by $n \mapsto 1 \otimes n$ (i.e. do $n \mapsto (1, n)$ in the free group and pass to the quotient). Since $1 \otimes rn = r \otimes n = r(1 \otimes n)$, this is an R-module homomorphism. However, it isn't generally injective as we are working in a quotient group. As such, though a homomorphism may exist, there is no need for $S \otimes N$ to contain an isomorphic copy of N.

Theorem 10.13. Let $R \subseteq S$ be a subring, N an R-module, and $i : N \to S \otimes_R N$ an R-module homomorphism given by $i(n) = 1 \otimes n$. Let L be an S-module and $\varphi : N \to L$ an R-module homomorphism. Then there is a unique S-module homomorphism $\Phi : S \otimes_R N \to L$ such that φ factors through Φ, i.e. $\varphi = \Phi \circ i$ and the diagram commutes. Conversely, if $\Phi : S \otimes_R N \to L$ is an S-module homomorphism then $\varphi = \Phi \circ i : N \to L$ is an R-module homomorphism.

Remark. For any ring R and R-module N, we have $R \otimes_R N \cong N$, so extending scalars from a ring to itself doesn't do anything. This is because we just take φ to be the identity from N to itself and $S = R$ in the above diagram. As a result, if A is any abelian group then $\mathbb{Z} \otimes_{\mathbb{Z}} A = A$.

Example 10.14. Let A be an order n abelian group. Then the $\mathbb{Q}$-module $\mathbb{Q} \otimes_{\mathbb{Z}} A$ obtained by extending scalars from $\mathbb{Z}$ is just 0: note first that in any tensor product, $1 \otimes 0 = 1 \otimes (0 + 0) = 1 \otimes 0 + 1 \otimes 0$ so that $1 \otimes 0 = 0$. Now let $q \otimes a \in \mathbb{Q} \otimes_{\mathbb{Z}} A$ and write $q = (q/n)n \in \mathbb{Q}$. Since $na = 0$ in A, we have $q \otimes a = (\frac{q}{n} \cdot n) \otimes a = \frac{q}{n} \otimes na = \frac{q}{n} \otimes 0 = 0$.

Remark. Let $N \cong R^n$ be a free rank n R-module. Then $S \otimes_R N \cong S^n$ is a free rank n S-module. For example, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong \mathbb{Q}^n$.

10.4.2. *The general definition.* This is similar to the above. Let N and M be any R-modules and consider the quotient of the free abelian group on $M \times N$ with the same relations as we specified previously. Then we again form the tensor product $M \otimes_r N$. We get a natural map $i : M \times N \to M \otimes_R N$ given by $i(m,n) = m \otimes n$. It isn't generally even a group homomorphism, but it is additive in m and n separately and satisfies $i(mr,n) = mr \otimes n = m \otimes rn = i(m,rn)$. Since we assume that R is commutative, this turns the tensor product into an R-module (we are not necessarily trying to extend anything, though we could even in more general language than above). The universal property of tensor products gives us:

Theorem 10.15. Let R be a commutative ring and M, N R-modules with $M \otimes_R N$ their tensor product over R. Then $M \otimes_R N$ is an R-module with $r(m \otimes n) = (rm) \otimes n = (mr) \otimes n = m \otimes (rn)$ and $i : M \times N \to M \otimes_R N$ is R-bilinear. If L is any R-module then we have a bijection

$$\left\{ \begin{array}{l} R\text{-bilinear maps} \\ \varphi : M \times N \to L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} R\text{-module homomorphisms} \\ \Phi : M \otimes_R N \to L \end{array} \right\}$$

where the correspondence between φ and Φ is given by

$$\begin{array}{ccc} M \times N & \xrightarrow{\ i\ } & M \otimes_R N \\ & \searrow^{\varphi} & \downarrow \Phi \\ & & L \end{array}$$

Example 10.16. Consider $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$. Since $a = 3a$ for all $a \in \mathbb{Z}/2\mathbb{Z}$, we have $a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes 0 = 0$ so the entire tensor product is 0 (even $1 \otimes 1 = 0$). However, $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is generated by $0 \otimes 0 = 1 \otimes 0 = 0 \otimes 1$ and $1 \otimes 1$. Since $2(1 \otimes 1) = 2 \otimes 1 = 0 \otimes 1 = 0$, the tensor product is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

In general, $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(m,n)\mathbb{Z}$. Let $(m,n) = d$ for ease. Note that $a \otimes b = ab(1 \otimes 1)$ so the tensor product is cyclic and generated by $1 \otimes 1$. Since $m(1 \otimes 1) = 0 = n(1 \otimes 1)$, we must also have $d(1 \otimes 1) = 0$, so the cyclic group has order dividing d. The map $\varphi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ given by $\varphi(a \mod m, b \mod n) = ab \mod d$ is well-defined since $d \mid m, n$ and is $\mathbb{Z}$-bilinear. The induced map Φ from the tensor product to $\mathbb{Z}/d\mathbb{Z}$ sends $1 \otimes 1 \mapsto 1 \in \mathbb{Z}/d\mathbb{Z}$ which has order d. Thus the order of the tensor product is at least d. Thus $1 \otimes 1$ has order d and we have the desired isomorphism.

Example 10.17. Consider $(a/b \mod \mathbb{Z}) \otimes (c/d \mod \mathbb{Z}) \in \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$. We have $(a/b \mod \mathbb{Z}) \otimes (c/d \mod \mathbb{Z}) = d(a/bd \mod \mathbb{Z}) \otimes (c/d \mod \mathbb{Z}) = (a/bd \mod \mathbb{Z}) \otimes d(c/d \mod \mathbb{Z}) = (a/bd \mod \mathbb{Z}) \otimes 0 = 0$ so the whole tensor product is 0. In fact, for any divisible abelian group A and torsion abelian group B, $A \otimes_{\mathbb{Z}} B = 0$. Thus $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$ as well.

