Algebra I

Fall 2019

---

1 Monoids & Groups

Definition. A **monoid** M is a set together with a law of composition that is (1) associative and (2) there exists $e \in M$ such that $ex = x = xe$ for all $x \in M$. In particular, $M \neq \varnothing$. A **semigroup** is a monoid that is not required to have an identity.

Proposition 1.1. The identity element is unique.

Proof. Let e, e' be two identities. Then $e = ee' = e'$. *Note: the proof shows that if one has a left and right identity in a binary algebraic system then they must be equal and hence a two-sided identity.* ■

Definition. A **submonoid** of a monoid M is a subset $S \subseteq M$ that is also a monoid under the same operation *with the same identity*.

Definition. A **group** is a set G together with a law of composition that is (1) associative (2) has a two-sided identity (3) every element has a two-sided inverse. A **subgroup** of a group G is a subset $H \subseteq G$ that is also a group under the same operation.

Examples.

- Dihedral group $D_{2n} = \langle \sigma, \tau \rangle$ where $o(\sigma) = n$ and $o(\tau) = 2$ and $\tau\sigma = \sigma^{-1}\tau$. Alternatively, we can view D_{2n} as the group of symmetries of the regular n-gon (σ are rotations about the center by $2\pi/n$ radians and τ is reflecting over an axis through a vertex and the center.)
- Quaternions $Q_8 = \langle i, j, k | i^2 = j^2 = k^2 = ijk \rangle$. Note $i^2 = -1$.
- Symmetric group S_n: Group of permutations on n letters.
- Groups of order 1: Only trivial.
- Groups of order 2, 3, 5, 7: Only $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$, resp.

- Groups of order 4: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.
- Groups of order 6: $\mathbb{Z}_6$ and $S_3 \cong D_6$.
- Groups of order 8: D_8, Q_8, $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2^3$.

Challenge: Find all subgroups of Q_8 and D_8. Which are normal?

Note. To verify $H \subseteq G$ is a subgroup we need to show (a) closure (b) closed under inverses (c) $e \in H$. However, if H is non-empty, then (c) is redundant.

Proposition 1.2. If $H \subseteq G$ is a finite, non-empty subset of a group G that is closed with respect the operation of G. Then H is a subgroup of G.

Proof. Let $a \in H$. We want to show $a^{-1} \in H$. If $a = e$, we're done. Otherwise, since H is finite and closed, we have that $a, a^2, \dots$ are in H and there exist $j > i$ such that $a^i = a^j$. Hence $a^{j-i} = e$. Since $a \neq e$, we have $j - i > 1$, so $a(a^{j-i-1}) = e$, i.e. $a^{-1} = a^{j-i-1} \in H$. ∎

Definition. Let S be a non-empty subset of a group G. Then the **subgroup generated by** S, denoted $\langle S \rangle$ is the smallest subgroup of G containing S, or equivalently, $\cap_{S \subseteq H \subseteq G} H$, or equivalently $\{s_1 \dots s_n : s_i \in S \text{ or } s_i^{-1} \in S\}$. If $S = \{x_1, \dots, x_m\}$ we write $\langle S \rangle = \langle x_1, \dots, x_m \rangle$.

1.1 Cyclic Groups

A group G is **cyclic** if there exists $a \in G$ such that $G = \langle a \rangle$.

Note. All cyclic groups of the same order are isomorphic. Let $G = \langle a \rangle$. Define $\phi : \mathbb{Z} \to G$ by $n \mapsto a^n$, then ϕ is a homomorphism and it is onto as every element of G is a power of a. If $\ker \phi$ is trivial, then $\mathbb{Z} \cong G$; otherwise, $\ker \phi = n\mathbb{Z}$ (the only ideals of $\mathbb{Z}$), so $G \cong \mathbb{Z}/n\mathbb{Z}$.

Theorem 1.3: Any subgroup H of a cyclic group $G = \langle a \rangle$ is cyclic; moreover, except in the case where both $|G| = \infty$ and H is trivial, we can write $H = \langle a^d \rangle$ with d being the smallest positive integer such that $a^d \in H$ and in that case $a^s \in H$ iff $d \mid s$.

Proof. If $|G| = \infty$ and $H = \{e\}$, we're done. Otherwise, $\exists n \in \mathbb{Z}^+$ such that $a^n \in H$. Choose d to be the smallest such integer. Then $\langle a^d \rangle \subseteq H$. Conversely, if $x \in H$ then $x = a^{qd+r}$ where $q, r \in \mathbb{Z}$, $0 \leq r < d$ since $H \subseteq G$. Now $a^d \in H$ so $a^{dq} \in H$, thus

$a^{-qd} \in H$. Hence $a^r = a^{qd+r} \cdot q^{-qd} \in H$. If $r \neq 0$, we contradict the definition of d. So $x = a^{qd}$. ∎

Corollary. The only subgroups of $\langle a \rangle$ are e and $\langle a^d \rangle$ for $d \in \mathbb{Z}^+$. In particular, the only subgroups of $\mathbb{Z}$ are 0 and $n\mathbb{Z}$.

Corollary. If $G = \langle a \rangle$ is finite and n is the smallest positive integer a such that $a^n = e$, then $a^s = e$ iff $n \mid s$. It follows $a^i = a^j$ iff $i \equiv j \bmod n$. In particular, $G = \{e, a, a^2, \ldots, a^{n-1}\}$.

Proof. Let $H = \{e\}$ with n as above. Then $a^s = e$ iff $a^s \in H$ iff $n \mid s$. ∎

We define the **order** of a, $o(a)$, to be the smallest positive integer such that $a^n = e$ or ∞ if no such integer exists. Equivalently, $o(a) = |\langle a \rangle|$.

Corollary. If $o(a) = n$ and $H = \langle a^d \rangle$ with d as in Theorem 1.3, then $d \mid n$. Moreover, $|H| = \frac{n}{d}$.

Proof. $a^n = e \in H$ implies $d \mid n$. ∎

Corollary. Let G be a finite cyclic group of order n, then G has one and only one subgroup of order d for each $d \mid n$. *****This one is the significant result.*****

Corollary. If $o(a) = n$ then $o(a^i) = n/\gcd(i, n)$, or equivalently, $\langle a^i \rangle = \langle a^{\gcd(i,n)} \rangle$.

Proof. $\langle a^i \rangle$ is the smallest subgroup of $\langle a \rangle$ containing a^i. Thus $\langle a^i \rangle = \langle a^d \rangle$ where d is the largest integer such that $d \mid i$ and $d \mid n$, which is precisely $\gcd(i, n)$. ∎

Corollary. Suppose $o(a) = n$.

a) Then $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(i, n) = \gcd(j, n)$.

b) Then $\langle a \rangle = \langle a^i \rangle$ iff $\gcd(i, n) = 1$.

c) Then $\langle a \rangle$ has $\varphi(n)$ generators.

Proposition 1.4. If G is a cyclic group of order n then G has $\varphi(d)$ elements of order for each $d \mid n$.

Theorem 1.5: Let G be a finite group of order n. The following conditions each imply G is cyclic.

a) G has one and only one subgroup of order d for each $d \mid n$.

b) G has at most one subgroup of order d for each $d \mid n$.

c) G has at most one *cyclic* subgroup of order d for each $d \mid n$.

Note that theorem (c) is the strongest result (it requires the weakest condition), so it suffices to prove G is cyclic whenever condition (c) hold. So assume G satisfies condition (c). In the case where G is abelian, by the fundamental theorem of finite abelian groups, $G \cong \mathbb{Z}_{p_1^{r_1}} \times \ldots \mathbb{Z}_{p_s^{r_s}}$. If The p_i are distinct G is cyclic, so WLOG assume $\exists i, j$ such that $p_i = p_j$. Then G contains a copy of $\mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}_{p_j^{r_j}}$. So G has more than one subgroup of order p (in particular $(0, \ldots, p^{r_i - 1}, \ldots, 0)$ and $(0, \ldots, p_{r_j - 1}, \ldots, 0)$ each generate a subgroup of order p), contradiction.

The complete proof will use the following fact: If G is a finite group of order n and $a \in G$ then $o(a) \mid n$.

Lemma. For any positive integer n, we have $n = \sum_{d \mid n} \varphi(n)$.

Proof. Let $G = (a)$ and $o(a) = n$. We know the following:

- G has one and only one subgroup of order d for each $d \mid n$. Also G has 0 subgroups of order d for $d \nmid n$.
- Each subgroup of order d is cyclic and has $\varphi(n)$ elements of order d (generators).

Combining these, G has $\varphi(d)$ elements of order d for each $d \mid n$ and 0 elements of order d for each $d \nmid n$ since every element of G has a well-defined order. So $n = |G| = \sum_{d \mid n} \varphi(n)$. ∎

Proof. Let $N(d)$ denote the number of elements of G of order d. If $d \nmid n$, then $N(d) = 0$. Otherwise, by hypothesis, G has at most 1 cyclic subgroup of order d. Thus G has at most $\varphi(d)$ elements of order d (each one would generate the same cyclic subgroup of order d). Hence $n = \sum_{d \mid n} \varphi(d) = \sum_{d \mid n} N(d)$. Since $0 \leq N(d) \leq \varphi(d)$, equality requires $N(d) = \varphi(d)$ for each $d \mid n$. Hence $N(n) = \varphi(n) \geq 1$. ∎

Corollary. Finite subgroups of the multiplicative group of a field are cyclic.

Proof. Let G be a finite subgroup of the mult. group of a field K. Recall $x^d - 1$ has at most d roots in K. If G had two cyclic subgroups of order d, $d \mid n$, then $x^d - 1$ would have at least $d + 1$ solution in K, contradiction. So we can apply theorem 1.5(c). ∎

Remarks. The following are applications of the previous corollary.

- If μ_n denotes the set of nth roots of unity in a field K, then $|\mu_n| < \infty$ and $(\mu_n, \times)$ is cyclic.
- The multiplicative group of a finite field is cyclic, in particular, $\mathbb{Z}_p^*$ is cyclic. More generally, $\mathbb{Z}_n^*$ is cyclic whenever n is a prime, a power of an odd prime, twice the power of an odd prime, or 4.

1.2 Homomorphisms

Definition. A **homomorphism** of monoids is a mapping $\phi : M \to M'$ such that (a). $\phi(ab) = \phi(a)\phi(b)$ and (b). $\phi(e_M) = e_{M'}$. ϕ is a homomorphism of groups if M, M' are groups. *For groups, it suffices to only verify condition (b).*

Remarks. Let $f : G \to G'$ be a group homomorphism.

- Then $f(e_G) = e_{G'}$ and $f(x^{-1}) = (f(x))^{-1}$ for all $x \in G$.
- Then f is an isomorphism iff there exists $g : G' \to G$ such that $f \circ g = id_{G'}$ (implying f is onto) and $g \circ f = id_G$ (implying f is one-to-one). In this case, f is a homomorphism iff g is
- If $G = \langle S \rangle$, then f is determined by its action on S.
- In general, composition of homomorphisms is a homomorphism.

Definition. An **endomorphism** of G is a homomorphism $\phi : G \to G$. If ϕ is bijective, we say ϕ is also an **automorphism**.

Definition. Fix $g \in G$. A **(right) coset** of G is $Gg = \{kg : k \in G\}$. A **(left) coset** is defined analogously.

Proposition 1.6. Let $f : G \to G'$ be a homomorphism. Let $K = \ker(f)$. Then $Kg = \{x \in G : f(x) = f(g)\}$.

Proof. Clearly, $Kg \subseteq$ RHS as if $x \in Kg$, then $x = kg$ for some $k \in K$, so $f(x) = f(kg) = f(g)$. Hence $x \in$ RHS. Conversely, if $x \in$ RHS, then $f(x) = f(g)$, so $f(xg^{-1}) = e_{G'}$, i.e. $xg^{-1} \in K$. Hence $x \in Kg$. ∎

Corollary. Let $f : G \to G'$ be a homomorphism. Then f is injective iff $K = \ker(f) = \{e\}$.

Proof. f injective iff $\{g\} = \{x \in G : f(x) = f(g)\} \forall g \in G$ iff $Kg = \{g\} \forall g \in G$ iff $K = \{e\}$. ∎

Proposition 1.7. Let G be a group with subgroups H, K such that (a). the elements of H commute with the elements of K and (b). $H \cap K = \{e\}$. Then HK is a subgroup of G and $H \times K \cong HK$ via $f : (h, k) \mapsto hk$.

Proof. By (a), we can show the map is a surjective homomorphism. So suppose $(h, k) \in \ker(f)$, i.e. $hk = e$. So $h = k^{-1}$ so $h \in K$. But $h \in H$ so $h = e$. Thus $k = e$. So f has a trivial kernel and hence is an isomorphism. ∎

Proposition 1.8. Suppose H, K are subgroups such that each is contained in the normalizer of the other, hence $hkh^{-1} \in K$ for all $h \in H$ and vice versa. (*This is always true if $H \triangleleft G$ and $K \triangleleft G$.*) Then (b) implies (a) in the previous proposition.

Proof. Let $h \in H, k \in K$. Let $x = hkh^{-1}k^{-1}$ Then $x = (hkh^{-1})k^{-1}$, so clearly $x \in K$ and $x = h(kh^{-1}k^{-1})$ so clearly $x \in H$. Hence $x = e$ implying $hk = kh$. ∎

Remark. (Application to Sylow Theory). All groups of order pq, where p, q are primes, $p > q$, $p \not\equiv 1 \bmod q$, are cyclic.

Proof. By Sylow, G has a subgroup H of order p and a subgroup K of order q. Also by Sylow, $H \triangleleft G$ and $K \triangleleft G$. Since the orders of H and K are both prime, they're both cyclic and have a trivial intersection, so HK is a subgroup of G. Since $|HK| = |H||K|/|H \cap K| = pq$, it follows $G \cong HK \cong H \times K$, but $H \times K$ is cyclic. ∎

1.2.1 Generalizations

Proposition 1.9. Suppose $H_1, \ldots, H_n$ are subgroups of G such that (a). elements of H_i commute with H_j for $i \neq j$ and (b). $H_1 H_2 \ldots H_i \cap H_{i+1} = \{e\}$ for $1 \leq i \leq n-1$. Then $H_1 H_2 \ldots H_n \cong H_1 \times \ldots \times H_N$ and $H_1 \ldots H_n$ is a subgroup of G.

Similarly, proposition 1.8., generalizes if each H_i normalizes each H_j, e.g. if each $H_i \triangleleft G$.

Finally, suppose $|G| = p_1^{e_1} \ldots p_n^{e_n}$ for distinct primes p_i and suppose the Sylow p-subgroup $S_{p_i} \triangleleft G$. Then $G = S_{p_1} \ldots S_{p_n}$ and $G \cong S_{p_1} \times \ldots \times S_{p_n}$.

1.3 Cosets

Facts.

- $b \in aH$ iff $bH = aH$.

  Proof. If $b \in aH$ then $b = ah$ for some $h \in H$. So $bH = ahH$, but clearly $ahH = aH$. Conversely, $bH = aH$ clearly implies $b \in aH$. ∎

- As a corollary, any two cosets are either equal or disjoint.

  Proof. If $c \in aH$, then $cH = aH$ and if also $c \in bH$, then $cH = bH$. ∎

- $G = \bigcup aH$, where a varies over the coset representatives of H. By the corollary above, this will be a disjoint union.
- *Special case of bullet 1: $aH = H$ iff $a \in H$.*
- $|aH| = |H|$ as $h_1, \ldots, h_n$ distinct implies $ah_1, \ldots, ah_n$ distinct.
- As a corollary of bullet 3 and 5, we have **Lagrange's theorem**: If G is a finite group, then $|G| = |H| * [G : H]$, where $[G : H]$ denote the **index** of H in G, i.e. the number of distinct H-cosets (left or right) in G. In particular, if H is a subgroup of G, then the order of H divides the order of G.
- A non-trivial group G has no non-trivial proper subgroups iff $|G|$ is a prime and in that case G is cyclic.

  Proof. Assume $|G| = p$, a prime. Let $H \subseteq G$. Then $|H| \mid |G|$, so either $|H| = 1$ or $|H| = p$. Hence G has no non-trivial proper subgroups. Conversely, assume G has no non-trivial proper subgroups. Let $a \neq e$, $a \in G$. Then $H = \langle a \rangle$ is a non-trivial subgroup of G, so $H = G$, hence G is cyclic. This implies $|G| \neq \infty$, since then G would have ∞-many subgroups. Also $|G|$ must be prime as cyclic groups have one and only one subgroup of order d for each $d \mid |G|$. Hence $|G|$ must be prime. ■

- If $|G| = n < \infty$ and $a \in G$. Then $o(a) \mid n$. Moreover, $a^n = e$.