Example 10.18. Let $f : R \to S$ be a ring homomorphism with $1_R \mapsto 1_S$. Then $s \cdot r = f(s)r$ turns S into an R-module so that for an R-module N, we can construct the tensor product $S \otimes_R N$ to be an S-module. This is called *base change* from R to S. This slightly generalizes extension of scalars where we specifically had R a subring of S.

In this setup, $S \otimes_R R \cong S$: the map $\varphi : S \times R \to S$ given by $(s,r) \mapsto s \cdot r = sf(r)$ satisfies $\varphi(s_1 + s_2, r) = \varphi(s_1, r) + \varphi(s_2, r)$, the same for the second argument, and $\varphi(sr, r') = (sr)r' = s(rr') = \varphi(s, rr')$. Then we get an associated grioup homomorphism $\Phi : S \otimes_R R \to S$ with $\Phi(s \otimes r) = sr$. This is an S-module homomorphism with inverse $\Phi' : S \to S \otimes_R R$ given by $s \mapsto s \otimes 1$. This $\Phi'\Phi = 1$ so we have the desired isomorphism.

Theorem 10.19. Let M, M', N, N' be R-modules with $\varphi : M \to M'$ and $\psi : N \to N'$ R-module homomorphisms. Then there is a unique group homomorphism $\varphi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$ with $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$.

Theorem 10.20. The tensor product is associative, i.e. $(M \otimes_R N) \otimes_T L \cong M \otimes_R (N \otimes_T L)$ as abelian groups via the map $(m \otimes n) \otimes l \mapsto m \otimes (n \otimes l)$.

Note that *everything* we've done so far can be extended to multilinear maps by the above theorem.

Theorem 10.21. Let M, M', N, N' be R-modules. Then there are unique R-module isomorphisms

$$(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$$
$$M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes_R N').$$

In other words, tensor products commute with direct sums (as operations). The above result can be extended to any index set (including uncountable).

Corollary 10.22. Let $N \cong R^n$ be a free R-module. Then extension of scalars from R to S gives $S \otimes_R R^n \cong S^n$ as S-modules.

Proof. This follows from the fact that $S \otimes_R R \cong S$ and the theorem above, as we just take direct sums. ■

Corollary 10.23. Let $M \cong R^s$ and $N \cong R^t$ be free R-modules with bases $m_1, \dots, m_s$ and $n_1, \dots, n_t$. Then $M \otimes_R N$ is a free R-module of rank st with basis $m_i \otimes n_j$, i.e. $R^s \otimes R^t \cong R^{st}$.

Proposition 10.24. Let R be commutative and M, N R-modules. Then $M \otimes_R N \cong N \otimes_R M$.

Proposition 10.25. Let R be a commutative ring and A, B R-algebras. Then the multiplication $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ is well defined and makes $A \otimes_R B$ an R-algebra.

Example 10.26. $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is a free rank 4 modules over $\mathbb{R}$ with basis $1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i$ (since $\mathbb{C} \cong \mathbb{R}^2$). It's a commutative ring with unit $1 \otimes 1$ and $(i \otimes i)(i \otimes i) = i^2 \otimes i^2 = -1 \otimes -1 = (-1)^2 \otimes 1 = 1 \otimes 1 = 1$. Let $e = i \otimes i$. Then this shows that $(e-1)(e+1) = 0$ so $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is not an integral domain.

Note that the left and right $\mathbb{R}$-actions coincide but $i \cdot (1 \otimes 1) = i \otimes 1$ and $(1 \otimes 1) \cdot i = 1 \cdot i$ so the left and right $\mathbb{C}$-actions are not necessarily the same.

10.5. **Exact sequences; projective, injective, flat modules.** We want to go in the reverse direction of the first isomorphism theorem: namely, given two modules A and C we want to consider whether there is a module B containing A such that $B/A \cong C$. A being isomorphic to a submodule of B is equivalent to specifying an injective homomorphism $\psi : A \to B$ (as then $A \cong \psi(A)$). For C to be isomorphic to the resulting quotient is equivalent to the existence of a surjective homomorphism $\varphi : B \to C$ such that $\ker \varphi = \psi(A)$. In particular we get a pair of homomorphisms $A \xrightarrow{\psi} B \xrightarrow{\varphi} C$ with $\mathrm{im}\psi = \ker\ phi$.

Definition 10.27. A pair of homomorphisms $X \xrightarrow{a} Y \xrightarrow{b} Z$ is *exact* if $\mathrm{im}a = \ker b$. A sequence of such homomorphisms $\cdots \to X_{n-1} \to X_n \to X_{n+1} \to \cdots$ is an *exact sequence* if it's exact at every X_n.

Proposition 10.28. Let A, B, C be R-modules. Then $0 \to A \xrightarrow{\psi} B$ is exact at A if and only if ψ is injective. Similarly, the sequence $B \xrightarrow{\varphi} C \to 0$ is exact at C if and only if φ is surjective.

Proof. The image of $0 \to A$ is just 0, so ψ is injective if and only if this is its kernel. Similarly, the kernel of $C \to 0$ is all of C, which is exactly $\varphi(B)$ if and only if φ is surjective. ∎

Thus having an exact sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is equivalent to ψ being injective, φ being surjective, and $\mathrm{im}\psi = \ker\varphi$. We call this a *short exact sequence*. Thus we can rephrase the extension problem as: given modules A and C, find all short exact sequences as above. If we write everything multiplicatively, we'll use 1 instead of 0 (it's all the same anyway). Note that if we have an exact sequence $X \xrightarrow{a} Y \xrightarrow{b} Z$, the sequence $0 \to a(X) \to Y \to Y/\ker b \to 0$ is short exact. Similarly, if $\varphi : B \to C$ is any homomorphism then we always get the exact sequence $0 \to \ker\varphi \to B \to \mathrm{im}\varphi \to 0$.

Example 10.29. We can always form the direct sum $B = A \oplus C$ of two modules which gives rise to an obvious short exact sequence. Thus we always get at least one extension. As a special case, we can do this for $A = \mathbb{Z}$ and $\mathbb{C} = \mathbb{Z}/n\mathbb{Z}$. However, there is another extension wherein the middle term of the short exact sequence is just $\mathbb{Z}$, not $\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. The map $\mathbb{Z} \to \mathbb{Z}$ is given by $x \mapsto nx$ and $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is just the usual reduction mod n. Note that of course $\mathbb{Z} \ncong \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ even though they fit into the same short exact sequence.

Example 10.30. Let M be an R-module and S a set of generators for M. Let $F(S)$ be the free R-module on S. Then $0 \to K \xrightarrow{i} F(S) \xrightarrow{\varphi} M \to 0$ is exact where φ is the unique R-module homomorphism which is the identity on S (guaranteed to exist by the universal property) and $K = \ker\varphi$.

Definition 10.31. Let $0 \to A \to B \to C \to 0$ and $0 \to A' \to B' \to C' \to 0$ be short exact sequences. A *homomorphism of short exact sequences* is a triple a, b, c of homomorphisms $A \to A'$, $B \to B'$, and $C \to C'$ such that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

commutes. It's an isomorphism of short exact sequences if a, b, c are all isomorphisms, in which case B and B' are *isomorphic extensions*. Furthermore, the two sequences are *equivalent* if $A = A'$, $C = C'$, and a and c as above are just the identity maps. Then B and B' are *equivalent extensions*.

Example 10.32. Let $m, n > 1$ be integers and assume $n \mid m$ with $k = m/n$. We define a map between exact sequences of $\mathbb{Z}$-modules as

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \xrightarrow{\pi} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\ 0 & \longrightarrow & \mathbb{Z}/k\mathbb{Z} & \xrightarrow{i} & \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\pi'} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \end{array}$$

where a and b are the natural projections, c is the identity, $i(a \mod k) = na \mod m$, and π' projections $\mathbb{Z}/m\mathbb{Z}$ to $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. Then this is a homomorphism of short exact sequences. We could also just take the top row and map each module to itself by $x \mapsto -x$, which gives an isomorphism of this exact sequence with itself. However, it's not an equivalence since it isn't the identity on the first $\mathbb{Z}$.

Example 10.33. Consider

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\psi} & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \mathrm{id} & & \downarrow b & & \downarrow \mathrm{id} & & \\ 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\psi'} & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\varphi'} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \end{array}$$

where ψ embeds $\mathbb{Z}/2\mathbb{Z}$ into the first component while ψ' embeds into the second component and φ projects onto its second component while φ' projects onto its first component. The map b interchanges the two factors. This gives an equivalence of two exact sequences that isn't the identity isomorphism.

Example 10.34. For $i = 1, 2$ define

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\psi} \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi_i} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to 0$$

where $\psi(1) = (2, 0)$ in both sequences but $\varphi_1(a \mod 4, b \mod 2) = (a \mod 2, b \mod 2)$ and $\varphi_2(a \mod 4, b \mod 2) = (b \mod 2, a \mod 2)$. Then these are both short exact. An isomorphism between them is given by the triple $\mathrm{id}, \mathrm{id}, f$ where $f(c, d) = (d, c)$ interchanges the two factors of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. These sequences are *not equivalent*: since $\varphi_1(0, 1) = (0, 1)$, any equivalence, $\mathrm{id}, b, \mathrm{id}$ between the two sequences must map $(0, 1) \in \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ to either $(1, 0)$ or $(3, 0)$ in $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. But this is an impossible, since b can't send an order 2 element to an order 4 element.

In general, equivalences involving the same extension B are automorphisms of B that restrict to the identity on $\psi(A)$ and $B/\psi(A)$. Any automorphism of $B = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ must fix $(0, 1) + \psi(A)$ since it's the unique nonidentity coset containing order 2 elements. Thus maps sending this to different elements in C give inequivalent extensions. In fact, there's a third inequivalent extension involving all three of the same modules which sends $(0, 1) + \psi(A)$ to $(1, 1) \in \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Proposition 10.35 (Five lemma)**.** Let α, β, γ be a homomorphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

(1) If α and γ are injective then so is β
(2) If α and γ are surjective then so is β
(3) If α and γ are isomorphisms then so is β

Proof. We'll just prove (1). Let α and γ be injective and let $b \in B$ with $\beta(b) = 0$. Let $\psi : A \to B$ and $\varphi : B \to C$ be the homomorphisms in the top short exact sequence. Since $\beta(b) = 0$ it follows that the image of $\beta(b)$ in the quotient C' is 0. This $\gamma(\varphi(b)) = 0$ since the diagram commutes, and since γ is injective this means $\varphi(b) = 0$ so $b \in \ker \varphi$. Thus $b \in \mathrm{im}\psi$ since the sequence is exact, say $b = \psi(a)$ for some $a \in A$. Again by commutativity of the diagram, the image of $\alpha(a)$ in B' is the same as $\beta(\psi(a)) = \beta(b) = 0$. Since α and the map $A' \to B'$ are injective, so $a = 0$. Thus $b = \psi(a) = \psi(0) = 0$ so β is injective. ∎

For the simplest extension $B = A \oplus C$, we always have that B contains a submodule C' which is isomorphic to C, namely $C' = 0 \oplus C$. The same is true for A. This "splits" B into a direct sum. For groups, we saw that the existence of a subgroup complement C' to a normal subgroup in B implies that B is a semidirect product. That B is a direct sum in this context is a result of the fact that its underlying group is abelian—then semidirect products are just direct products.