Proposition 1.10. (Fermat's Little Theorem). If $a \in \mathbb{Z}$ and p is a prime such that $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$.

Proof. Note the p prime implies $\mathbb{Z}_p$ is a field, so $\mathbb{Z}_p^*$ is a group under $\cdot$ of order $p-1$. If $p \nmid a$, then $\overline{a} \neq \overline{0}$, so $\overline{a} \in \mathbb{Z}_p^*$, hence $\overline{a}^{p-1} = \overline{1}$. ■

Proposition 1.11. (Euler's Theorem). If $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \bmod n$.

Proof. The order of $\mathbb{Z}_n^*$ is $\varphi(n)$. ■

> **Example.** (Improving on Euler). Let $n = 35$ (so $\mathbb{Z}_{35}^*$ isn't cyclic and no element has order 34). If $\gcd(a, n) = 1$, then neither 5 or 7 divides a, so $a^4 \equiv 1 \bmod 5$ and $a^6 \equiv 1 \bmod 7$, so $a^{12} \equiv 1$ modulo 5 and 7, so $a^{12} \equiv 1 \bmod 35$.

Remark. (Converse of Lagrange). Let G be a finite group of order n. If $d \mid n$, then G has a subgroup of order d. (True if G is cyclic or abelian or nilpotent; not true in general, e.g. A_4 has no subgroup of order 6).

Proposition 1.12. If $K \subseteq H \subseteq G$, then $[G : K] = [G : H][H : K]$. In fact, if the $\{x_i\}$ form a complete set of distinct (left) coset representatives for K in H and $\{y_j\}$ form a complete set of distinct (left) coset representatives for H in G, then $\{y_j x_i\}$ form a complete set of distinct (left) coset representatives for K in G.

Proof. We're given $H = \cup_i x_i K$ and $G = \cup_j y_j H$. Hence $G = \cup_{i,j} y_j x_i K$. So $y_j x_i$ give representatives for all cosets of K in G. It remains to show their distinct. Suppose $y_j x_i K = y_{j'} x_{i'} K$, then $y_j x_i K H = y_{j'} x_{i'} K H$, so since $K \subseteq H$ and $x_i, x_{i'} \in H$, we have $y_j H = y_{j'} H$. Hence $j = j'$ by choice of the y's. So $x_i K = x_{i'} K$, which implies $i = i'$, by choice of the x's. ∎

Example. Let $G = S_n$ and $H = \{\sigma \in G : \sigma(n) = n\}$. Then $|G| = n!$ and $|H| = (n-1)!$, so $[G : H] = n$. Find a complete set of left coset reps. for H in G and describe cosets. Let $\sigma_i = (n,\ i)$ where $\sigma_n = e$. Then $\sigma_i H = \{\sigma \in G : \sigma(n) = i\}$ (clearly lhs is contained in rhs and both have same cardinality).

Let $K \subseteq H$ where $K = \{\tau \in H : \tau(n-1) = n-1\}$. Note $[H : K] = n - 1$. Find the distinct left coset reps. for K in H and for K in G. Take $\tau_j = (n-1,\ j)$.

Remark. If $x_1, \ldots, x_n$ are a complete set of left coset reps. of H in G, then $x_1^{-1}, \ldots, x_d^{-1}$ are a complete set of right coset reps. of H in G. Note: $(xH)^{-1} = Hx^{-1}$.

1.4 Normal Subgroups

Proposition 1.13. The following are equivalent:

a) Any left coset of H is also a right coset of H.

b) $aH = Ha$ for all $a \in G$.

c) $aHa^{-1} = H$ for all $a \in G$.

d) $aHa^{-1} \subseteq H$ for all $a \in G$.

Proof. Suppose (d), i.e. $aHa^{-1} \subseteq H$ for all $a \in G$. Then $a^{-1}Ha \subseteq H$ for all $a \in G$. Hence $H \subseteq aHa^{-1}$. Remaining cases are easy enough. ∎

Definition. A subgroup $H \subseteq G$ is **normal** if any of (a), (b), (c), or (d), hold.

Example. Normal subgroups of D_8: D_8, e, $\langle \sigma \rangle$, $\{\sigma^2, \tau, \sigma^2\tau, e\}$, $\{\sigma\tau, \sigma^3\tau, \sigma^2, e\}$, $\langle \sigma^2 \rangle$.

$Q_8 : Q_8, e, \langle -1 \rangle, \langle i \rangle, \langle j \rangle, \langle k \rangle$ (**all subgroups are normal!**)

Proposition 1.14. If $[G : H] = 2$, then $H \triangleleft G$.

Proof. The two left (right) cosets are H and the complement of H. ∎

Definition. $G/N = \{gN : g \in G\}$. (Not necessarily a group).

Defining multiplication of left cosets:

a) For any $S_1, S_2 \subseteq G$, define $S_1 S_2 = \{s_1 s_2 : s_1 \in S_1, s_2 \in S_2\}$. So $g_1 N g_2 N = \{g_1 n g_2 n' : n, n' \in N\}$. If N is normal in G, then $(g_1 N)(g_2 N) = g_1(N g_2)N = (g_1 g_2)N$. If fact, N is normal iff G/N is a group under the multiplication defined above.

b) Let $S \subseteq G$. Define $x \sim y$ iff $x^{-1}y \in S$. We can show $\sim$ is an equivalence relation iff S is a subgroup. Check $\overline{x} = xS$: $x \sim y$ iff $x^{-1}y \in H$ iff $y \in xH$ iff $yH = xH$. Define $\overline{x} \cdot \overline{y} = \overline{xy}$. Suppose $x \sim w$ and $y \sim z$, we need to check $xy \sim wz$. (This is true iff $S \triangleleft G$.) Note: If multiplication is well-defined, then the homomorphism in prop. 1.15, is well-defined and has kernel S. Thus $S \triangleleft G$ since kernels are always normal.

c) For right cosets, define $x \sim y$ iff xy^{-1}.

Proposition 1.15. A subgroup is normal iff it is the kernel of some group homomorphism.

Proof. Let $N \triangleleft G$ and define $\varphi : G \to G/N$ via $x \mapsto \overline{x}$. Note $\varphi(xy) = \overline{xy} = \overline{x} \cdot \overline{y} = \varphi(x)\varphi(y)$. The kernel is $\{x \in G : \overline{x} = \overline{e}\}$, i.e. $\{x \in G : xN = N\} = N$. Converse is trivial. ∎

Definition. The **normalizer of** H **in** G is $N_G(H) = \{a \in G : aHa^{-1} = H\}$. ($\neq \{a \in G : aHa^{-1} \subseteq H\}$ in the infinite case, find example).

The **centralizer of** H **in** G is $C_G(H) = \{g \in G : ghg^{-1} = h \forall h \in H\}$.

The **center** of $G = \{g \in G : gx = xg \forall x \in G\}$.

Proposition 1.16. $H \triangleleft N_G(H)$ and $N_G(H)$ is the biggest subgroup of G containing H in which H is normal. Also if K is a subgroup of $N_G(H)$, then HK is a subgroup of G (the converse does not hold).

More generally, for $S \subseteq G$, we define $N_G(S)$ and $C_G(S)$ analogously. If $S = \{a\}$, then $N_G(S) = C_G(S)$.

There is a canonical homomorphism $G/Z(G) \hookrightarrow \mathrm{Aut}(G)$. Define $\varphi : G \to \mathrm{Aut}(G)$. For any $g \in G$, define $i_g \in \mathrm{Aut}(G)$ by $i_g(x) = gxg^{-1}$ for all $x \in G$. Then the kernel of this map is $Z(G)$.

More generally, if H is a subgroup of G, then $N_G(H)/C_G(H) \hookrightarrow \mathrm{Aut}(H)$.

Theorem 1.17: 1st Isomorphism Theorem Suppose $f : G \to G'$ is a homomorphism and $K = \ker(f)$. Let $\varphi : G \twoheadrightarrow G/K$ be the canonical homomorphism from G onto G/K. Then there is a unique injective homomorphism $f^* : G/K \to G'$ making the following diagram commute:

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, two heads, "\varphi"] & G' \\ G/K \arrow[ur, hook, "f^*"'] & \end{tikzcd}$$

Proof. Define $f^*(xK) = f(x)$.

- *Well-defined*: $xK = yK$ implies $f(x) = f(y)$ as $xK = \{g \in G : f(g) = f(x)\}$ and $yK = \{g \in G : f(g) = f(y)\}$.
- *Homomorphism*: $f^*((xK)(yK)) = f^*(xyK) = f(xy) = f(x)f(y) = f^*(xK)f^*(yK)$.
- *Injective*: $f^*(xK) = e'$ iff $f(x) = e'$ iff $x \in K$ iff $xK = K$.

∎

Theorem 1.18: Suppose $H \lhd G$ and $K \lhd G$ and $K \subseteq H$. Then there exists $\varphi : G/K \to G/H$ defined by $xK \mapsto xH$ with kernel H/K. Hence $(G/K)/(H/K) \cong G/H$.

Proof. Check that if $xK = yK$, then $xH = yH$. But $xK = yK$ iff $x^{-1}y \in K$ iff $x^{-1}y \in H$ iff $xH = yH$.

It is obviously a homomorphism. It's obviously onto. The $\ker(\varphi) = \{xK : xH = e_{G/H} = H\} = \{xK : x \in H\} = H/K$. ∎

Theorem 1.19: Let G be a group and H, K be subgroups of G such that $H \subseteq N_G(K)$. Thus

a) $H \cap K \lhd H$;

b) HK is a subgroup of G;

c) $K \lhd HK$.

d) $H/(H \cap K) \cong HK/K$

The composite homomorphism $H \hookrightarrow HK \twoheadrightarrow HK/K$ is onto since $hkK = hK$ and has kernel $H \cap K$.

Theorem 1.20: Let H, K be finite subgroups of a group G, then $|HK| = |H||K|/|H \cap K|$.

Proof. Write K as a disjoint union of cosets of $H \cap K$.

$$K = \bigcup_{i=1}^{n} (H \cap K)k_i,$$

where $(H \cap K)k_i$ are disjoint. Then $n = |K|/|H \cap K|$. Also

$$HK = H\left(\bigcup_{i=1}^{n} (H \cap K)k_i\right) = \bigcup_{i=1}^{n} Hk_i.$$

We'll be done if we can show $|HK| = n|H|$, which will follow if the Hk_i are disjoint. Thus, it suffices to show the Hk_i are distinct. Suppose $Hk_i = Hk_j$, then $k_i \in Hk_j$, so $k_i k_j^{-1} \in H$. However, $k_i k_j^{-1} \in K$, so $k_i \in (H \cap K)k_j$, so $(H \cap K)k_i = (H \cap K)k_j$, so $k_i = k_j$, by the choice of coset representatives. ∎

Proposition 1.21. *Let $f : G \to G'$ be a homomorphism. Let H' be a subgroup of G' and define $H = f^{-1}(H')$. Then $H' \lhd G'$ implies $H \lhd G$. The converse holds when f onto.*

Proof. Consider the composite homomorphism $G \to G' \twoheadrightarrow G'/H'$. This has kernel $f^{-1}(H'') = H$. ∎

Theorem 1.22: Correspondence Theorem Let $f : G \to G'$ be a surjective homomorphism with kernel K. Let X be the set of subgroups of G containing K and Y be the set of subgroups of G.

a) There is a one-to-one correspondence between X and Y given by

$$\varphi : X \to Y,\ \varphi(H) = f(H) \text{ or } \psi : Y \to X,\ \psi(H') = f^{-1}(H')$$

b) Moreover, $\varphi(H) \triangleleft G'$ iff $H \triangleleft G$ and in that case, $G/H \cong G'/\varphi(H)$.

This gives a one-to-one correspondence between normal subgroups of G' and normal subgroups of G containing K. An important special case is the quotient map $G \to G/N$ for some $N \triangleleft G$.

Proof. Let X be the set of subgroups of G containing K and Y be the set of subgroups of G.

- We want to show $f^{-1}(f(H)) = H$ for any $H \in X$. Clearly, $H \subseteq f^{-1}(f(H))$. Conversely, if $x \in f^{-1}(f(H))$, then $f(x) \in f(H)$, so $f(x) = f(h)$ for some $h \in H$. Thus $xh^{-1} \in K$, but $K \subseteq H$, so $xh^{-1} \in H$. Hence $x \in H$.
- We want to show $f(f^{-1}(H')) = H'$ for all $H' \in Y$. Clearly, $f(f^{-1}(H')) \subseteq H'$. Conversely, if $y \in H'$, then since f is onto, $y = f(x)$ for some $x \in f^{-1}(H')$. Hence $y \in f(f^{-1}(H'))$.

This establishes the desired correspondence, in particular φ and ψ, are inverses of each other.

The first part of (b) is not hard to prove. Moreover, we have $G/H \cong G'/\varphi(H)$ by considering $\chi \circ f : G \to G'/\varphi(H)$, where $\chi : G' \to G'/\varphi(H)$ is the quotient map (onto since χ and f are onto and has kernel $f^{-1}(f(H)) = H$). ■

1.5 Exact Sequences

Definition. We say $G' \xrightarrow{f} G \xrightarrow{g} G''$ is an **exact sequence** if $\mathrm{Im}(f) = \ker(g)$. A longer sequence, say $\to G_{i-1} \to G_i \to G_{i+1} \to \dots$, is **exact** if it is exact at each juncture.

Special Cases

a) $0 \to G' \xrightarrow{f} G$ is exact: f is injective.

b) $G \xrightarrow{g} G'' \to 0$ is exact: g is surjective.

c) $0 \to G \xrightarrow{g} G'' \to 0$ is exact: g is bijective.

d) **Short**: $0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$ is exact: f is injective and g is surjective. Since f is injective, we can identify G' with its image $f(G')$, so we think of G' as being a subgroup of G. As such $G' = \ker(g)$. Also g is onto, so $G/\ker(g) \cong G''$, so $G/G' \cong G''$. Conversely, if $N \lhd G$, then $0 \to N \to G \to G/N \to 0$ is exact.

e) $0 \to G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} G_4 \to 0$ is exact: f_1 is injective so we can identify G_1 with its image in G_2, i.e. think of G_1 as a subgroup of G_2. f_3 is surjective. G_1 when though of as a subgroup of G_2 equals $\ker(f_2)$. $G_4 \cong G_3/\ker(f_3) \cong G_3/\operatorname{Im}(f_2)$ (this is called the **cokernel** of f_2.

$\ldots \to G_{i-1} \xrightarrow{f_i} G_i \xrightarrow{f_{i+1}} G_{i+1} \to \ldots$ is exact iff all of the $0 \to f_i(G_{i-1}) \xrightarrow{f_i} G_i \xrightarrow{f_{i+1}} f_{i+1}(G_i) \to 0$ are exact.

Proposition 1.23. If $f : G \to G'$ then $0 \to \ker f \to G \to G' \to \operatorname{coker} f \to 0$ is always exact.

1.6 Solvable Groups

Definition. Let G be a group. A sequence of subgroups $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m$ is called a **tower** of subgroups. It is called a **normal tower** if $G_{i+1} \lhd G_i$ for $1 \leq i \leq m$. It is called **abelian** (resp. **cyclic**) [ARC] if (1) it is normal (2) all of the factor groups G_i/G_{i+1} are abelian (resp. cyclic).

A **refinement** of a (normal) tower $G_0 \rhd G_1 \rhd \ldots \rhd G_m$ is a tower gotten by inserting a finite number of subgroups into the given tower so that is remains normal.

Proposition 1.24. Refinements of ARC towers are ARC.

Proof. Suppose $G_i \rhd G_{i+1}$ and we refine it to $G_i \rhd K \rhd G_{i+1}$, where G_i/G_{i+1} is ARC. We want to show G_i/K and K/G_{i+1} are ARC. We know $G_i/K \cong (G_i/G_{i+1})/(K/G_{i+1})$. So G_i/G_{i+1} ARC implies G_i/K is ARC.

Similarly, $K \hookrightarrow G_i \twoheadrightarrow G_i/G_{i+1}$ and the compositum φ, has kernel $K \cap G_{i+1} = G_{i+1}$, so $K/G_{i+1} \hookrightarrow G_i/G_{i+1}$. So G_i/G_{i+1} ARC implies K/G_{i+1} ARC (subgroups of ARC groups are ARC). ∎

Definition. A group G is **solvable** if it has an abelian tower that ends in e.