Definition 10.36.

(1) Let R be a ring and $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ be a short exact sequence of R-modules. The sequence is *split* if there is an R-module complement to $\psi(A)$ in B. Then, up to isomorphism, we have $B = \psi(A) \oplus C' \cong A \oplus C$ (since $\psi(A) \cong A$ and we have $\varphi(C') \cong C$).
(2) Let $1 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 1$ be a short exact sequence of groups. It is *split* if there is a subgroup complement to $\psi(A)$ in B, where we now have $B = A \rtimes C$ (again, it is more accurate to say $B = \psi(A) \rtimes C'$ where $\varphi(C') \cong C$).

Proposition 10.37. The short exact sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ of R-modules is split if and only if there is an R-module homomorphism $\mu : C \to B$ such that $\varphi \circ \mu$ is the identity on C. The same holds for groups.

Proof. This follows from the definitions: if μ is given, then we define $C' = \mu(C) \subseteq B$. If C' is given, then define $\mu = \varphi^{-1} : C \cong C' \subseteq B$. ■

Definition 10.38. With the notation as above, any set map $\mu : C \to B$ with $\varphi \circ \mu = \mathrm{id}$ is a *section* of φ. If μ is a homomorphism then it's a *splitting homomorphism* for the sequence.

Note that a section of φ is just a choice of coset representatives in B for the quotient $B/\ker\varphi \cong C$. A section is a splitting homomorphism if the coset representatives forms a submodule in B, in which case we get a complement to $\psi(A)$ in B.

Example 10.39. The split short exact sequence $0 \to A \xrightarrow{i} A \oplus C \xrightarrow{\pi} C \to 0$ has the splitting homomorphism $\mu(c) = (0, c)$.

Example 10.40. The extension $0 \to \mathbb{Z} \xrightarrow{i} \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/n\mathbb{Z} \to 0$ of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$ is split, where μ is just mapping $\mathbb{Z}/n\mathbb{Z}$ isomorphically onto the second factor of the direct sum. However, the exact sequence $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$ isn't split since there is no nonzero homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$.

Proposition 10.41. Let $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ be a short exact sequence of modules. Then $B = \psi(A) \oplus C'$ for some submodule $C' \subseteq B$ with $\varphi(C') \cong C$ if and only if there is a homomorphism $\lambda : B \to A$ such that $\lambda \circ \psi$ is the identity on A.

Proof. This is similar to the above proof. If λ is given then just define $C' = \ker\lambda \subseteq B$ and if C' is given then define $\lambda : B = \psi(A) \oplus C' \to A$ by $\lambda(\psi(a), c') = a$. Note that as groups, $\ker\lambda$ is normal in B so C' is a normal complement to $\psi(A)$ in B, which means that B is the direct sum of $\psi(A)$ and C'. ■

Thus the existence of a splitting homomorphism λ on the left is actually stronger than if the sequence splits on the right: in the latter case we only get a semidirect product, while the former gives a direct product. That these are equivalent for modules is again a reflection of the fact that their underlying group structure is abelian.

10.5.1. *Modules and $Hom_R(D, -)$.* Let R be a ring with 1 and let M be an R-module which is an extension of N by L where $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is the corresponding short exact sequence. A natural question is whether the structure of L and N force anything on M. Fix and R-module D. We'll first consider whether an R-module homomorphism from D to L or N implies there is also one to M. For $f \in \mathrm{Hom}_R(D, L)$, the answer is easy: we almost have $\psi \circ f = f' \in \mathrm{Hom}_R(D, M)$. We can draw this as

$$\begin{array}{ccc} D & & \\ {\scriptstyle f}\downarrow & \searrow^{f'} & \\ L & \xrightarrow{\psi} & M \end{array}$$

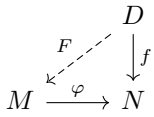
Proposition 10.42. Let D, L, M be R-modules and $\psi : L \to M$ an R-module homomorphism. Then

$$\psi' : \mathrm{Hom}_R(D, L) \to \mathrm{Hom}_R(D, M) \quad \text{given by} \quad f \mapsto f' = \psi \circ f$$

is a group homomorphism. If ψ is injective then so is ψ', i.e. if $0 \to L \xrightarrow{\psi} M$ is exact then so is $0 \to \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M)$.

Proof. That ψ' is a homomorphism is immediate. If ψ is injective, then distinct $f, g \in \mathrm{Hom}_R(D, L)$ give distinct $\psi \circ f, \psi \circ g \in \mathrm{Hom}_R(D, M)$, so ψ' is also injective. ■

This question is much harder given $f \in \mathrm{Hom}_R(D, N)$. In particular, we want to know if given such an f there exists $F \in \mathrm{Hom}_R(D, M)$ which extends f to M. As a diagram, this is given by



As before, φ induces a map $\varphi' : \mathrm{Hom}_R(D, M) \to \mathrm{Hom}_R(D, N)$ given by $F \mapsto F' = \varphi \circ F$. Then f lifts to M if and only if $f \in \mathrm{im}\varphi'$, i.e. f is the image of the lift F. In general of course this isn't possible: consider $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0$ and let $D = \mathbb{Z}/2\mathbb{Z}$ with $f : D \to N$ the identity. Then any $F : D \to M = \mathbb{Z}$ must be the zero homomorphism so $\pi \circ F$ maps D to 0 in N. Thus $\pi \circ F \neq f$. This shows that if $M \xrightarrow{\varphi} N \to 0$ is exact then $\mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N) \to 0$ is not necessarily exact!

Theorem 10.43. Let D, L, M, N be R-modules. If $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact, then $0 \to \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N)$ is exact. A homomorphism $f : D \to N$ lifts to a homomorphism $F : D \to M$ if and only if $f \in \mathrm{Hom}_R(D, N)$ is in the image of φ'. In general, φ' isn't surjective; it is surjective if and only if every homomorphism $D \to N$ lifts to $D \to M$, in which case the second sequence is short exact. Moreover, the second sequence is exact for all R-modules D if and only if $0 \to N \xrightarrow{\psi} M \xrightarrow{\varphi} N$ is exact.

Proof. The only thing we haven't proved so far is the exactness of the Hom sequence, i.e. that $\ker \varphi' = \mathrm{im}\psi'$. Let $F \in \mathrm{Hom}_R(D, M)$ be in $\ker \varphi'$, i.e. $\varphi \circ F = 0$ as a map $D \to N$. If $d \in D$ then $\varphi(F(d)) = 0$ and $F(d) \in \ker \varphi$. By exactness we have $\ker \varphi = \mathrm{im}\varphi$ so there is some $l \in L$ with $F(d) = \psi(l)$. Since ψ is injective l is unique and we get a well-defined map $F' : D \to L$ with $F'(d) = l$ which is actually a homomorphism, i.e. $F' \in \mathrm{Hom}_R(D, L)$. Since $\psi \circ F'(d) = \psi(l) = F(d)$ we have $F = \psi'(F')$, so $F \in \mathrm{im}\psi'$ and thus $\ker \varphi' \subseteq \mathrm{im}\psi'$.

Conversely, let $F \in \mathrm{im}\psi'$ so that $F = \psi'(F')$ for some $F' \in \mathrm{Hom}_R(D, L)$ and we have $\varphi(F(d)) = \varphi(\psi(F'(d)))$ for all $d \in D$. Since $\ker \varphi = \mathrm{im}\psi$ we have $\varphi \circ \psi = 0$ s o $\varphi(F(d)) = 0$ for all d. Thus $\varphi'(F) = 0$ so $F \in \ker \varphi$ and we have the reverse inclusion as desired. ∎

Thus the sequence $0 \to \mathrm{Hom}_R(D, L) \xrightarrow{\psi'} \mathrm{Hom}_R(D, M) \xrightarrow{\varphi'} \mathrm{Hom}_R(D, N) \to 0$ isn't generally short exact due to the failure of φ' beign surjective. It's exact if and only if there's a bijection $F \leftrightarrow (g, f)$ between homomorphisms $F : D \to M$ and pairs of homomorphisms $g : D \to L$ and $f : D \to N$ given by $F|_{\psi(L)} = \psi'(g)$ and $f = \varphi'(F)$. In particular, this sequence is exact when the original short exact sequence $0 \to L \to M \to N \to 0$ is split, i.e. $M = L \oplus N$. In this case, the Hom sequence is also split:

Proposition 10.44. Let D, L, N be R-modules. Then

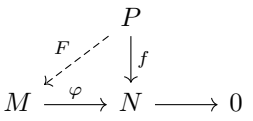
(1) $\mathrm{Hom}_R(D, L \oplus N) \cong \mathrm{Hom}_R(D, L) \oplus \mathrm{Hom}_R(D, N)$
(2) $\mathrm{Hom}_R(L \oplus N, D) \cong \mathrm{Hom}_R(L, D) \oplus \mathrm{Hom}_R(N, D)$

Proof. Let $\pi_1 : L \oplus N \to L$ and π_2 be the natural projections. Let $f \in \mathrm{Hom}_R(D, L \oplus N)$ so that $\pi_1 \circ f \in \mathrm{Hom}_R(D, L)$ and $\pi_2 \circ f \in \mathrm{Hom}_R(D, N)$. This gives a map between the LHS and RHS in (1) which is obviously a homomorphism. Conversely, given $f_1 \in \mathrm{Hom}_R(D, L)$ and $f_2 \in \mathrm{Hom}_R(D, N)$ then we define $f \in \mathrm{Hom}_R(D, L \oplus N)$ by $f(d) = (f_1(d), f_2(d))$. This gives us a map in the reverse direction which is an inverse to the first map constructed, so they are isomorphisms. The proof of (2) is the same. ∎

This extends immediately to finite direct sums. In other words, Hom commutes with finite direct sums (in either variable). This proves that for a split short exact sequence, the associated Hom sequence is also split and short exact for all R-modules D. Moreover, the converse holds.

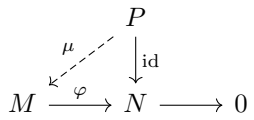
Proposition 10.45. Let P be an R-module. The following are equivalent:

(1) Let L, M, N be R-modules. If $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is short exact then the associated Hom sequence (after applying $\mathrm{Hom}_R(P, -)$ is also short exact.
(2) For any R-modules M and N, if $M \xrightarrow{\varphi} N \to 0$ is exact, then every R-module homomorphism $P \to N$ lifts to an R-module homomorphism into M, i.e. given $f \in \mathrm{Hom}_R(P, N)$ there is a lift $F \in \mathrm{Hom}_R(P, M)$ such that the following diagram commutes:



(3) If P is a quotient of an R-module M then $0 \to L \to M \to P \to 0$ splits.
(4) P is a direct summand for a free R-module.

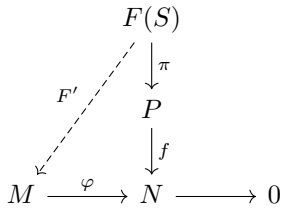
Proof. That the first two are equivalent has already been established. Assume (2) is satisfied and let $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} P \to 0$ be exact. Then the identity map on P lifts to a homomorphism μ such that



commutes, so $\varphi \circ \mu = 1$ and thus μ is a splitting homomorphism.

Every module P is the quotient of some free module so there's always an exact sequence $0 \to \ker \varphi \to F \xrightarrow{\varphi} P \to 0$ where F is a free R-module. If (3) is satisfied then this sequence splits and $F \cong \ker \varphi \oplus P$, which proves (4).