Example. Take $G = D_{2n}$. Then $G \rhd \langle\sigma\rangle \rhd e$ where $G/\langle\sigma\rangle \cong C_2$ and $\langle\sigma\rangle/e \cong C_n$. So G is solvable.

All abelian groups, nilpotent groups, and finite p-groups are solvable. Feit-Thompson theorem, says all groups of odd order are solvable. All simple, non-abelian groups are not solvable.

Definition. A non-repetitive normal tower is called a **composition series** if it admits no non-trivial refinements.

$G_0 \rhd \ldots \rhd G_m$ is a composition series iff each G_{i+1} is a maximal proper normal subgroup of G_i. Equivalently, the only normal subgroups of G_i containing G_{i+1} are G_i or G_{i+1}. Equivalently, if G_i/G_{i+1} is simple (since then G_i has only two normal subgroups containing G_i by correspondence between subgroups of G_i containing G_{i+1} and subgroups of G_i/G_{i+1}).

Proposition 1.25. Any non-repetitive normal tower, $G = G_0 \rhd \ldots \rhd G_m = \{e\}$ for a finite group G, can be refined to get a composition series. (b/c only finitely-many subgroups)

Corollary. A finite group is solvable iff it has a cyclic tower ending in e where each G_i/G_{i+1} has prime order.

Proof. Reverse is trivial. Conversely, suppose G is solvable and admits some abelian tower ending in e. Refine this tower to get a composition series, $G = G_0 \rhd \ldots \rhd G_m = \{e\}$ is a normal tower. This composition series will still be abelian (proposition 1.22). Moreover, each G_i/G_{i+1} will be simple. The only simple abelian groups are cyclic of prime order (only two normal subgroups, abelian implies all subgroups normal, so only two subgroups, see theorem 1.5(b) to get cyclic, then prime order is obvious). ∎

Example. $G = S_3 \times C_5$. Then $G \rhd C_3 \times C_5 \rhd e \times C_5 \rhd e \times e$ is a cyclic tower.

Definition. We say two normal towers $G = G_0 \rhd \ldots \rhd G_s = \{e\}$ and $G = H_0 \rhd \ldots \rhd H_r = \{e\}$ are **equivalent** if $r = s$ and and if there exists a permutation σ such that $G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}$.

Theorem 1.26: Jordan-Holder Let G be a finite group, then any two composition series for G are equivalent.

Proof. Proceed by induction on $n = |G|$. If $G = \{e\}$, the claim is obvious. Suppose the claim holds for all groups of order $k \leq n$. Let G be a group of order $n + 1$.

Let $G = G_0 \triangleright \ldots \triangleright G_s = \{e\}$ and $G = H_0 \triangleright \ldots \triangleright H_r = \{e\}$ be two composition series for G.

a) Case 1: If $H_1 = G_1$, then by induction on $G_1 \triangleright \ldots \triangleright G_s = \{e\}$ and $H_1 \triangleright \ldots \triangleright H_r = \{e\}$, we have $s = r$ and the factor groups are isomorphic (up to some permutation). Also $G_0/G_1 = H_0/H_1$. Combining, we get the original composition series were equivalent.

b) Case 2: If $H_1 \neq G_1$, then $G_1 \triangleleft G_0 = G$ and $H_1 \triangleleft H_0 = G$, so $G_1H_1 \triangleleft G$ and also G_1H_1 is strictly bigger than both G_1 and H_1 (since neither is contained in the other), but G_1, H_1, were maximal proper normal subgroups of G, so necessarily $G = G_1H_1$. So $G_0/G_1 = (G_1H_1)/G_1 \cong H_1/(H_1 \cap G_1)$. Also $H_0/H_1 = (G_1H_1)/H_1 \cong G_1/(H_1 \cap G_1)$. Let $K_2 = H_1 \cap G_1$. Thus

$$G_0/G_1 \cong H_1/K_2$$

and

$$H_0/H_1 \cong G_1/K_2.$$

Recall that H_0/H_1 and G_0/G_1 are both simple, hence H_1/K_2 and G_1/K_2 are also both simple. So K_2 is maximal normal in both H_1 and G_1.

Let $K_2 \triangleright K_3 \triangleright \ldots \triangleright K_u = \{e\}$ be any composition series for K_2. Then this implies that

$$G_0 \triangleright G_1 \triangleright K_2 \triangleright K_3 \triangleright \ldots \triangleright K_u = \{e\} \tag{1.1}$$

and

$$H_0 \triangleright H_1 \triangleright K_2 \triangleright K_3 \triangleright \ldots \triangleright K_u = \{e\} \tag{1.2}$$

are two composition series for G because K_2 is maximal normal in H_1 and G_1. Moreover, since $G_0/G_1 \cong H_1/K_2$ and $H_0/H_1 \cong G_1/K_2$, it's clear that the two towers are equivalent.

We have that (1.1) equals the original G_0 series by case 1. Similarly, (1.2) is equivalent to the original H_0 series.

∎

Proposition 1.27. If H is a subgroup of G and G is solvable, then H is solvable.

Proof. Let $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_n = \{e\}$ be an abelian tower. Define $H_i = H \cap G_i$.

- *Show* $H_{i+1} \triangleleft H_i$. The mapping $H_i = H \cap G_i \hookrightarrow G_i \to G_i/G_{i+1}$ has kernel $(H \cap G_i) \cap G_{i+1} = H \cap G_{i+1} = H_{i+1}$.

- H_i/H_{i+1} *is abelian.* Let $\varphi : G_i \to G_i/G_{i+1}$ be the quotient homomorphism. Let ρ be the restriction of φ to H_i. Then $\ker \rho = H_i \cap G_{i+1} = H_{i+1}$. Hence H_i/H_{i+1} is isomorphic to a subgroup of G_i/G_{i+1}, which is abelian.

■

Proposition 1.28. If $N \triangleleft G$ then G is solvable iff G/N and N are solvable.

Proof. Suppose G is solvable and $G = G_0 \triangleright \ldots \triangleright G_n = \{e\}$ is an abelian tower. By prop. 1.25, N is solvable.

Now note that $(G/N)^c = G^c N/N$, since $N \triangleleft G$ implies $aNbNa^{-1}Nb^{-1}N = [a,b]N$ for all $a, b \in G$. Thus by induction, it follows that $(G/N)^{(i)} = G^{(i)}N/N$ for $i \geq 0$. Therefore, since G solvable implies $G^{(r)} = e$ for some $r \geq 0$, it follows $(G/N)^{(r)} = eN/N = e$. So G/N is solvable.

Conversely, suppose N and G/N are solvable. Let $\{e\} = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_n = N$ and $\{e\} \triangleleft H_0 \triangleleft \ldots \triangleleft H_m = G/N$ be two abelian towers. Let $\varphi : G \to G/N$ be the quotient map. I claim

$$\{e\} = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_n = N = \varphi^{-1}(H_0) \triangleleft \ldots \triangleleft \varphi^{-1}(H_m) = G \tag{1.3}$$

is an abelian tower for G. Consider the surjective homomorphism $\varphi^{-1}(H_{i+1}) \to H_{i+1}/H_i$. This has kernel $\varphi^{-1}(H_i)$, so $\varphi^{-1}(J_i)$ is normal in $\varphi^{-1}(J_{i+1})$ and by the first isomorphism theorem $\varphi^{-1}(J_{i+1})/\varphi^{-1}(J_i) \cong J_{i+1}/J_i$ which is abelian.

■

Definition. For $x, y \in G$, we define the **commutator** of x and y to be $xyx^{-1}y^{-1}$. The **commutator subgroup** of G, G^c, is the subgroup of G generated by the commutators of G.

Proposition 1.29.

a) Any subgroup containing G^c is a normal subgroup of G. In particular, G^c is a normal subgroup of G.

b) If $N \triangleleft G$ then G/N is abelian iff $G^c \subseteq N$.

Proof. Suppose $G^c \subseteq H \subseteq G$. We want to show if $h \in H$, then $ghg^{-1} \in H$ for all $g \in G$. Note $[g, h] = ghg^{-1}h^{-1} \in H$ and $h \in H$ so there product is also.

G/N abelian iff $\overline{xy} = \overline{yx}$ for all $\overline{x}, \overline{y} \in G/N$ iff $\overline{xyx^{-1}y^{-1}} = \overline{e}$ for all $x, y \in G$ iff $[x, y] \in N$ for all $x, y \in G$ iff $G^c \subseteq N$. ■

Proposition 1.30. $N \lhd G$ implies $N^c \lhd G$.

Definition. Define $G^{(0)} = G$ and for $i \geq 1$, define $G^{(i)} = [G^{(i-1)}]^c$. Note $G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \dots$ is an abelian tower (by prop. 1.28) and for each $n \geq 0$, $G^{(n)} \lhd G$ (by prop. 1.29).

Proposition 1.31. G is solvable iff $G^{(s)} = \{e\}$ for some s.

Proof. ($\Leftarrow$). We have $G = G^{(0)} \rhd \dots \rhd G^{(s)} = \{e\}$ is an abelian tower.

($\Rightarrow$). Suppose G is solvable and $G = G_0 \rhd \dots \rhd G_n = \{e\}$ is an abelian tower. Then by prop. 1.26, G_i/G_{i+1} is abelian, so $G_{i+1} \supseteq G_i^c$.

Note $G_1 \supseteq G_0^c = G^c = G^{(1)}$.

This implies, $G_2 \supseteq G_1^c \supseteq (G^{(1)})^c = G^{(2)}$. By induction, we can show for $i \geq 2$, $G_i \supseteq G^{(i)}$. Therefore, $\{e\} = G_n \subseteq G^{(n)}$ and the claim follows. ∎

Corollary. If G is solvable then there exists an abelian tower $G = G_0 \rhd \dots \rhd G_n = \{e\}$ where each G_i is normal in G.

> **Example.** Does the above corollary hold if the word abelian is replaced with the word cyclic? (Ans. NO)

1.7 Group Action

Definition. We say a group G **acts** on a set S (from the left) if for all $g \in G$ and all $s \in S$, we have an element $gs \in S$ (that is a mapping $G \times S \to S$) satisfying

a) $g(hs) = (gh)s$ for all $g, h \in G$ and $s \in S$

b) $es = s$ for all $s \in S$.

Equivalently, a group action G on H is a homomorphism $\star : G \to \text{Aut}(S)$.

a) $\Rightarrow$. Define $\star : G \to M(S) = \{f : S \to S\}$ by $g \mapsto f_g : S \to S$ where $f_g(s) = gs$. We want to show $f_{gh} = f_g \circ f_h$. Well, $f_{gh}(s) = (gh)(s) = g(hs) = f_g(hs) = f_g(f_h(s))$. Also, $f_e(s) = es = s$, so $f_e \equiv id_S$. Thus $\star$ is a monoid homomorphism. It suffices to show $\text{Im}(\star) \subset \text{Aut}(S)$. But $f_g \circ f_{g^{-1}} = f_{gg^{-1}} = f_e$, so each f_g is invertible.

b) $\Leftarrow$. We have that $\star$ is a homomorphism. Define $gs = f_g(s)$. We require $g(hs) = (gh)(s)$, but $f_g(f_h(s)) = (f_g \circ f_h)(s) = f_{gh} = (gh)(s)$, since $\star$ is a homomorphism. Also $es = f_e(s) = s$

Example.

- Let G acts on $S = G$ by conjugation. For $g \in G$, $f_g : G \to G$ by $g \cdot x = f_g(x) = gxg^{-1}$.
- $S = \mathcal{P}(G)$. If $A \subseteq G$, then $f_g(A) = gAg^{-1}$.
- $S = G$. $T_g : G \to G$ by $g \cdot x = T_g(x) = gx$.
- $S = \mathcal{P}(G)$. $T_g = gA$.
- G is a group and H is a subgroup and $S = G/H$. G acts on S by $g \mapsto T_g$ where $T_g(xH) = gxH$. This defines a homomorphism $\star : G \to \mathrm{Perm}(G/H)$. See proposition 1.31 for discussion about the kernel of $\star$.

Proposition 1.32. Let $K = \bigcap_{x \in G} xHx^{-1}$. Then $K \lhd G$ and $K \subseteq H$ and if N is any normal subgroup of G contained in H, then $N \subseteq K$.

Proof. $N \subseteq H$ implies $xNx^{-1} \subseteq xHx^{-1}$ for all $x \in G$. But $N \lhd G$ so $N = xNx^{-1}$. Therefore, $N \subseteq xHx^{-1}$ for all $x \in G$. Thus $N \subseteq \bigcap_{x \in G} xHx^{-1} = K$. ∎

Corollary. If H is a proper subgroup of G of index d such that H does not contain any nontrivial normal subgroups of G. Then $|G| \mid d!$.

Proof. By above we have a homomorphism $\star$ whose kernel $K = \cap_{x \in G} xHx^{-1}$ is normal in G and contained in G. So K is trivial. So G is isomorphic to a subgroup of $\mathrm{Perm}(G/H)$ and $|\mathrm{Perm}(G/H)| = d!$. ∎

Corollary. Let $d > 1$. If $|G| \nmid d!$, then any subgroup H of G of index d must contain a nontrivial normal subgroup of G.

Definition.

- Let S and S' both be G-sets. Then a map $f : S \to S'$ is a **G-map** (or a **morphism of G-sets**) if $f(gs) = gf(s)$. If f is a bijection, then it's called an **equivalence of actions**.
- If G acts on S and $s \in S$, then the **stabilizer** of s (also called the **isotopy subgroup** of s) is defined to be $G_s = \{g \in G : gs = s\}$.

Example. Let S be the set of subgroups of G and let G act on S by conjugation. Suppose $H \in S$, then $G_H = N_G(H)$.

Let $S = G$ and G acts on S by conjugation. Let $x \in S$. Then $G_x = C_G(\{x\})$.

Proposition 1.33. Suppose G acts on S and $s, s' \in S$ where $s' = gs$ for some $g \in G$ (also $s = g^{-1}s$). Then $G_{s'} = gG_sg^{-1}$.

Proof. Clearly, $gG_sg^{-1} \in G_{s'}$. Conversely, $g^{-1}G_{s'}g \subseteq G_s$. ∎

Definition.

- Let G act on S and $K = \ker(\star)$ where $\star : G \to \mathrm{Perm}(S)$. We say G acts **faithfully** if K is trivial.

  Note if S is a G-set it is also a G/K set. In fact, it is a G/N-set for any $N \triangleleft G$ such that $N \subseteq K$ where we define $\overline{g}s = gs$.

- Suppose G acts on S. A **fixed point** of G is some $s \in S$ such that $gs = s$ for all $g \in G$. The **orbit** of $s \in S$ under the action of G is $\{gs : g \in G\}$.

Proposition 1.34. Define a relation on S by $s \sim r$ iff s is in the orbit of r. Then $\sim$ is an equivalence relation. The equivalence classes of s is the orbit of s, so S can be written as a disjoint union of orbits.

Definition. We say G acts **transitively** on S if for all $s, s' \in S$, there is some $g \in G$ such that $s' = gs$. Equivalently, G acts transitively on S if there is only one orbit for S under the action of G.

Proposition 1.35. Let S be a G set and $s \in S$. Then $|[s]| = [G : G_s]$.

Proof. Suffices to give a bijection between $[s]$ and the set G/G_s. Define $\varphi : G/G_s \to [s]$ by $gG_s \mapsto gs$.

It's obviously onto. For well-defined, suppose $g_1G_s = g_2G_s$, then $g_2 = g_1h$ for some $h \in G_s$. Then $g_2s = g_1hs = g_1s$. Suppose $g_1s = g_2s$, then $g_2^{-1}g_1s = s$. So $g_2^{-1}g_1 \in G_s$, i.e. $g_1 \in g_2G_s$, i.e. $g_1G_s = g_2G_s$. ∎

Proposition 1.36. Suppose S is a G-set and let $s_i \in S$, $1 \leq i \leq n$ be the distinct orbit representatives. Then

$$\begin{aligned} |S| &= \sum_i |[s_i]| = \sum_i [G : G_{s_i}] \\ &= \#\text{Fixed points} + \sum_{i : G_{s_i} \neq G} [G : G_{s_i}]. \end{aligned} \tag{1.4}$$

The class equation is the special case where G acts on itself. This says $|G| = |Z(G)| + \sum_{C_G(x) \neq G} [G : C_G(x)]$, where the x's are distinct orbit representatives.

1.7.1 Symmetric Group

Definition. Let $J_n = \{1, \ldots, n\}$ and $S_n = \mathrm{Perm}(J_n)$.

If $\sigma = (i_1 \, \ldots \, i_r) \in S_n$ is an r-cycle then the orbit i_1 under $G = \langle \sigma \rangle$ is $\{i_1, \ldots, i_r\}$ and σ fixes $J_n - \{i_1, \ldots, i_r\}$. Moreover, the orbit of $j \in J_n - \{i_1, \ldots, i_r\}$ is $\{j\}$.

We know J_n can be written as a disjoint union of its orbits under $\langle \sigma \rangle$ and σ acts as a cycle on each of these orbits (the elements of the cycle are the elements of the orbit). One can deduce from this that any element $\sigma \in S_n$ can be written as a product of disjoint cycles.

Proposition 1.37. If n is a prime, $S_n = \langle \sigma, \tau \rangle$, where σ is any n-cycle and τ is any 2-cycle (transposition). More generally, for $n \in \mathbb{Z}^+$, $S_n = \langle \sigma, \tau \rangle$ where $\sigma = (1\,2\,\ldots\,n)$ and $\tau = (a\,b)$ where $|a - b|$ is relatively prime to n.

Proposition 1.38. Any $\sigma \in S_n$ can be written as a product of transpositions.

Proof. Suffices to show any cycle can be written as a product of transpositions. Moreover,

$$(i_1 \, \ldots \, i_r) = (i_1 \, i_r)(i_1 \, i_{r-1}) \ldots (i_1 \, i_2).$$

∎

Definition. We call a permutation **even** if we can write it as a product of an even number of transpositions; otherwise, we call it **odd**.

Proposition 1.39. There exists a unique homomorphism $\epsilon : S_n \to \{\pm 1\}$ such that if τ is any transposition, $\epsilon(\tau) = -1$.

Proof. For any $A \in M_{n \times n}(\mathbb{R})$ and any $\sigma \in S_n$, define $\sigma(A)$ to be the matrix obtained by starting with A and rearranging the rows according to σ. Define ϵ by $\epsilon(\sigma) = \det(\sigma(I))$. Clearly, ϵ is a homomorphism and if τ is a transposition, then $\epsilon(\tau) = -1$. ∎

Corollary. No permutation can be both even and odd.

Definition. The kernel of the ϵ homomorphism is A_n, **the alternating group** of even permutations. Thus $A_n \lhd S_n$ and $[S_n : A_n] = 2$.

Proposition 1.40.

- S_n is not solvable if $n \geq 5$.

- A_n is simple if $n \geq 5$. (Note this implies the 1st fact).

Lemma. Suppose N, H are subgroups of S_n, $n \geq 5$ such that $N \triangleleft H$, H/N is abelian and H contains all 3-cycles. Then N also contains all 3-cycles.

Proof. Since $N \triangleleft H$ and H/N is abelian, this implies $H^c \subseteq N$. Since H contains the 3-cycles, N contains the commutators of any two 3-cycles. In particular, if $\{i, j, k, r, s\} \in J_n$ and are distinct, let $\sigma = (i\,j\,k)$ and $\tau = (k\,r\,s)$, then $[\sigma, \tau] = (r\,k\,i) \in N$. ∎

Proof of fact 1. Suppose S_n were solvable. Then $S_n \triangleright N_1 \triangleright \ldots \triangleright N_r = \{e\}$ is an abelian tower, so the lemma implies each N_i contains all 3-cycles, a contradiction. □

A_n is generated by the 3-cycles, i.e. any even permutation equals the product of 3-cycles. It suffices to show any product of 2 transpositions is the product of 3-cycles.

- Case 1. Two letters in common between transpositions. $(r\,s)(r\,s) = e$.
- Case 2. One letter in common. $(r\,s)(s\,t) = (r\,s\,t)$.
- Case 3. Zero in common. $(i\,j)(r\,s) = (i\,j\,r)(j\,r\,s)$. □

All 3-cycles are conjugate in S_n: $\gamma(i_1\,\ldots\,i_r)\gamma^{-1} = (\gamma(i_1)\,\ldots\,\gamma(i_r))$.

All 3-cycles are conjugate in A_n, $n \geq 5$: By the previous statement $(i'\,j'\,k') = \gamma(i\,j\,k)\gamma^{-1}$. If $\gamma \in A_n$, we're done. Otherwise, there exist distinct elements $r, s \in J_n$ not equal to i, j, k. Then replace γ by $\gamma(r\,s)$ which is in A_n. □

Proof of fact 2. Assume $N \triangleleft A_n$ and $N \neq \{e\}$. We want to show $N = A_n$. It suffices to show N contains a 3-cycle since $N \triangleleft A_n$ and all 3-cycles are conjugate and A_n is generated by 3-cycles. Choose $\sigma \in N$ such that $\sigma \neq e$ and σ has the maximum number of fixed points. Write J_n as a disjoint union of orbits under $\langle\sigma\rangle$. Since $\sigma \neq e$, at least one orbit has length > 1.

- Case 1. All orbits have length ≤ 2: Then $\sigma = (r\,s)(i\,j)\gamma$ for distinct r, s, i, j and γ is the product of some other disjoint transpositions or e. Choose $k \in J_n$ distinct from r, s, i, j (as $n \geq 5$). Let $\tau = (r\,s\,k)$ and $\sigma' = [\tau, \sigma] = (\tau\sigma\tau^{-1})\sigma^{-1} \in N$. Clearly, σ' fixes i, j. So σ' fixes at least 2 elements of $\{i, j, k, r, s\}$, whereas σ fixes at most 1. Moreover, if $x \in J_n - \{i, j, k, r, s\}$ then σ fixes x implies σ' does. Note $\sigma' \neq e$, since $\sigma'(k) = r$. Contradiction.
- Case 2. Some order has length ≥ 3. We're done if σ is a 3-cycle, so assume it isn't. Then $\sigma = (i\,j\,k\,\ldots)$(other disjoint stuff). Then σ must move at least one other element of J_n, else σ is a 3-cycle. But this implies it must move at

least 2 other elements, as otherwise σ would be a 4-cycle. So σ moves at least 5 elements, i, j, k, r, s. Then $\tau = (r\, s\, k)$ and $\sigma' = [\tau, \sigma] \in N$. Note σ' fixes j but σ doesn't by and any elements fixed σ is not one of i, j, k, r, s, so its also fixed by τ. Hence they're all fixed by σ'. So σ' has more fixed points, a contradiction. □

2 Sylow Theory

Definition. G has **exponent** n if $x^n = e$ for all $x \in G$.

Theorem 2.1: Cauchy If G is a finite abelian group and p is a prime dividing $|G|$, then G has an element of order p.

Proof. Suppose G has exponent n.

- *$|G|$ divides a power of n.* Proceed by induction of the order of G. Suppose $|G| > 1$. Take $b \neq e, b \in G$. Let $H = \langle b \rangle \triangleleft G$, as G is abelian. Then G/H has exponent n and $|G/H| < |G|$, thus $|G/H|$ divides a power of n, by induction. However $b^n = e$, so $o(b) = |H|$ divides n. However, $|G| = [G : H]|H|$, so the claim follows.
- *If $p \mid |G|$, p prime, then there exists $a \in G$ such that $p \mid o(a)$.* Suppose not. Then for all $a \in G$, $p \nmid o(a)$. Let $\ell = \prod_{a \in G} o(a)$, then $p \nmid \ell$. But ℓ is an exponent of G. Thus $|G| \mid \ell^k$ for some k by step 1. Therefore $p \mid \ell^k$, a contradiction.
- Thus $o(a) = pd$, for some $a \in G$ and $d \in \mathbb{Z}$. Then $o(a^d) = \frac{pd}{\gcd(pd,d)} = p$.

■

Definition. Let p be a prime dividing $|G|$. A **Sylow p-subgroup** of G is a subgroup of G whose order is the maximal power of p dividing G. Equivalently, $H \leq G$ is a p-group whose index in G is not divisible by p.

Theorem 2.2: Sylow I If $p \mid |G|$, then G has at least one p-Sylow subgroup.

Proof. Induct on $n = |G|$. Base case: $|G| = p$ then G is cyclic and hence it has an element of order p.

Suppose $|G| = p^r s$ where $p \nmid s$.

- Case 1: There exists a subgroup H such that $p \nmid [G : H]$. Then $|H| = p^r s'$ where $s' < s$. Apply induction to get a p-Sylow subgroup for H.
- Case 2: There is no such subgroup, i.e. every subgroup has index divisible by p. Choose conjugacy class representatives x:

$$|G| = |Z(G)| + \sum_{x : G \neq G_x} [G : G_x]$$

By assumption, this implies $p \mid |Z(G)|$, so the center of G is nontrivial. So there exists $a \in Z(G)$ such that $o(a) = p$. Let $H = \langle a \rangle$. Then $H \triangleleft G$ since $H \subseteq Z(G)$. Let $f : G \to G/H = \overline{G}$. Then $|G/H| = |G|/|H| = p^{r-1}s$. By induction, there is $\overline{K} \subseteq \overline{G}$, such that $|\overline{K}| = p^{r-1}$. Let $K = f^{-1}(\overline{K})$. Then $\ker(f) = H \subseteq K$. Since $\overline{K} = K/H$, we have $|\overline{K}| = |K|/|H|$. Thus $|K| = p^r$.

∎

Lemma. Let H be a p-subgroup acting on a set S. Let F be the number of fixed points of the action. Then

a) $F \equiv |S| \bmod p$.

b) If H has exactly one fixed point, then $|S| \equiv 1 \bmod p$.

c) If $p \mid |S|$, then $F \equiv 0 \bmod p$. In particular, if H has at least one fixed point, it has at least p fixed points.

d) If $p \nmid |S|$, then there is at least one fixed point.

Proof. Observe (b), (c), and (d) are immediate consequences of (a). Moreover, by choosing orbit representatives s_i such that $H_{s_i} \neq H$, we have

$$|S| = F + \sum_i [H : H_{s_i}].$$

Since $[H : H_{s_i}]$ divides $p^r = |H|$, so the claim follows by reducing modulo p. ∎

Theorem 2.3: Sylow II & III Let G be a finite group and p a prime dividing $|G|$. Then

a) If H is a p-subgroup of G, then H is contained in some Sylow p-subgroup.

b) All Sylow p-subgroups are conjugate in G.

c) The number of Sylow p-subgroups divides $|G|$ and is congruent to 1 mod p.

Proof. Let $|G| = p^r m$ where $p \nmid m$. Let H be a p-subgroup of G and let Q be p-Sylow.

- *If $H \subseteq N_G(Q)$, then $H \subseteq Q$.*

  We have HQ is a group and $|HQ| = \frac{|H||Q|}{|H \cap Q|}$. So since $H, Q, H \cap Q$ are all p-groups, so is HQ. But $Q \subseteq HQ$, so it follows $|H| = |H \cap Q|$, i.e. $H = H \cap Q$.

- *There is some Sylow subgroup P with $H \subseteq N_G(P)$.*

  Let S be the set of G-conjugates of Q. Let G act on S by conjugation. By the class equation, $|S| = [G : N_G(Q)]$. Then $[G : Q] = [G : N_G(Q)][N_G(Q) : Q]$, so since $p \nmid [G : Q]$ (as Q is Sylow), we have $p \nmid [G : N_G(Q)]$. Hence, by the lemma, the action on H on S has at least 1 fixed point, say $P = gQg^{-1}$, $g \in G$. Then $H \subseteq N_G(P)$ since for any $x \in H$, we have $xPx^{-1} = P$.

Part (a) follows. Let R be p-Sylow.

- *Show Q & R are conjugates.* By bullet 2, $R \subseteq N_G(P)$ for some conjugate $P = gQg^{-1}$ of Q. So by bullet 1, $R \subseteq P$. Since $|R| = |P|$, we have $R = P = gQg^{-1}$.

- Recall $|S| = [G : N_G(Q)]$, so it divides $|G|$. We've already shown $|S| \not\equiv 0 \bmod p$, so there is at least one fixed point, $F \in S$, of the action of Q on S. Then $Q \subseteq N_G(F)$, so $Q \subseteq F$, so $Q = F$. Hence F is unique, i.e. $|S| \equiv 1 \mod p$.

∎

Corollary. If H is the only subgroup of order d, then $H \triangleleft G$. Conversely, if H is a normal Sylow subgroup, it is the unique subgroup of that order. *Proof.* Conjugation.

Corollary. If $|G| = pq$, for prime $p < q$ with $q \not\equiv 1 \bmod p$, then G is cyclic. (e.g. $|G| = 77$)

Proof. Let K be a Sylow p-subgroup and H a Sylow q-subgroup. Let $\text{Sylow}_p(G)$ be the number of Sylow p-subgroups in G. Then $\text{Sylow}_p(G) \mid pq$ and is $\equiv 1 \bmod p$. So $\text{Sylow}_p(G) = 1$. Similarly, $\text{Sylow}_q(G) = 1$.

- Thus G has at most 1 subgroup of order d for each $d \mid |G|$, i.e. G is cyclic.

- Since $K, H \triangleleft G$ (unique subgroup of given order) and $K \cap H = \{e\}$ (rel. prime orders), we have $G = HK \cong H \times K$, which is cyclic since H, K are cyclic of rel. prime order.

- Since $H \triangleleft G$ and $|G/H| = p$ (so G/H is abelian), we have $G^c \subseteq H$. Similarly, $G^c \subset K$. Thus $|G^c|$ divides both p and q, so $|G^c| = 1$; hence, G is abelian. Since K, H are cyclic and their generators have relatively prime order (and G is abelian), the product of their generators has order pq.

■

Proposition 2.4. If $p < q$ and $q \equiv 1 \bmod p$, then there are exactly 2 nonisomorphic groups of order pq. One is cyclic and the other is a nonabelian group equal to $\langle c, d \rangle$ where $o(c) = p$ and $o(d) = q$ and $cd = d^s c$ for some $s^p \equiv 1 \bmod q$ with $s \not\equiv 1 \bmod q$.

Proof. By Sylow, we have $n_q = 1$ and $n_p \in \{1, q\}$. If $n_p = 1$, G is cyclic by the last corollary. So assume WLOG that $n_p = q$. Let C_q be the Sylow q-subgroup of G. Pick one of the Sylow p-groups, call it C_p. Here $C_q \lhd G$ and $C_p \ntriangleleft G$. Write $C_q = \langle d \rangle$ and $C_p = \langle c \rangle$. Note $C_q C_p$ is a subgroup of G and $|C_q C_p| = pq$, so $G = C_q C_p$. Therefore, we have $g = d^i c^j$ for any $g \in G$. Since $C_q \lhd G$, we have $cdc^{-1} \in C_q$, so $cd = d^s c$ for some s.

Note: $s \not\equiv 1 \bmod q$, since if $s \equiv 1$, then $cd = dc$, so G is abelian. This contradicts the fact that $n_p = q$. Observe that $c^n dc^{-n} = d^{s^n}$. In particular, $c^p dc^{-p} = d^{s^p}$, so $s^p \equiv 1 \bmod q$.

Now it suffices to show all groups satisfying $G = \langle c, d \rangle$ where $o(c) = p$ and $o(d) = q$ and $cd = d^s c$ for some $s^p \equiv 1 \bmod p$ with $s \not\equiv 1 \bmod q$ are isomorphic. Clearly, any two groups with the same s are isomorphic, but there are $p - 1$ choices for s. Since c can be chosen to be any generator of C_p (of which there are $p - 1$), by replacing c with c^i and s with s_i, we compensate for different choices of s via different choices of generator for C_p. ■

Corollary. Any group of order pq for primes p, q is solvable.

Proof. This is obvious if G is cyclic. Otherwise, $C_q \lhd G$ and $e \lhd C_q \lhd G$ is an abelian tower as G/C_q is cyclic. ■

Corollary. If G is a group in which all of its Sylow subgroups are normal, then G is isomorphic to the direct product of its Sylow groups. In particular, if in addition, all of G's Sylow subgroups are cyclic (e.g. when $|G|$ is square-free), then G will be isomorphic to the direct product of cyclic groups of relatively prime order. Hence G will be cyclic.

Proof. This is corollary of proposition 1.9. ■

> **Example.** See written notes for proof that there are 4 groups of order 30, up to isomorphism and other applications of Sylow theory, e.g. various techniques for showing all groups of order $5 \cdot 7 \cdot 19$ or $5 \cdot 7 \cdot 13$ and $5 \cdot 7 \cdot 17$ are cyclic.