We now show that (4) implies (2). Let P be a direct summand of a free R-module on a set S, say $F(S) = P \oplus K$, and let $f : P \to N$ be a homomorphism as in the diagram in (2). Let $\pi : F(S) \to P$ be projection so $f \circ \pi : F(S) \to N$ is a homomorphism. For $s \in S$ define $n_s = f \circ \pi(s) \in N$ and let $m_s \in M$ be any element with $\varphi(m_s) = n_s$ (φ is surjective). The universal property for free modules guarantees that there is a unique R-module homomorphism $F' : F(S) \to M$ with $F'(s) = m_s$, giving the following diagram:



By definition of F' we have $\varphi \circ F'(s) = \varphi(m_s) = n_s = f \circ \pi(s)$, so $\varphi \circ F' = f \circ \pi$—the diagram is commutative. Define $F : P \to M$ by $F(d) = F'((d, 0))$. Since F is the composition of the injection $P \to F(S)$ with F', it's an R-module homomorphism. Then $\varphi \circ F(d) = \varphi \circ F'((d, 0)) = f \circ \pi((d, 0)) = f(d)$, i.e. $\varphi \circ F = f$. Thus the diagram as in (2) commutes and we are done. ■

Definition 10.46. An R-module P is *projective* if it satisfies any of the above conditions.

Corollary 10.47. Free modules are projective. A finitely generated module is projective if and only if it is a direct summand of a finitely generated free module. Every module is a quotient of a rpoject module.

In the language of abstract nonsense, this entire discussion is proving that $\mathrm{Hom}_R(D, -)$ is a covariant functor from the category of R-modules to the category of abelian groups which is left exact. It is exact if and only if D is projective.

Example 10.48. $\mathbb{Z}$ is a projective $\mathbb{Z}$-module since it is free. We can also see this directly: let $f : \mathbb{Z} \to N$ and $M \xrightarrow{\varphi} N \to 0$ be exact. Note that f is uniquely determined by $f(1) = n$. Then we can lift f to $F : \mathbb{Z} \to M$ by defining $F(1) = m$ where $\varphi(m) = n$ and then extending F to all of $\mathbb{Z}$ by additivity. Since $\mathbb{Z}$ is projective, applying Hom to an exact sequence gives an exact sequence. However, since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M) \cong M$, applying Hom gives us a sequence which is essentially the same as the one we started with.

Example 10.49. Free $\mathbb{Z}$-modules have no nonzero torsion elements so no nonzero finite abelian group can be isomorphic to a submodule of a free modules. Thus no nonzero finite abelian group is a projective $\mathbb{Z}$-module.

For example, let $n \geq 2$ be an integer and consider $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$. First we have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$. Also, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$: every homomorphism f is determined by $f(1) = a \in \mathbb{Z}/n\mathbb{Z}$ and given $a \in \mathbb{Z}/n\mathbb{Z}$ there is a unique homomorphism f_a with $f_a(1) = a$; the map $f_a \mapsto a$ is the

desired isomorphism.

Applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, -)$ to the above exact sequence yields $0 \to 0 \xrightarrow{n'} 0 \xrightarrow{\pi'} \mathbb{Z}/n\mathbb{Z} \to 0$ which is not exact at its only nonzero term. Thus $\mathbb{Z}/n\mathbb{Z}$ is not projective, since we have found a short exact sequence which is not exact on the right after applying Hom to it.

Example 10.50. Since $\mathbb{Q}/\mathbb{Z}$ is a torsion $\mathbb{Z}$-module it isn't a submodule of a free $\mathbb{Z}$-module so isn't projective. Also, the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ doesn't split since $\mathbb{Q}$ doesn't contain a submodule isomorphic to $\mathbb{Q}/\mathbb{Z}$. Even $\mathbb{Q}$ as a $\mathbb{Z}$-module is not projective.

Example 10.51. Let $R = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $P_1 = (1,0), P_2 = (0,1)$ be ideals in R. Then $R = P_1 \oplus P_2$ so then each P_i is a projective R-module. However, neither are free.

10.5.2. *Injective modules and $Hom_R(-, D)$.* We now consider homomorphisms coming out of an R-module instead of going into one. This is the "dual" problem of the above discussion. As usual, we begin with the short exact sequence $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$. First, we consider the case of a map $f \in \mathrm{Hom}_R(N, D)$. This immediately gives a map $F \in \mathrm{Hom}_R(M, D)$ just by composing with φ. This gives an injective homomorphism $\varphi' : \mathrm{Hom}_R(N, D) \to \mathrm{Hom}_R(M, D)$ defined by $f \mapsto f' = f \circ \varphi$. In other words, if $M \xrightarrow{\varphi} N \to 0$ is exact then so is $0 \to \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D)$. Now we focus our attention on if we are given $f \in \mathrm{Hom}_R(L, D)$—we want to extend it to $F \in \mathrm{Hom}_R(M, D)$, but of course this may not be possible. In other words, if $0 \to L \xrightarrow{\psi} M$ is exact then $\mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D) \to 0$ isn't necessarily exact. The extension is given by the diagram

$$\begin{array}{ccc} L & \xrightarrow{\psi} & M \\ {\scriptstyle f}\downarrow & \swarrow_{F} & \\ D & & \end{array}$$

Theorem 10.52. Let D, L, M, N be R-modules. If $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact then so is $0 \to \mathrm{Hom}_R(N, D) \xrightarrow{\varphi'} \mathrm{Hom}_R(M, D) \xrightarrow{\psi'} \mathrm{Hom}_R(L, D)$. A homomorphism $f : L \to D$ lifts to $F : M \to D$ if and only if $f \in \mathrm{Hom}_R(L, D)$ is in the image of ψ'. In general, ψ' isn't surjective; it is if and only if every homomorphism $L \to D$ can be lifted to one $M \to D$, in which case the Hom sequence is short exact. Moreover, the Hom sequence is exact for all R-modules D if and only if $L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact.