Theorem 2.5: Let G be a group of order pqr for distinct primes $p > q > r$. Let S_p (resp. S_q denote a Sylow-p (resp. Sylow-q) subgroup of G. Then

- At least one of S_p or S_q is normal.
- In fact, S_p must be normal.
- G must be solvable.
- G is cyclic iff none of p, q, r is congruent to 1 mod another.

Proof. (i). Suppose not. Then $n_p = qr$, i.e. G has qr subgroups of order p. Moreover, there are either pr or p subgroups of order q. So G has $qr(p-1)$ elements of order p, i.e. there are $\leq qr$ elements of order $\neq p$. Also there are $\geq p(q-1)$ elements of order q. But $p(q-1) \geq q^2 > qr$.

(ii) Suppose $S_q \triangleleft G$. (By (i) this is enough since we'll show S_q normal implies S_p normal). Then $|G/S_q| = pr$. The number of p-Sylow subgroups of G/S_q is 1 (divides pr and is congruent to 1 mod p). Say $\overline{N}$ is the p-Sylow subgroup of G/S_q.

Lift $\overline{N}$ up to get $N \triangleleft G$ with $|N| = pq$. Also $S_q \triangleleft N$ and $C_p \triangleleft N$. So N is cyclic by the corollary above. Then N cyclic and $C_p \triangleleft N$ implies $C_p \triangleleft G$. So $S_p \triangleleft G$.

(iii). $S_p \triangleleft G$ and S_p is cyclic (hence solvable). Also G/S_p has order qr and hence is solvable (see corollary above). But S_p solvable and G/S_p solvable implies G is solvable.

(iv). Suppose, for example, $p \equiv 1 \bmod q$. Then there exists a nonabelian group H of order pq (proposition 2.4). Consider $C_r \times H$. This is nonabelian and has order pqr.

Suppose none of the primes p, q, r are congruent to 1 modulo the others. By the corollary, it suffices to show all the Sylow subgroups are normal. By (ii), we have $S_p \triangleleft G$. Also G/S_p is a group of order qr and there exists $\overline{N} \triangleleft G/S_p$ with $|\overline{N}| = q$. Lift up to get $N \triangleleft G$ with $|N| = pq$. Since $p \not\equiv 1 \bmod q$, we have N is cyclic. Then there exists $C_q \triangleleft N$. So we also have $C_q \triangleleft G$. Thus $S_q \triangleleft G$.

Also there exists $\overline{N'} \triangleleft G/S_p$ with $|\overline{N'}| = r$ as $q \not\equiv 1 \bmod r$. Lift up to get $N' \triangleleft G$ with $|N'| = pr$. Since $p \not\equiv 1 \bmod r$, we have N is cyclic. Then there exists $C_r \triangleleft N$. So we also have $C_r \triangleleft G$. Thus $S_r \triangleleft G$. ∎

Proposition 2.6. Any group of square-free order in which none of the prime factors are congruent to 1 modulo another must be cyclic.

Proof. Induct on the number of primes dividing G. We've already proved the $n =$

$1, 2, 3$ cases.

$|G| = p_1 p_2 \dots p_n$, $n \geq 4$. Suffices to show each Sylow subgroup is normal.

- We are done if there exists i such that $S_{p_i} \triangleleft G$. Then G/S_{p_i} has order $|G|/p_i$. By induction G/S_{p_i} is cyclic. So for $j \neq i$, there exists $\overline{N}_j \triangleleft G/S_{p_i}$ and $|\overline{N}_j| = p_j$. This gives $N_j \triangleleft G$ with $|N_j| = p_i p_j$. N_j is cyclic and contains C_{p_j} so $C_{p_j} \triangleleft G$. Hence $S_{p_j} \triangleleft G$.

- Show at least 1 Sylow subgroup is normal.

  Suppose G is not simple. Then there exists $N' \triangleleft G$ and $N' \neq \{e\}, G$. We can apply induction to N' to get that N' is cyclic. Thus $S_{p_i} \triangleleft N \triangleleft G$, so $S_{p_i} \triangleleft G$.

  Remains to argue G is not simple. By induction every proper subgroup of G is cyclic (hence abelian). If G is abelian, G is not simple ($n \geq 2$). If G is nonabelian, by the corollary below, we have that G is not simple.

  (Also follows from Feit-Thompson — by our congruence restrictions none of the p_i are 2).

■

Lemma. Let G be a finite nonabelian group in which the intersection of two unequal maximal proper subgroups is always trivial, then G is not simple.

Proof. Suppose G is simple.

- $\{e\}$ is not maximal proper. If it were, then $\{e\}$ is the only proper subgroup of G, so G would be cyclic, e.g. for $x \neq e$, $\{e\} \subset \langle x \rangle \subseteq G$, contradiction as G is nonabelian.

- So $H \subseteq G$ maximal proper implies $|H| \geq 2$. G is not equal to the union of the conjugates of H. Say x lies in the difference of G and this union. There exists $K \subseteq G$, maximal, proper such that $x \in K$.

  There doesn't exist g, g' such that $gHg^{-1} = g'Kg'^{-1}$ as $x \in K$ does not lie in any conjugate of H. Every conjugate of H, K is maximal, proper.

  $$\left(\cup_{g \in G} gHg^{-1}\right) \cap \left(\cup_{g \in G} gKg^{-1}\right) = \{e\}.$$

  Note $|G| \geq |\cup_{g \in G} gHg^{-1}| + |\cup_{g \in G} gKg^{-1}| - 1$ and

$$
\begin{aligned}
|\cup_{g\in G} gHg^{-1}| &\geq (\#\text{ conjugates of } H)(|H|-1)+1\\
&= [G:N_G(H)](|H|-1)+1\\
&\geq [G:H](|H|-1)+1\\
&= |G|-[G:H]+1\\
&\geq |G|/2+1.
\end{aligned}
$$

since $H \subseteq N_G(H) \subseteq G$. As G is simple, $N_G(H) \neq G$, so $N_G(H) = H$ and $|H| \geq 2$ so $[G:H] \leq |G|/2$.

Similarly, $|\cup_{g\in G} gKg^{-1}| \geq |G|/2+1$. Hence $|G| \geq |G|+1$, contradiction.

∎

Corollary. Let G be a nonabelian group such that every proper subgroup is abelian. Then G cannot be simple.

Proof. Suppose G is simple. Let H, K be unequal maximal, proper subgroups of G (see previous proof for why these exist). Look at $C_G(H\cap K)$. Note $H, K \subseteq C_G(H\cap K)$. Thus $C_G(H\cap K) = G$. Thus $H\cap K \subseteq Z(G)$. But $Z(G)$ is trivial as G is nonabelian and simple. So $H\cap K = \{e\}$. By the lemma, we have a contradiction. ∎

Theorem 2.7:

a) All groups of order p^r are solvable.

b) A p-group of order p^r will have a normal subgroup of order p^{r-1}.

Observe that (a) and (b) are equivalent [see corollary of proposition 1.25].

Corollary. If G is finite, it has a subgroup of order p^s for each p^s dividing $|G|$, as we can start with a Sylow-p subgroup and work our way down. Equivalently, the converse of Lagrange is true in p-groups.

Theorem 2.8: If G is a nontrivial p-group, we can always find a tower

$$G = G_0 \triangleright \ldots \triangleright G_s = \{e\}$$

where each G_i is normal in G and G_i/G_{i+1} are cyclic of order p.

Proof. Proceed by induction. Clearly true if $|G| = p$. Assume $|G| \geq p^2$ and we have the result for all groups of smaller order. Recall $Z(G)$ is nontrivial, i.e. there is some $e \neq a \in Z(G)$ such that $o(a) = p$. Let $H = \langle a \rangle$. We've done if $G = H$. Otherwise, by induction G/H has a tower as above. We can lift this tower to get a tower for G. ∎

Lemma. Whenever H is a p-subgroup of G,

$$[N_G(H) : H] \equiv [G : H] \bmod p.$$

In particular, if H is not a Sylow-p subgroup of G, then $p \mid [N_G(H) : H]$. Hence $N_G(H) \neq H$.

Proof. H acts by left translation on the set of left cosets, $S = G/H$. This gives us a homomorphism $\star : H \to \mathrm{Perm}(S)$.

gH fixed point iff $h(gH) = gH$ for all $h \in H$ iff $g^{-1}hgH = H$ for all $h \in H$ iff $g^{-1}hg \in H$ for all $h \in H$ iff $gHg^{-1} \subseteq H$ iff $gHg^{-1} = H$ iff $g \in N_G(H)$. Hence the fixed points are precisely $N_G(H)/H$, i.e. there are $[N_G(H) : H]$ fixed points. By a previous lemma, for a p-subgroup acting on a set, the number of fixed points of the action is congruent to $|S| = [G : H]$. ∎

Theorem 2.9: If $|G| = p^r m$, $p \nmid m$, then any p-subgroup H of G of order p^i, $i < r$, is a normal subgroup of a subgroup of order p^{i+1} in G.

Proof. Since $i < r$, H is not Sylow, so $H \triangleleft N_G(H)$ and by the lemma $p \mid |N_G(H)/H|$. So $N_G(H)/H$ has a subgroup $\overline{K}$ of order p. Let K be the inverse image of $\overline{K}$ under the quotient map $f : N_G(H) \to N_G(H)/H$. Note $H \subseteq K$ and $H \triangleleft K$.

Look at $f|_K : K \to \overline{K}$. This has kernel H. Therefore, $\overline{K} \cong K/H$, so $|K| = p^{i+1}$. ∎

2.1 Nilpotent

Definition. A group is nilpotent iff it is the direct product of its Sylow p-subgroups. Equivalently, all the Sylow p-subgroups are normal.

In a nilpotent group, elements of relatively prime order commute.

Cyclic $\subset$ Abelian $\subset$ Nilpotent $\subset$ Converse of Lagrange $\subset$ Solvable. All these are proper subsets. e.g. S_3 satisfies converse of Lagrange but isn't nilpotent.

Let G be a solvable group of order mn, $\gcd(m,n) = 1$.

- Then G has a subgroup of order m.
- All subgroups of order m are conjugate.
- Any subgroup of order $k \mid m$ is contained in a subgroup of order m.
- In the case where $m = p^r$ is the highest power of p dividing $|G|$, the above restates the Sylow theorems, which would be true even in nonsolvable groups.

3 Direct Sum of Abelian Groups

Definition. For a family of abelian groups $\{A_i\}_{i\in\mathcal{I}}$, we define the direct sum $\bigoplus_{i\in\mathcal{I}} A_i$ to be the subgroup of the direct product consisting of all $(x_i)_{i\in\mathcal{I}}$ with only a finite number of nonzero x_i.

Proposition 3.1. For each $i \in \mathcal{I}$, there exists a canonical homomorphism $\lambda_i : A_i \to A = \oplus A_i$ such that given any abelian group B and a family of homomorphisms $f_i : A_i \to B$, there is a unique homomorphism $f : A \to B$ such that $f_i = f \circ \lambda_i$.

Proof. For $a \in A_i$, $\lambda_i(a)$ is the element of the direct sum whose i-th component is a and whose remaining components are 0. Define $f : A \to B$ by $f((x_i)) = \sum f_i(x_i)$. Need abelian to show homomorphism. ∎

Proposition 3.2. A group will be isomorphic to the direct sum of 2 subgroups if either one of the following holds:

- $A = B + C$ and $B \cap C = \{e\}$
- Every element of A can be written uniquely as a sum of an element of B and an element of C.

Definition. An abelian group A has a **basis** $\{e_i\}_{i\in\mathcal{I}}$ if every element of A can be written uniquely as a finite linear combination of the e_i with coefficients in $\mathbb{Z}$. An abelian group is a **free abelian group** if it has a basis.

The **free abelian group** $\mathbb{Z}\langle S\rangle$ **generated by S** is the set of all maps $\varphi : S \to \mathbb{Z}$ such that $\varphi(x) = 0$ for all but a finite number of $x \in S$. We also write $F_{\mathrm{ab}}(S)$ for $\mathbb{Z}\langle S\rangle$.

Define $f_S : S \to \mathbb{Z}\langle S\rangle$ via $x \mapsto 1 \cdot x$ where $1 \cdot x : S \to \mathbb{Z}$ that maps $x \mapsto 1$ and everything else maps to 0. Similarly, for $k \in \mathbb{Z}$, $k \cdot x$ maps $x \mapsto k$ and everything else to 0. Note f_S is injective. It's clear, any element of $f \in \mathbb{Z}\langle S\rangle$ can be written $f = k_1x_1 + \ldots + k_sx_s$ where $x_i \in S$ are the finitely-many points at which f does not vanish, and the k_i are the values of f at those points. Moreover, f can be written as a finite linear combination of $x_i \in S$ in exactly one way.

Note: An abelian group is free iff it equal $F_{\text{ab}}(S)$ for some set S.

Fact. Any abelian group is isomorphic to a quotient of a free abelian group. Any finitely-generated abelian group is a quotient of a free abelian group on a finite number of generators.

Lemma. Let $f : A \to A'$ be a surjective homomorphism, where A is an abelian group and A' is a *free* abelian group. Let $B = \ker(f)$. Then there exists a subgroup $C \subseteq A$ such that $f|_C$ is an isomorphism $C \to A'$ and $A \cong B \oplus C$, i.e. $A \cong \ker(f) \oplus \mathrm{Im}(f)$.

Proof. Let $\{x_i'\}$ be a basis for A'. Let $x_i \in A$ such that $f(x_i) = x_i'$. Let C be the subgroup of A generated by the x_i. Clearly, $f|_C$ maps C onto A'. Moreover, $\ker(f|_C) = 0$ as if $x \in \ker(f|_C)$, then $x = \sum n_ix_i$ and $f(x) = 0$, so $0 = \sum n_i f(x_i) = \sum n_i x_i'$. But x_i' is a basis for A', so $n_i = 0$. Hence $f|_C$ is an isomorphism $C \to A'$.

Now let $x \in A$. Then $f(x) = f(c)$ for some $c \in C$, so $x - c \in \ker(f)$. Hence $x = b + c$ for some $b \in \ker(f)$ and $c \in C$. Also $B \cap C = \ker(f) \cap C = \ker(f|_C) = 0$. Thus $A = B \oplus C$. ∎

Theorem 3.3: Let A be a free abelian group and B be a subgroup of A. Then B is also a free abelian group and the cardinality of any basis for B is $\leq$ the cardinality of any basis for A. In particular, any two bases for A have the same cardinality.

Proof. Say $\{x_1, \ldots, x_n\}$ is a basis for A, i.e. $A = \mathbb{Z}x_1 \oplus \ldots \oplus \mathbb{Z}x_n$. Proceed by induction on n.

Clearly true if $n = 1$ by result on infinite cyclic group. We will show (i) B has a basis of $\leq n$ elements and (ii) all bases for B have the same number of elements.

(i). Let $f : A \to \mathbb{Z}x_1$ be the canonical projection. Let $B_1 = \ker(f|_B) = \{b \in B : b \text{ is a linear combination of } x_2, \ldots, x_n\}$. Then B_1 is a subgroup of the free abelian group generated by $x_2, \ldots, x_n$. So B_1 is a subgroup of a free abelian group that has a basis for cardinality $n-1$. So by induction B_1 is free and has a basis with $\leq n-1$ elements. We have the surjective homomorphism, $f|_B : B \to \mathbb{Z}x_1$, so by the lemma B contains a subgroup $C_1 \cong \mathrm{Im}(f|_B)$ such that $B \cong B_1 \oplus C_1$ where C_1 is either the free abelian group on 1 generator or $\{0\}$. So B has a basis with $\leq n$ elements.

(ii). Let T, S be 2 bases for B. We can assume one of these is finite as we've already proven B has at least 1 finite basis. WLOG assume $|S| = m < \infty$. We will be done if we show $r \leq m$ whenever $|T| \geq r$.

Claim. Let p be a prime. Then $|S| = m$ implies $|B/pB| = p^m$ and $|T| \geq r$ implies $|B/pB| \geq p^r$. Hence $m \geq r$.

Let $S = \{x_1, \ldots, x_m\}$ and $\varphi : B \to \oplus_{i=1}^m \mathbb{Z}/p\mathbb{Z}$ by $a_1x_1 + \ldots + a_mx_m \mapsto (\overline{a_1}, \ldots, \overline{a_m})$. Clearly, φ is a well-defined, surjective homomorphism as S forms a basis. Also $\ker \varphi = pB$. The same argument works for an infinite basis since if $T = \{z_i\}_{i \in \mathcal{I}}$ then $B = \oplus_{z_i \in T} \mathbb{Z} z_i$. So $B/pB \cong \oplus_{z_i \in T} \mathbb{Z}/p\mathbb{Z}$, the latter clearly has order $\geq p^r$.

∎

Definition. Let A be a free abelian group, then $\text{rank}(A)$ is the number of elements in any basis for A.

Proposition 3.4. If A is a free abelian group of rank n and B is a nonzero subgroup of A, then there exists a basis $\{x_1, \ldots, x_n\}$ for and positive integers $d_1 \mid d_2 \mid \ldots \mid d_r$ where $r \leq n$ such that $\{d_1x_1, \ldots, d_rx_r\}$ forms a basis for B.

Definition. Let A be an abelian group. An element $x \in A$ is called a **torsion element** if $na = 0$ for some nonzero $n \in \mathbb{Z}$. Equivalently, if x has finite order.

A_{tor} is the **torsion subgroup** of A, the subgroup of A consisting of all torsion elements of A. A is a **torsion group** if $A = A_{tor}$.

A finitely-generated torsion group is finite.

The p-**part** of A, $A(p) = \{x \in A | o(x) \text{ is a power of } p\}$. *If $A(p)$ is finite, it is a p-group.*

Examples.

- $\times_{p \text{ prime}} \mathbb{Z}_p$ is not torsion. It's torsion subgroup is $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \ldots$
- The torsion subgroup of $\oplus_{i=2}^\infty \mathbb{Z}_i$?
- $\mathbb{Z}_{25}^\infty$ is torsion and $\oplus_{i=1}^\infty \mathbb{Z}_{25}$ is also torsion.
- $\mathbb{Q}/\mathbb{Z}$ is torsion.

Proposition 3.5. If A be a torsion abelian group. Then $A \cong \oplus A(p)$.

Proof. Let $\varphi : \oplus A(p) \to A$ by $x = (x_p) \mapsto \sum_p x_p$ (note the sum is finite). Clearly a homomorphism.

Suppose $x = (x_p) \in \ker\varphi$, i.e. $\sum_p x_p = 0$. Then $x_q = \sum_{p\neq q}(-x_p)$. The LHS is killed by some q^i and the RHS is killed by the lcm of the orders of x_p, $p \neq q$ (call this m). But $\gcd(m, q^i) = 1$, so $x = 0$.

Let $x \in A$ and suppose $o(x) = m = \prod p_i^{r_i}$, p_i distinct. Suffices to show $x = \sum x_i$ where each $x_i \in A(p_i)$, but this follows from induction on the lemma below. ∎

Lemma. If $x \in A$ has order m where $m = rs$ for $\gcd(r, s) = 1$. Then $x = y + z$ where $sy = rz = 0$.

Proof. We know $1 = \lambda r + \delta s$ where $\lambda, \delta \in \mathbb{Z}$, so $x = \lambda rx + \delta sx = y + z$ ($y = \lambda rx$, so $sy = \lambda mx = 0$ and $z = \delta sx$, so $rz = \delta mx = 0$). ∎

Corollary. Any finite abelian group is isomorphic to the direct sum of finite abelian groups.

Definition. A finite abelian p-group is of type $(r_1, \ldots, r_s)$ if it is isomorphic to $\mathbb{Z}/p^{r_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{r_s}\mathbb{Z}$.

Theorem 3.6: Any finite abelian p-group is isomorphic to the direct product of cyclic p-groups. If it is of type $(r_1, \ldots, r_s)$ where r_i are decreasing, then the sequence is uniquely determined.

Proof. Proceed by induction on $|A|$. Clearly, true if $|A|$ is prime. Assume the result holds for all finite abelian p-groups of order $< |A|$. Choose $a_1 \in A$ of maximal order p^{r_1}. Let $A_1 = \langle a_1 \rangle$. Note A/A_1 is a finite abelian p-group of order $< |A|$. So by induction $A/A_1 \cong \overline{A_1} \oplus \ldots \oplus \overline{A_s}$, where the $\overline{A_i}$ are cyclic or order p^{r_i} with $r_i \geq r_{i+1}$. Let $\overline{A_i} = \langle \overline{a_i} \rangle$ and $A_i = \langle a_i \rangle$. By the lemma, we can chose $a_i \in A$ such that a_i reduces to $\overline{a_i}$ mod A_1 and $o_A(a_i) = p^{r_i}$.

Claim. $A \cong A_1 \oplus \ldots \oplus A_s$. *Proof.* First show $A = A_1 + \ldots + A_s$. If $x \in A$, then $\overline{x} \in A/A_1$, so $\overline{x} = m_2\overline{a_2} + \ldots + m_s\overline{a_s}$ for some $m_i \in \mathbb{Z}$. Thus $\overline{x} - m_2\overline{a_2} - \ldots - m_s\overline{a_s} = \overline{0}$, so $x - m_2a_2 - \ldots - m_sa_2 \in A_1$, i.e. $x = \sum_{i=1}^s m_ia_i$. We also need to show this linear combination is unique; equivalently, show $0 = \sum_{i=1}^s n_ia_i$ implies $n_ia_i = 0$. But we have $\overline{0} = \sum_{i=1}^s n_i\overline{a_i}$, thus $m_i\overline{a_i} = 0$ so $m_i \mid o(\overline{a_i})$, so $m_i \mid o(a_i)$ so $n_ia_i = 0$ for $2 \leq i \leq s$.

Show uniqueness. Suppose A is of type $(r_1, \ldots, r_s)$, $r_i \geq r_{i+1}$ and also of type $(m_1, \ldots, m_t)$, $m_i \geq m_{i+1}$. We'll proceed by induction on $|A|$. Note pA is abelian, but $|pA| < |A|$ and pA is of type $(r_1 - 1, \ldots, r_s - 1)$ and of type $(m_1 - 1, \ldots, m_t - 1)$.

By induction, the sequence for pA is uniquely determined. (Note this tells us nothing about components where $r_i - 1 = 0$ or $m_i - 1 = 0$, so $r_1, \dots, r_s$ and $m_1, \dots, m_t$ can only differ in the number of 1's which appear, but this can't happen by a counting argument.) ∎

Lemma. Let A be a finite abelian p-group and $a_1 \in A$ be an element of maximal order p^{r_1}. Let $A_1 = \langle a_1 \rangle$ and $\bar{b} \in A/A_1$ of order p^r in A/A_1. Then there exists $a \in A$ that reduces to $\bar{b}$ mod A_1 such that a has order p^r in A.

Proof. Note for any representative b of $\bar{b}$ the order of b in A must be $\geq o(\bar{b}) = p^r$ in A/A_1. Suffices to find a representative a of $\bar{b}$ such that $o(a) \leq p^r$, which will follow if $p^r a = 0$.

Let b be any representative of $\bar{b}$. We're done if $p^r b = 0$, so assume this is not the case. It is enough to find $c \in A_1$ such that $p^r c = p^r b$ as then we can let $a = b - c$ and then a reduces to $\bar{b}$ mod A_1 and $p^r a = 0$. Then since $0 \neq p^r b \in A$, we have $p^r b = n a_1$ for some $n \in \mathbb{Z}$. Write $n = p^k \mu$ where $p \nmid \mu$. So $p^r b = p^k \mu a_1$. As $\gcd(\mu, p^{r_1}) = 1$, μa_1 generates $\langle a_1 \rangle$. Relabeling, $p^r b = p^k a_1$. If suffices to show $k \geq r$, then we can let $c = p^{k-r} a_1$ so $c \in A_1$ and $p^r c = p^k a_1 = p^r b$. But since $p^k a_1 = p^r b \neq 0$ and $o(a_1) = p^{r_1}$, we have $o(p^k a_1) = p^{r_1 - k}$. Thus $o(p^r b) = p^{r_1 - k}$. Hence $o(b) = p^{r_1 + r - k}$, so by maximality of r_1, we have $k \geq r$. ∎

Theorem 3.7: Let $A \neq 0$ be a finitely-generated torsion-free abelian group. Then A is free.

Proof. Let S be a finite generating set for A. Let $x_1, \dots, x_n$ be a maximal linearly independent subset of S. Clearly, $n \geq 1$ as if $x \in S$, $x \neq 0$, then $\{x\}$ is linearly independent as $A \neq A_{\text{tor}}$. Let B be the subgroup of A generated by $x_1, \dots, x_n$. Note B is free since the x_i are linearly independent and span B. So we're done if $S = \{x_1, \dots, x_n\}$ as then $A = B$. Otherwise, if $y \in S - \{x_i\}$, then $\exists m, m_1, \dots, m_n \in \mathbb{Z}$ (not all 0) such that $my + \sum_{i=1}^n m_i x_i = 0$. If $m = 0$, this contradicts the fact that the x_i are linearly independent. So $m \neq 0$ and $my \in B$. Thus for each $y \in S$, there exists m_y such that $m_y y \in B$. As $|S| < \infty$, there exists some $d \in \mathbb{Z} \backslash 0$ such that $dy \in B$ for all $y \in S$. As S generates A, this implies $dA \subseteq B$. By theorem 3.3, dA is free and $r = \operatorname{rank} dA \leq \operatorname{rank} B = n$, so dA has a basis $\{da_1, \dots, da_r\}$. Define $\varphi : A \to dA$ by $a \mapsto da$ which is clearly a homomorphism. As A is torsion-free, $\ker \varphi = 0$. Thus $A \cong dA$, so A is free of rank r. ∎

Example. Let $A = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z}$ (so A is finitely-generated but not torsion-free). Then dA is free with basis $\{d(1,0,k), d(0,1,k)\}$ but A isn't free.

Lemma. Let A be a finitely-generated abelian group. Let B be a subgroup of A. Then B is f.g. and if A is generated by n generators, then B can be generated with $\leq n$ generators.

Proof. Suppose A is generated by n generators. Let F be the free abelian group on n generators. We know there exists a surjective homomorphism $\varphi : F \to A$ mapping the generators for F to the generators for A. As $B \leq A$, we have $\varphi^{-1}(B) \leq F$. By theorem 3.3, $\varphi^{-1}(B)$ is free and f.g. by $\leq n$ elements. Since φ is onto, $\varphi(\varphi^{-1}(B)) = B$. So clearly, B is f.g. abelian group on $\leq n$ generators. ■

Theorem 3.8: Let A be a finitely-generated abelian group with torsion subgroup A_{tor}. Then

a) A_{tor} is finite

b) A/A_{tor} is finitely-generated and free

c) there exists a subgroup C of A that is isomorphic to A/A_{tor} such that $A \cong A_{\text{tor}} \oplus C$.

Proof. (a). By the lemma, A_{tor} is f.g., so since it is torsion, this implies finite.

(b). Show A/A_{tor} is torsion-free (together with f.g. this implies free). Let $\overline{x}$ be a torsion element of A/A_{tor}. Then $n\overline{x} = \overline{0}$ for some nonzero $n \in \mathbb{Z}$, i.e. $\overline{nx} = \overline{0}$. Thus $nx \in A_{\text{tor}}$. Thus $m(nx) = 0$ for some nonzero $m \in \mathbb{Z}$. Thus $(mn)x = 0$ and $mn \neq 0$, so $x \in A_{\text{tor}}$. Hence $\overline{x} = \overline{0}$.

(c). Immediate from the lemma to theorem 3.3. ■

Definition. If A is a f.g. abelian group, $\text{rank}(A) = \text{rank}(A/A_{\text{tor}})$. If A has rank d, then d is uniquely determined by A and $A \cong A_{\text{tor}} \oplus \mathbb{Z}^d$.

4 Rings

Definition. A **ring** consists of a nonempty set R with two binary operations $+$ and $\cdot$ and two distinguished elements 0 and 1 such that:

- $(R, +, 0)$ is an abelian group
- $(R, \cdot, 1)$ is a monoid

- $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$ for all $a, b, c \in R$.

We say the ring is commutative, if additionally $(R, \cdot, 1)$ is abelian.

A **left ideal** is an additive subgroup $I \subseteq A$ such that $AI \subseteq I$.

A **principal ring** is a commutative ring in which all ideals are principal, i.e. generated by a single element. An **integral domain** in a commutative ring with $1 \neq 0$ with no zero divisors. An element π in an integral domain A is called irreducible, if $\pi = xy$ implies x or y is a unit. A **PID** is an integral domain in which all ideals are principal.

Let $\mathcal{O}(\mathbb{C})$ denote the set of entire functions. This forms a commutative ring.

Fact. Given any closed discrete set $\{z_i\} \subseteq \mathbb{C}$ with a corresponding set $\{m_i\} \subseteq \mathbb{Z}^+$, then there exists $f(x) \in \mathcal{O}(\mathbb{C})$ that vanishes at those points with multiplicity m_i and has no other zeros.

- $\mathcal{O}(\mathbb{C})$ is an integral domain. The units are elements of $\mathcal{O}(\mathbb{C})$ without zeros, i.e functions of the form $\lambda e^g(x)$ where $g(x) \in \mathcal{O}(\mathbb{C})$.
- All finitely-generated ideals are principal. An integral domain with this property is called a **Bezout domain**.
- Let $I = \{f \in \mathcal{O}(\mathbb{C}) : \exists m_f \in \mathbb{Z} \text{ such that } f(z) = 0, \forall z \in m_f\mathbb{Z}\}$. This is not a principal ideal (it's not even finitely-generated).
- Bezout $\Rightarrow$ GCD domain, but GCD $\not\Rightarrow$ Bezout. In fact, UFD $\Rightarrow$ GCD, but UFD $\not\Rightarrow$ Bezout as [UFD + Bezout] $\Rightarrow$ PID, yet PID $\not\Rightarrow$ UFD.
- Bezout implies irreducible elements generate prime ideals. Note: irreducible elements generating prime ideals is a sufficient condition for unique factorization. But UFD $\not\Rightarrow$ Bezout because you don't always have factorization.
- In fact, Bezout implies irreducible elements form maximal ideals.
- Irreducibles of $\mathcal{O}(\mathbb{C})$: Entire functions with exactly one simple zero. Thus the only elements which can be written as a product of irreducibles are those with finitely-many zeros. Thus $\mathcal{O}(\mathbb{C})$ is a **non-atomic Bezout domain**.

Proposition 4.1. All finitely-generated ideals of $\mathcal{O}(\mathbb{C})$ are principal.

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J \right\} \subseteq I \cap J$$

In $\mathbb{Z}$, $(m)+(n) = (\gcd(m,n))$, $(m)(n) = (mn)$, and $(m)\cap(n) = (\operatorname{lcm}(m,n))$. Moreover, in $\mathbb{Z}$, $(I+J)(I\cap J) = IJ$.

Proposition 4.2. Let R be a ring. If $I+J=(1)$, then $I\cap J = IJ$.

Proof. Fact. $I(J_1+J_2) = IJ_2+IJ_2$. Thus $I\cap J = (I+J)(I\cap J) = I(I\cap J)+J(I\cap J) \subseteq IJ$. ∎

Proposition 4.3. If $I_1,\ldots,I_n$ are pairwise coprime, then $I_1\ldots I_n = I_1\cap\ldots\cap I_n$.

Proof. Follows easily by induction. In this case, pairwise coprime implies $I_1\ldots I_k + I_{k+1} = (1)$, as for example, if $n=3$ and $I_1+I_3=(1)$ and $I_2+I_3=(1)$, then $I_1I_2+I_3 \supseteq (I_1+I_3)(I_2+I_3) = (1)$. ∎

Addition of ideals is commutative and associative. Products of ideals are associative and commutative (in commutative rings). Ideals of R form a monoid under addition and multiplication.

Definition. A **fractional ideal** M is an A-module contained in K (the field of fractions for A), but is not contained in A, and $M = \frac{I}{d}$ for some $d\in A$ and ideal $I\subseteq A$.

A **Dedekind domain** is an integral domain in which the set of nonzero fractional ideals forms a group under multiplication. Equivalently, it's an integral domain in which every ideal can be written as a product of prime ideals.

In a Dedekind domain A, let $\mathcal{I}$ be the commutative group of nonzero fractional ideals. Let $\mathcal{P}$ be the subgroup of principal ideals. Then the **ideal class group** of A is a factor group $\mathcal{H} = \mathcal{I}/\mathcal{P}$.

Proposition 4.4. The ideal class group in the ring of integers of a number field is finite. (This is true in a general Dedekind domain). The **class number** of a number field K is $|\mathcal{H}|$.

In a Dedekind domain, UFD is equivalent to PID.

Definition. A map $f: A\to B$ is a **ring homomorphism** if

a) $f(a+b) = f(a)+f(b)$

b) $f(ab) = f(a)f(b)$

c) $f(1_A) = 1_B$.