Proposition 10.53. Let Q be an R-module. The following are equivalent:

(1) If $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is a short exact sequence then so is the associated Hom sequence obtained by applying $\mathrm{Hom}_R(-, Q)$.

(2) If $0 \to L \xrightarrow{\psi} M$ is exact then every $f \in \mathrm{Hom}_R(L, Q)$ lifts to $F \in \mathrm{Hom}_R(M, Q)$, i.e. given $f \in \mathrm{Hom}_R(L, Q)$ there is a lift $F \in \mathrm{Hom}_R(M, Q)$ such that the following diagram commutes:

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \xrightarrow{\psi} & M \\ & & {\scriptstyle f}\downarrow & \swarrow_{F} & \\ & & Q & & \end{array}$$

(3) If Q is a submodule of an R-module M then Q is a direct summand of M, i.e. every short exact sequence $0 \to Q \to M \to N \to 0$ splits.

Proof. That (1) and (2) are equivalent was already done. Now assume (2) and let $0 \to Q \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ be exact. Taking $L = Q$ and letting f be the identity on Q, we get a homomorphism $F : M \to Q$ with $F \circ \psi = 1$, so F is a splitting homomorphism and we have (3). We'll skip that (3) implies (2). ∎

Definition 10.54. An R-module Q is *injective* if it satisfies any of the above conditions.

Note that applying $\mathrm{Hom}_R(-, D)$ reverses arrows while $\mathrm{Hom}_R(D, -)$ preserves them; this is to say that $\mathrm{Hom}_R(-, D)$ is a contravariant functor. By the above, it is also left exact. It is exact if and only if D is injective.

Proposition 10.55. Let Q be an R-module.

(1) Q is injective if and only if for every ideal I of R, any R-module homomorphism $g : I \to Q$ can be extended to $G : R \to Q$.
(2) If R is a PID then Q is injective if and only if $rQ = Q$ for all nonzero $r \in R$. In particular, a $\mathbb{Z}$-module is injective if and only if it is divisible. Moreover, when R is a PID then quotients of injective R-modules are injective.

Example 10.56. Since $\mathbb{Z}$ isn't divisible, it isn't an injective $\mathbb{Z}$-module. This also follows since $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ doesn't split. However, $\mathbb{Q}$ is an injective $\mathbb{Z}$-module and so is $\mathbb{Q}/\mathbb{Z}$. Moreover, since a direct sum of divisible $\mathbb{Z}$-modules is divisible, a direct sum of injective $\mathbb{Z}$-modules is injective. Thus $\mathbb{Q} \oplus \mathbb{Q}/\mathbb{Z}$ is injective.

Corollary 10.57. Every $\mathbb{Z}$-module is a submodule of an injective $\mathbb{Z}$-module.

Theorem 10.58. Let R be a ring with 1 and M an R-module. Then M is contained in an injective R-module.

10.5.3. *Flat modules and $D \otimes_R -$.* Finally, we consider the behavior of short exact sequences with respect to tensor products. Let D be an R-module. For any homomorphism $f : X \to Y$ of R-modules we can construct a homomorphism $1 \otimes f : D \otimes_R X \to D \otimes_R Y$. This is a covariant functor from the category of left R-modules to abelian groups similar to the Hom functors. One could also have constructed $- \otimes_R D$ which would be a covariant functor. However, the tensor product is covariant in both variables (unlike Hom) so we'll just work with $D \otimes_R -$.

There are already examples where $1 \otimes \psi : D \otimes_R L \to D \otimes_R M$ induced by an injective map $\psi : L \to M$ isn't injective: $\mathbb{Z} \to \mathbb{Q}$ induces the zero map $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$. On the other hand, let $\varphi \in \mathrm{Hom}_R(M, N)$ be surjective. Then $D \otimes_R N$ is generated by $d \otimes n$ for $d \in D, n \in N$. The surjectivity of φ implies that we can always write $n = \varphi(m)$ so that $1 \otimes \varphi(d \otimes m) = d \otimes \varphi(m) = d \otimes n$ shows that $1 \otimes \varphi$ is surjective as well. We thus have the following:

Theorem 10.59. Let $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ be short exact. Then $D \otimes_R L \xrightarrow{1\otimes\psi} D \otimes_R M \xrightarrow{1\otimes\varphi} D \otimes_R N \to 0$ is exact. The map $1 \otimes \psi$ isn't generally injective so we can't usually extend this to a short exact sequence. The tensored sequence is exact for all R-modules D if and only if $L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is exact.

However, if $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is short exact as well as split, then since tensor products commute with direct sums it follows that the tensored sequence (as in the above theorem) is also split and short exact.

Proposition 10.60. Let A be an R-module. The following are equivalent:

(1) If $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$ is short exact then $0 \to A \otimes_R L \xrightarrow{1\otimes\psi} A \otimes_R M \xrightarrow{1\otimes\varphi} A \otimes_R N \to 0$ is also short exact.
(2) If $0 \to L \xrightarrow{\psi} M$ is exact, i.e. ψ is injective, then $0 \to A \otimes_R L \xrightarrow{1\otimes\psi} A \otimes_R M$ is exact (so $1 \otimes \psi$ is injective).

Definition 10.61. An R-module A is *flat* if it satisfies either of the above conditions.

Corollary 10.62. Free and, more generally, projective modules are flat.

Proof. Let F be a free R-module. We want to show that if $\psi : L \to M$ is injective then $1 \otimes \psi : F \otimes_R L \to F \otimes_R M$ is injective. First assume $F \cong R^n$ is finitely generated. Then $F \otimes_R L \cong R^n \otimes_R L \cong L^n$ and $F \otimes_R M \cong M^n$. Then $1 \otimes \psi$ is the natural map $L^n \to M^n$ induced by the inclusion ψ in each component. Thus $1 \otimes \psi$ is injective, so we have the desired result.