$\ker(f) = \{x \in A : f(x) = 0_B\}$.

Proposition 4.5. If $f : A \to B$ is a ring homomorphism and I is an ideal such that $I \subset \ker(f)$, then there is a unique homomorphism $f_* : A/I \to B$ such that $f = f_* \circ \varphi$ where $\varphi : A \to A/I$ is the quotient map. Moreover, f_* is injective iff $I = \ker(f)$.

There is a one-to-one correspondence between ideals in A/I and ideals in A containing I.

Definition. If B is a commutative ring, A subring, $S \subseteq B$, we say B is generated by S over A, written $B = A[S]$, if B is the smallest subring of itself containing A and S.

Note $k[x]$ is finitely-generated as a ring over k, but not f.g. as a module over k.

A **field** is a commutative ring in which the nonzero elements form a group under multiplication.

Proposition 4.6. A commutative ring A with $1 \neq 0$ is a field iff the only ideals are (0) and (1). [Analogous statement false in noncommutative rings]

Proof. Let A be a field and $I \neq \{0\}$ an ideal. Let $a \neq 0$, $a \in I$. Then $a^{-1} \in A$, so $aa^{-1} = 1 \in I$. Then for any $x \in A$, $x1 = x \in I$, so $I = A$.

Conversely, suppose the only ideals in A are (0) and A. Let $x \in A$, $x \neq 0$. Then $(x) = A$. Thus $1_A \in (x)$, so $1_A = xy$ for some $y \in A$, so x is a unit. ∎

Definition. A proper ideal I in a commutative ring A is called **prime** if whenever $xy \in I$ then $x \in I$ or $y \in I$.

A proper ideal I in a commutative ring A, with $1 \neq 0$ is called **maximal** if whenever $I \subseteq J$ for an ideal J, then either $I = J$ or $J = A$.

Proposition 4.7. (a). A proper ideal I is prime iff A/I is an integral domain. (b). A proper ideal I is maximal iff A/I is a field.

Proof. (a). I proper implies A/I commutative ring with $1 \neq 0$. So A/I ID iff A/I has no zero divisors iff $\overline{xy} = \overline{0}$ implies $\overline{x} = 0$ or $\overline{y} = 0$ iff $xy \in I$ implies $x \in I$ or $y \in I$ iff I is prime.

(b). I maximal iff there are exactly two ideals of A that contain I (and A/I is a ring with $\overline{1} \neq \overline{0}$) iff A/I has exactly two ideals iff A/I is a field. ∎

Proposition 4.8. Suppose $B = \prod_{i=1}^{n} A_i$ for commutative rings A_i. Identify A_i with

$$J_i = \{(0, 0, \ldots, 0, a_i, 0, \ldots, 0) : a_i \in A\} \subseteq B$$

(this is an ideal, *not a subring*, of B). Let I be an ideal in B and let $I_i = I \cap J_i$. Then

$$(\star, \ldots, \star, a_i, \star, \ldots, \star) \in I \Rightarrow (0, \ldots, a_i, \ldots, 0) \in I.$$

Thus $\bigoplus_{i=1}^{n} I_i = I$. Hence any ideal in $\prod_{i=1}^{n} A_i$ can be written as a product $\prod_{i=1}^{n} I_i$, where I_i is an ideal in A_i. Moreover, $A/I \cong A_1/I_1 \times \ldots \times A_n/I_n$, so I is prime (maximal) iff $I_i = A_i$ for all but one i, and the ideal $I_{i_0} \neq A_{i_0}$ is prime (maximal).

Infinite Case. $B = \prod_{i=1}^{\infty} \mathbb{Z}_2$. Then $M_i = \{x \in B : x_i = 0\}$ is a maximal ideal in B. Also $M_\infty = \bigoplus_{i=1}^{\infty} A_i$ is not contained in any M_i (so the M_i can't be the only maximal ideals). Note M_∞ isn't maximal since $M_\infty \subsetneq J_1$ where all even numbered entries are zero from some point onward. J_1 isn't maximal since $J_1 \subsetneq J_2$ where are entries whose index are divisible by 4 are zero from some point onward, etc. Let $J = \bigcup_{i=1}^{\infty} J_i$. Note J isn't maximal since it's contained in the set of I which consists of elements of B such that there exists $m \in \mathbb{Z}^+$ such that all entries of indices divisible by m are 0 from some point on.

Corollary. If $f : A \to B$, f a homomorphism, B an integral domain, then $\ker f$ is prime. In particular, if $P \subseteq B$ is a prime ideal, then $f^{-1}(P)$ is also a prime ideal (consider $\phi : A \to B \to B/P$, then $\ker \phi = f^{-1}(P)$).

Corollary. Let $f : A \to B$ be a homomorphism.

a) If B is an integral domain, then $\ker f$ is prime.

b) If $P \subseteq B$ is a prime ideal, then $f^{-1}(P)$ is a prime ideal (consider the composition $A \to B \to B/P$ with kernel $f^{-1}(P)$).

c) If $\ker f$ is prime (maximal), then f onto implies B is an integral domain (a field).

d) If $P \subseteq B$ is a maximal ideal and f is onto, then $f^{-1}(P)$ is maximal.

e) $(0) \subseteq A$ is prime (maximal) iff A is an integral domain (field).

Proposition 4.9. Let A be a commutative ring with $1 \neq 0$ and I a proper ideal. Then $I \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.

Proof. Use Zorn's lemma. Let Σ be the set of all proper ideals containing I ordered by $\subseteq$. As $I \in \Sigma$, Σ is nonempty. Let

$$I_1 \subseteq I_2 \subseteq \ldots$$

be a chain of elements. Let $\mathcal{I} = \bigcup I_i$, then $\mathcal{I}$ is an ideal and it contains I. Note $\mathcal{I}$ is proper since $1 \notin \mathcal{I}$. So $\mathcal{I} \in \Sigma$, so Σ has a maximal element by Zorn's lemma. ■

Proposition 4.10. The prime (maximal) ideals in A/I are in one-to-one correspondence with prime (maximal) ideals in A containing I.

Proof. If J is an ideal containing I, then $(A/I)/(J/I) \cong A/J$, so J is prime (maximal) in A iff J/I is prime (maximal) in A/I. ■

Proposition 4.11. Let $I_1, \dots, I_n$ be ideals in a commutative ring A. Then there exists a natural map $\varphi : A \to \prod_{i=1}^n A/I_n$ given by

$$a \mapsto (a \bmod I_1, \dots, a \bmod I_n).$$

Note $\ker \varphi = \cap I_i$.

a) φ is surjective iff I_i are pairwise coprime, i.e. $I_i + I_j = A$ for $i \neq j$.

b) φ is injective iff $\cap I_i = 0$.

Proof. (a). Assume φ is surjective. Then for any $i \neq j$, there exists $x \in A$ such that $x \equiv 1 \bmod I_i$ and $x \equiv 0 \bmod I_j$. Then $1 = (1 - x) + x$, where $1 - x \in I_i$ and $x \in I_j$, so $1 \in I_i + I_j$, i.e. I_i, I_j are coprime.

Conversely, suppose the I_i are pairwise coprime. It suffices to show the image of φ contains $(1, 0, \dots, 0)$ (the rest follows by symmetry). For any $j \neq i$, we know $I_i + I_j = (1)$, so there exists $x_j \in I_i$ and $y_j \in I_j$ such that $x_j + y_j = 1$. Let

$$y = \prod_{j=2}^{n} y_j = \prod_{j=2}^{n} (1 - x_j).$$

Clearly, $y \equiv 1 \bmod I_1$ and $y \equiv 0 \bmod I_j$ for $i \neq j$. ■

Corollary. If $I_1, \dots, I_n$ are pairwise coprime then $A/\cap I_i = A/\prod I_i \cong \prod A/I_i$.

Corollary. If $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as rings, so $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times$. ■

4.1 Localization

Define $\sim$ on $A \times (A - 0)$ by $(a,s) \sim (b,t)$ iff $at - bs = 0$. This is an equivalence relation as long as we have no zero divisors, i.e. A is an integral domain. Define $\frac{a}{s} = \overline{(a,s)}$. Then we define

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \qquad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}.$$

(check these are well-defined). Then we have a field.

Generalizations: (1) only want to invert a subset of $A - 0$? (2) what if A isn't an ID?

Let A be a commutative ring with $1 \neq 0$ and S be a multiplicatively closed subset of A with $1 \in S$. Define a relation on $A \times S$ by $(a,s) \sim (b,t)$ if $(at - bs)u = 0$ for some $u \in S$. It can be shown this is an equivalence relation. Define everything else as above, then the set of equivalence classes $S^{-1}A$ form a ring (it will be nonzero as long as $0 \notin S$). There is a canonical map $f : A \to S^{-1}A$ by $a \mapsto \frac{a}{1}$. Note f is a ring homomorphism and elements of S map to units.

Warning. This map isn't one-to-one if S contains zero divisors. $\ker(f) = \{a : \frac{a}{1} = \frac{0}{1}\} = \{a : (a \cdot 1 - 1 \cdot 0)s = 0, \text{ for some } s \in S\} = \{a : \exists s \in S, as = 0\}$.

Universal Property. $g : A \to B$ is a ring homomorphism such that $g(S)$ are units, then there exists a unique homomorphism g^* such that $g^* \circ f = g$ where f is the canonical map $A \to S^{-1}A$.

Proof. Define $g^*(\frac{a}{s}) = g(a)g(s)^{-1}$. Check well-defined. Note: $\ker f \subseteq \ker g$ as $a \in \ker f$ then $as = 0$ for some $s \in S$, so $g(a)g(s) = 0$. Since $g(s)$ is a unit, $g(a) = 0$. ∎

Localization Isomorphism. Note $f : A \to S^{-1}A$ satisfies

- $s \in S$ implies $f(s)$ unit
- $f(a) = 0$ implies $\frac{a}{1} = 0$ so there exists $s \in S$ such that $as = 0$.
- every element of $S^{-1}A$ is of the form $f(a)f(s)^{-1}$, i.e. it equals $\frac{a}{1}\frac{1}{s}$ where $a \in A, s \in S$.

These properties are all that were used in the previous proof. Conversely, these three properties determine $S^{-1}A$ up to isomorphism, i.e. if $g : A \to B$ such that the analogous 3 properties hold, then $B \cong S^{-1}A$.

Example.

- A is a commutative ring and $S = \text{units}(A)$. Then $S^{-1}A \cong A$.
- $A =$ integral domain and $S =$ nonzero elements. Then $S^{-1}A$ is the quotient field.
- $A =$ commutative ring, P prime ideal, $S = A - P$. Then $A_P = S^{-1}A = \{\frac{a}{b} : b \notin P\}$ is a local ring. See prop 2.12, $\mathfrak{m} = pA_p$.

Proposition 4.12. Let A be a commutative ring $\neq 0$. Suppose the set $\mathfrak{m}$ of non-units in A forms an ideal. Then A is a local ring and $\mathfrak{m}$ is the unique maximal ideal.

Proof. Any proper ideal contains only nonunits. So any proper ideal of A is contained in $\mathfrak{m}$. So $\mathfrak{m}$ is a proper ideal in A that contains every other proper ideal. Hence $\mathfrak{m}$ is the unique maximal ideal. ■

Example.

- A local ring, $\mathfrak{m}$ maximal ideal, $S = A - \mathfrak{m}$. Then $A_\mathfrak{m} = \{\frac{a}{b} : b \notin \mathfrak{m}\}$. Then $A_\mathfrak{m} \cong A$.
- $A = A_1 \times \ldots \times A_n$, A_i local, $m_2^\star = A_1 \times m_2 \times \ldots \times A_n$ maximal ideal in A, m_2 maximal ideal in A_2.

  Then $A_{m_2^\star} \cong A_2$. Pf: Project $g : A \twoheadrightarrow A_2$. Check 3 conditions. $S = A - m_2^\star$ = everything whose 2nd component is a unit in A_2.

  (1) If $s \in S$, then $g(s)$ is a unit.

  (2) If $g(a) = 0$, then $a \in \ker(g)$, so 2nd component of a is 0. Thus a is killed by $(0, 1, 0, \ldots, 0) \in S$.

  (3) g onto, so any $x \in A_2$ can be written as $g(a)g(s)^{-1}$, $s \in S$, $a \in A$.
- A commutative ring, $f \in A$, $S = \{1, f, f^2, \ldots\}$. $A_f = S^{-1}A = \{\frac{a}{b} : b = f^n \in S\}$
- $A = k[x_1, \ldots, x_n]$, $S = A - 0$. Then $S^{-1}A = k(x_1, \ldots, x_n)$.
- $A = k[x_1, \ldots, x_n]$, k algebraically closed, $\mathfrak{m}$ maximal ideal in A, $S = A - \mathfrak{m}$. Fact: (Nullstellensatz) Any maximal ideal in A is of the form

$$(x_1 - a_1, \ldots, x_n - a_n)$$

for some $p = (a_1, \dots, a_n) \in k^n$. Then $S^{-1}A = \{\frac{f}{g} : g \text{ doesn't vanish at } p\}$

Proposition 4.13. $S^{-1}A = 0$ iff $0 \in S$.

Proof. $S^{-1}A = 0$ iff $\frac{1}{s} = \frac{0}{1}$ iff $(1 - 0s)t = 0$ for some $t \in S$ iff $t = 0$, $t \in S$. ∎

Proposition 4.14. If I is an ideal in A, then $S^{-1}I = \{\frac{a}{b} : a \in I, s \in S\}$ is an ideal in $S^{-1}A$. It is the smallest ideal in $S^{-1}A$ containing I. Also

$S^{-1}(I + J) = S^{-1}I + S^{-1}J$

$S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$

$S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$

Proposition 4.15. $S^{-1}I = S^{-1}A$ iff $S \cap I \neq \varnothing$.

Proof. $S^{-1}I = S^{-1}A$ iff $1 \in S^{-1}I$ iff $\frac{1}{1} = \frac{x}{s}$, $x \in I$, $s \in S$ iff $(s - x)t = 0$ for some $t \in S$ iff $xt = st$ iff $S \cap I = \varnothing$ since $st \in S$ and $xt \in I$. ∎

Proposition 4.16. Any ideal in $S^{-1}A$ is of the form $S^{-1}I$ for some ideal $I \subseteq A$. In particular, if J is an ideal in $S^{-1}A$, then $S^{-1}f^{-1}(J) = J$.

Proof. Note $f^{-1}(J) = \{a \in A : \frac{a}{1} \in J\}$. Clearly $S^{-1}(f^{-1}(J)) \subseteq J$. Conversely, let $\frac{x}{s} \in J$. Then $\frac{x}{1} \in J$, so $x \in f^{-1}(J)$. Hence $\frac{x}{s} \in S^{-1}f^{-1}(J)$. ∎

Proposition 4.17. Let X be the prime ideals in A not meeting S and Y be the prime ideals in $S^{-1}A$. There is a one-to-one correspondence between X and Y

Proof. Use the maps $I \mapsto S^{-1}I$ (from $X \to Y$) and $J \mapsto f^{-1}(J)$ (from $Y \to X$).

- Fact 1. If $p \in Y$, then $f^{-1}(p) \in X$ because contraction of a prime ideal is prime and $f^{-1}(p)$ doesn't meet S, as otherwise $p = S^{-1}A$.
- Fact 2. Let $p \in X$. Show $S^{-1}p \in Y$. Let $\frac{x}{s}, \frac{y}{t} \in S^{-1}A$ such that $\frac{xy}{st} \in S^{-1}P$. Then $\frac{xy}{st} = \frac{\pi}{u}$ for some $\pi \in p$ and $u \in S$. Thus $(xyu - st\pi)v = 0$ for some $v \in S$. Hence $xyuv = st\pi v$, so $xyuv \in p$. Thus $xy \in P$ since $u, v \in S$ implies $uv \in S$, so $uv \notin P$. Thus x or y is in p. So $\frac{x}{s} \in S^{-1}P$ and $\frac{y}{t} \in S^{-1}P$. Also $S^{-1}p \neq S^{-1}A$ as p does not meet S. So the ideal is prime, i.e. $S^{-1}p \in Y$.
- Fact 3. If $p \in Y$, then $P = S^{-1}(f^{-1}(p))$.

- Fact 4. If $p \in X$, then $f^{-1}(S^{-1}p) = p$.