Now let F be an arbitrary free module and let $\sum f_i \otimes l_i \in F \otimes_R L$ be mapped to 0 by $1 \otimes \psi$. Then $\sum(f_i, \psi(l_i))$ can be written in the free group on $F \times M$ as a sum of the generators that we quotient out by. This is a finite sum, so all of the first coordinates of the resulting equation line in a finitely generated free submodule F' of F. But F' is flat, so $\sum f_i \otimes l_i$ is 0 in $F' \otimes_R L$ and so also in $F \otimes_R L$. Thus $1 \otimes \psi$ is again injective and F is flat.

Now let P be projective. Then it's a direct summand of a free module F, say $F = P \oplus Q$. Let $\psi : L \to M$

be injective. Then tensoring with F gives us an injective map $1 \otimes \psi$. Since tensor products commute with direct sums, we see that

$$1 \otimes \psi : (P \otimes_R L) \oplus (Q \otimes_R L) \to (P \otimes_R M) \oplus (Q \otimes_R M)$$

is injective and so P is flat as well. ■

Example 10.63. $\mathbb{Z}$ is projective as a $\mathbb{Z}$-module so it is flat. However, $\mathbb{Z}/2\mathbb{Z}$ is not flat. Even $\mathbb{Q}$ is a flat $\mathbb{Z}$-module: let $\psi : L \to M$ be injective. Every element of $\mathbb{Q} \otimes_{\mathbb{Z}} L$ can be written $(1/d) \otimes l$. If such an element is in the kernel of $1 \otimes \psi$ then $1/d \otimes \psi(l) = 0 \in \mathbb{Q} \otimes_{\mathbb{Z}} M$. But then $c\psi(l) = 0$ for some nonzero $c \in \mathbb{Z}$. Thus $\psi(c \cdot l) = 0$ and since ψ is injective we get $c \cdot l = 0$. But then $1/d \otimes l = 1/cd \otimes c \cdot l = 0 \in L$, so $1 \otimes \psi$ is injective.

However, $\mathbb{Q}/\mathbb{Z}$ isn't flat (although it is injective): $\psi(z) = 2z$ is an injective map $\mathbb{Z} \to \mathbb{Z}$ but doesn't remain injective after tensoring with $\mathbb{Q}/\mathbb{Z}$ since $1 \otimes \psi : \mathbb{Q}/Z \otimes_{\mathbb{Z}} \mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}$ has $(1/2 + \mathbb{Z}) \otimes 1$ in its kernel, which is a nonzero element. Since $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} = \mathbb{Q}/\mathbb{Z}$, this is equivalent to the simpler statement that multiplication by 2 has $1/2$ in its kernel. Finally, since the direct sum of flat modules is flat, we see that $\mathbb{Q} \oplus \mathbb{Z}$ is flat, although it isn't projective or injective ($\mathbb{Q}$ isn't projective and $\mathbb{Z}$ isn't injective).

Theorem 10.64. $\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$

Corollary 10.65. If R is commutative then the tensor product of two projective R-modules is projective.

Proof. Let P and Q be projective modules. Then $\mathrm{Hom}_R(Q, -)$ is exact. Composing with $\mathrm{Hom}_R(P, -)$ we see that $\mathrm{Hom}_R(P, \mathrm{Hom}_R(Q, -))$ is also exact. Thus $\mathrm{Hom}_R(P \otimes_R Q, -)$ is exact so $P \otimes_R Q$ is projective. ■

11. Vector spaces

11.1. **Definitions and basic theory.**

11.2. **Matrix representation of a linear transformation.**

11.3. **Dual spaces.**

11.4. **Determinants.**

11.5. **Tensor, symmetric, and exterior algebras.**

12. Modules over a PID

12.1. **Basic theory.**

12.2. **Rational canonical form.**

12.3. **Jordan canonical form.**

13. Field theory

13.1. **Basics of field extensions.**

13.2. **Algebraic extensions.**

13.3. **Straightedge and compass constructions.**

13.4. **Splitting fields and algebraic closures.**

13.5. **Separable and inseparable extensions.**

13.6. **Cyclotomic polynomials and extensions.**

14. Galois theory

14.1. **Basic definitions.**

14.2. **Fundamental theorem of Galois theory.**

14.3. **Finite fields.**

14.4. **Composite and simple extensions.**

14.5. **Cyclotomic and abelian extensions over $\mathbb{Q}$.**

14.6. **Galois groups of polynomials.**

14.7. **Solvable and radical extensions.**

14.8. **Computing Galois groups over $\mathbb{Q}$.**

14.9. **Transcendental and inseparable extensions and infinite Galois groups.**

15. Commutative rings and algebraic geometry

15.1. **Noetherian rings and affine algebraic sets.**

15.2. **Radicals and affine varieties.**

15.3. **Integral extensions and the Nullstellensatz.**

15.4. **Localization.**

15.5. **Prime spectrum of a ring.**

16. Artinian rings, DVRs, and Dedekind domains

16.1. **Artinian rings.**

16.2. **DVRs.**

16.3. **Dedekind domains.**

17. Intro to homological algebra and group cohomology

17.1. **Ext and Tor.**

17.2. **Group cohomology.**

17.3. **Crossed homomorphisms and $H^1(G, A)$.**

17.4. **Group extensions, factor sets, and $H^2(G, A)$.**

18. Representations and character theory

18.1. **Linear actions and modules over group rings.**

18.2. **Wedderburn's theorem.**

18.3. **Character theory.**

19. Applications of character theory

19.1. **Characters of groups of small order.**

19.2. **Theorems of Burnside and Hall.**

19.3. **Induced characters.**