  $f^{-1}(S^{-1}p) = \{x \in A : \frac{x}{1} \in S^{-1}p\}$. It's clear that $p \subseteq f^{-1}(S^{-1}p)$. Conversely, if $x \in f^{-1}(S^{-1}p)$, then $\frac{x}{1} \in S^{-1}p$, so $\frac{x}{1} = \frac{\pi}{u}$ for some $\pi \in p$ and $u \in S$. Thus $(xu - \pi)t = 0$ for some $t \in S$. Hence $xut \in p$. But $ut \in S$ and p doesn't meet S, so $ut \notin p$. Thus since p is prime $x \in p$.

■

Suppose $q \subseteq p$, both prime, then $(A/q)_{\overline{p}} \cong A_p/q_p$.

5 Modules

Definition. If K is a field, a vector space V over K is an abelian group under addition together with scalar multiplication from K and for all $a, b \in K$ and $x, y \in V$:

- $a(x + y) = ax + ay$
- $(a + b)x = ax + bx$
- $(ab)x = a(bx)$
- $1x = x = x1$

A **module** is a generalization where the scalars can come from any ring. Equivalently, a module is an abelian group M together ring A and a ring homomorphism, $\varphi : A \to \mathrm{End}(M)$ ($a \mapsto \phi_a$ where $\phi_a(x) = ax$).

Examples.

- A is an A-module. The submodules are the ideals of A.
- $A =$ field, then an A-module is a vector space.
- Every $\mathbb{Z}$-module is an abelian group.
- $K =$ field and $A = K[x]$. An A-module is a K-vector space with a linear map.
- $K =$ field and B is a vector space, $A =$ all linear maps $B \to B$. Then A is a non-commutative ring under $+$ and $\circ$. Then B is an A-module.
- $G =$ finite group under $\times$. A k representation of a finite group G is a $k[G]$-module, or equivalently, a group homomorphism $G \to \mathrm{Aut}_k(V)$ for

> a k-vector space V, or equivalently, a k-vector space V together with an action of G on V that commutes with scalar multiplication and satisfies $g(g'v) = (gg')v$ and $\lambda(gv) = g(\lambda v)$ and $ev = v$.

Definition. A homomorphism of A-modules is a map $f : M \to M'$ that is a homomorphism of the underlying abelian groups and $f(ax) = af(x)$ for all $a \in A$ and $x \in M$. Note $\hom_A(M, N)$, the set of all A-module homomorphisms $M \to N$, is itself an A-module, where $(f + g)(x) = f(x) + g(x)$ and $(af)(x) = a(f(x))$. Note A can be considered as a module over itself, then $\hom_A(A, M) \cong M$ under the map $f \mapsto f(1)$.

Facts.

If $U : M' \to M$ is a module homomorphism, this induces a homomorphism $\overline{U}$: $\hom(M, N) \to \hom(M', N)$ given by $f \mapsto f \circ u$. Also $V : N \to N'$ induces a homomorphism $\overline{V} : \hom(M, N) \to \hom(M, N')$, given by $f \mapsto v \circ f$.

Proposition 5.1. The sequence of A-modules $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact iff for all A-modules N, $0 \to \hom(M'', N) \xrightarrow{\overline{g}} \hom(M, N) \xrightarrow{\overline{f}} \hom(M', N)$ is exact.

The sequence $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ is exact iff for all A-modules M, the sequence $0 \to \hom(M, N') \xrightarrow{\overline{f}} \hom(M, N) \xrightarrow{\overline{g}} \hom(M, N'')$ is exact.

Note. To check if N is a submodule of M we need to check:

- closed under addition
- closed under scalar multiplication.

$\mathbb{Q}$ is a $\mathbb{Z}$-module with no maximal proper submodule.

Definition. Suppose M is a module with submodule M'. Define M/M'. It is an abelian group and $a\overline{x} = \overline{ax}$. Check $\overline{x} = \overline{y}$, then $x - y \in M'$, so $ax - ay \in A'$, so $\overline{ax} = \overline{ax}$.

$f : M \to N$ homomorphism. $\ker(f)$ is a submodule of M. Image(f) is a submodule of N. $\operatorname{coker}(f) = N/\operatorname{Im}(f)$.

If M is an A-module with submodules N, P,

- $N \cap P$ and $N + P$ are submodules
- NP is not necessarily a submodule.

If M is an A-module and I is an ideal in A, then $IM = \{\sum_{i=1}^{n} a_i x_i : a_i \in I, x_i \in M\}$.

Definition. Let M be an A-module. $\operatorname{Ann}(M) = \{a \in A : ax = 0, \forall x \in M\} = (0 : M)$ is an ideal in A. More generally, if N, P are submodules of $(N : P) = \{a \in A : aP \subseteq N\}$.

If M is an A-module, then M is an $A/\operatorname{Ann}(M)$-module. (Define $\overline{a}x = ax$. Well-defined because if $\overline{a} = \overline{b}$, then $a - b \in \operatorname{Ann}(M)$. So $ax = bx$ for all $x \in M$). Similarly, if $I \subseteq \operatorname{Ann}(M)$, then M is an A/I-module.

M is a **faithful** A-module iff $\operatorname{Ann}(M) = 0$. If $x \in M$, M is an A-module, then the **principal submodule generated by** x is $Ax = \{ax : a \in A\}$. M is said to be **finitely-generated** as an A-module if there exists $x_1, \ldots, x_n$ such that $M = Ax_1 + \ldots + Ax_n$. If the linear combination is unique, then M is a **free module** generated by $x_1, \ldots, x_n$ (equivalently, $M = \oplus Ax_i$ and $\operatorname{Ann}(x_i) = 0$). A **(free)** $\mathbb{Z}$**-module** is a (free) abelian group.

e.g. $A[x]$ as an A-module is isomorphic to $\oplus_n Ax^n$. It is a free A-module with basis $\{1, x, x^1, \ldots\}$.

$\prod_n Ax^n$ is isomorphic to the A-module of formal power series.

Theorem 5.2: Nakayama Let M be a finitely-generated A-module such that $I \subseteq \mathcal{J} = \bigcap_{\mathfrak{m} \subset A\text{: maximal}} \mathfrak{m}$ (Jacobson radical). Then $IM = M$ implies $M = 0$.

Proof. Let $u_1, \ldots, u_n$ be a minimal set of generators for M. Assume $IM = M$ for $I \subseteq \mathcal{J}$. In particular, $u_n \in M$ implies $u_n \in IM$. So

$$u_n = \sum_{i=1}^{n} a_i u_i, a_i \in I.$$

Thus

$$u_n(1 - a_n) = \sum_{i=1}^{n-1} a_i u_i.$$

By hypothesis, $a_n \in \mathfrak{m}$ for all maximal ideals $\mathfrak{m}$. Therefore, $1 - a_n \notin \mathfrak{m}$ for any maximal ideal $\mathfrak{m}$. Thus $1 - a_n$ is a unit in A. So

$$u_n = \sum_{i=1}^{n-1} b_1 u_i,$$

a contradiction. ■

Corollary. Let M be a f.g. A-module and $N \subseteq M$ be a submodule. Suppose $I \subseteq \mathcal{J}$. If $M = IM + N$, then $M = N$.

Proof. We know M/N is finitely-generated. $I(M/N) = (IM + N)/N = M/N$, by hypothesis. Therefore, $I(M/N) = (M/N)$, so $M/N = 0$, hence $M = N$. ∎

Special Case: A is local ring. Then $\mathcal{J} = \mathfrak{m}$ is the set of non-units. $A/\mathfrak{m} = k$ is a field. Suppose $M \neq 0$ is a f.g. A-module. Then $M/\mathfrak{m}M$ is an $A/\operatorname{Ann}(M/\mathfrak{m}M)$-module $=$ $A/\mathfrak{m}$-module $=$ k-vector space.

Suppose $x_1, \dots, x_n$ is a set of generators for M. Then $\{\overline{x_1}, \dots, \overline{x_n}\}$ span $M/\mathfrak{m}M$ as a k-vector space.

Proposition 5.3. Let A be a local ring with maximal ideal $\mathfrak{m}$. Let M be a f.g. A-module. Then $M/\mathfrak{m}M$ is a finite-dimensional vector space of $k = A/\mathfrak{m}$. Let $x_1, \dots, x_n \in M$ whose images in $M/\mathfrak{m}M$ span $M/\mathfrak{m}M$ as a k-vector space. Then $\{x_1, \dots, x_n\}$ generate M as an A-module.

Proof. Let N be the submodule of M generated by $\{x_1, \dots, x_n\}$. Then $\varphi : N \hookrightarrow M \twoheadrightarrow M/\mathfrak{m}M$ is onto by hypothesis. This implies $N + \mathfrak{m}M = M$ (anything in M differs from N by something in $\ker\varphi$). By the corollary above, $M = N$. ∎

Special Case: A is a local Noetherian ring and $M = m$ maximal ideal (so m is f.g.). Apply previous result to $M/mM = m/m^2$ a k-vector space ($k = A/m$).

Definition. Zariski tangent dimension (ZTD) is $\dim_k(m/m^2)$.

Suppose $\mathrm{ZTD}(A) = 0$. Then $m/m^2 = 0$, so $m = m^2$. By Nakayama, $m = 0$, hence A is a field.

Suppose $\mathrm{ZTD}(A) = 1$. Then $\dim_k(m/m^2) = 1$. Thus m/m^2 is generated by $\overline{x}$ for some $x \in A$. Thus m is generated by x (prop 5.3).

Suppose $\mathrm{ZTD}(A) = 2$. Then m/m^2 is generated by $\overline{x}, \overline{y}$ as a k-vector space for some $x, y \in A$, but is not generated by a single element. So m is generated by x, y.

Equivalently, $\mathrm{ZTD}(A)$ is the minimal number of generators of m (when A is local, Noetherian).

6 Artinian & Noetherian Rings

Let Σ be a partially ordered set by $\leq$. TFAE:

- Every chain $x_1 \leq x_2 \leq \dots$ must stabilize.

- Every nonempty subset of Σ has a maximal element.

Proof. $(1 \to 2)$. If 2 is false, there exists a non-empty subset of Σ with no maximal element. Thus we get a chain that never stabilizes.

$(2 \to 1)$. By assumption, every chain $x_1 \leq x_2 \leq \dots$ has a maximal element, so it must stabilize. ■

Example. M is an A-module and Σ is the set of all submodules of M. If we order Σ by $\subseteq$, we call this the **Noetherian condition** or the **Accending chain condition (ACC)** or the **maximality property**.

If we order Σ by $\supseteq$, this is called the **Artinian property**/descending chain condition/minimality property.

Definition. If A is a commutative ring which when viewed as an A-module is **Noetherian**, then we say A is a Noetherian ring, i.e. the ideals of A satisfy ACC or equivalently the maximality property.

An **Artin ring** is one in which ideals satisfy DCC or minimality property.

Artin module does not imply Noetherian module. But Artin rings are all Noetherian.

Proposition 6.1. Let A be a Noetherian ring. Then any ideal of A contains a product of prime ideals.

Proof. Let Σ be the set of ideal in A that do not contain products of prime ideals. Assume $\Sigma \neq \varnothing$. Since A is Noetherian and Σ is nonempty, Σ has a maximal element, I. Then I cannot be prime, as $I \in \Sigma$. There exists $a, b \in A$ such that $a, b \notin I$ but $ab \in I$. Then $I + (a)$ and $I + (b)$ properly contain I, so neither can be in Σ. Thus both contain a product of prime ideals. Consider $(I + (a))(I + (b)) \subseteq I + (ab) \subseteq I$ as $ab \in I$. When combined with the fact that $I + (a)$ and $I + (b)$ both contain a product of prime ideals, it follows that I contains a product of prime ideals, a contradiction. ■

Corollary. In a Noetherian ring, the zero ideal is a product of prime ideals.

Corollary. In a Noetherian ring, in which all primes are maximal, (0) is a product of maximal ideals.

Proposition 6.2. Any Artin integral domain is a field.

Proposition 6.3. Let A be an Artin integral domain. Let $0 \neq x \in A$. Then $(x) \supseteq (x^2) \subseteq \ldots$. By DCC, $(x^n) = (x^{n+1})$ for some n. Hence $x^n = ax^{n+1}$ for some $a \in A$. Thus, $x^n = (ax)x^n$. Since we're in an integral domain, $x \neq 0$, implies $x^n \neq 0$. Thus $ax = 1$, i.e. x is a unit.

Proposition 6.4. *M is a Noetherian A-module iff all submodules are f.g. (Noetherian ring iff all ideals are f.g.)*

Proof. Assume M is a Noetherian A-module. Let N be a submodule. Let Σ be the set of all finitely-generated submodules of N. Clearly, $\Sigma \neq \varnothing$. So Σ has a maximal element, N_0. Let $x \in N$ such that $x \notin N_0$. Then $N_0 + Ax$ strictly contains N_0, is contained in N, and is still finitely-generated, a contradiction. Thus $N = N_0$.

Conversely, suppose every submodule of M is f.g. Let $M_1 \subseteq M_2 \subseteq \ldots$ be a chain of submodules of M. Note $\bigcup M_i$ is a submodule of M, so by hypothesis, it is f.g., say it equals $Ax_1 + \ldots + Ax_s$. Some M_j must contain all x_i. It follows that the chain must stabilize after j. ■

Example.

- Any finite abelian group is Noetherian/Artinian as a $\mathbb{Z}$-module. (More generally, any A-module with a finite number of submodules)
- Any finite dimensional k-vector space considered as a k-module is Noetherian/Artinian.
- $\mathbb{Z}$ is a Noetherian ring (becuase it's a PID) but not an Artin ring.
- G subgroup of $\mathbb{Q}/\mathbb{Z}$ consisting of all elements whose orders are a power of p. The only subgroups of G are $G_0 = \mathbb{Z}/\mathbb{Z}$, $G_1 = (\frac{1}{p}\mathbb{Z})/\mathbb{Z}$, $G_2 = (\frac{1}{p^2}\mathbb{Z})/\mathbb{Z}$, etc. This has DCC, but no ACC, so it's **Artinian as a $\mathbb{Z}$-module, but not a Noetherian $\mathbb{Z}$-module.**
- $H = \{\frac{a}{p^n} : a \in \mathbb{Z}, n \geq 0\} \subseteq \mathbb{Q}$ as a $\mathbb{Z}$-module. This time, $H_0 = \mathbb{Z}$, $H_1 = \frac{1}{p}\mathbb{Z}$, etc. No ACC and no DCC (as H_0 isn't Artin).

  We have $0 \to \mathbb{Z} \to H \to G \to 0$ is exact.
- If k is a field, $k[x_1, \ldots, x_n]$ is a Noetherian ring. (Not Artin b/c ID not a field)
- $k[x_1, x_2, \ldots]$ is a non-Noetherian ring nor is it Artin.
- $\mathbb{Z}^n$ is Noetherian/non-Artin ring. $\mathbb{Z}^\infty$ is non-Noetherian/non-Artin ring.

Proposition 6.5. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of A-modules. Then M is Noetherian (resp. Artinian) [NRA] iff M' and M'' are NRA.

Proof. Suppose M is Noetherian. Clear M' is Noetherian, as any submodule of M' will also be a submodule of M. So if submodules of M satisfy ACC, so do submodules of M'. Also any submodule of $M'' \cong M/M'$ lifts back to gives a submodule of M.

Assume M' and M'' are Noetherian. Let $M_1 \subseteq M_2 \ldots$ be a chain of submodules of M. We want to show this stabilizes. Let $M_i' = M_i \cap M'$. So $M_1' \subseteq M_2' \ldots$ is an ascending chain of submodules of M'. Also a chain $M_1/M_1 \cap M' \subseteq M_2 \subseteq M_2 \cap M' \ldots$ is an ascending chain of M''. We have containment because

$$M_1 \to M_2 \to M_2/M_2 \cap M'$$

has kernel $M_1 \cap M'$. By hypothesis both M', M'' have ACC, i.e. there exists n such that both sequences stabilize after n.

As $M_n/M_n \cap M' = M_{n+1}/M_{n+1} \cap M'$ and $M_n \cap M' = M_{n+1} \cap M'$. This implies $M_n = M_{n+1}$ as view, $M_n \cap M', M_{n+1} \cap M'$ as the kernel of a homomorphism where M_n and M_{n+1} both contain the kernel. They have the same image after modding out by kernel.

They must be equal by the one-to-one correspondence b/w submodules of $M_n/M_n \cap M'$ and submodules of M_n containing the kernel. ■

Corollary. Submodules and factor modules of NRA modules are NRA.

Warning. Subrings of Noetherian rings aren't necessarily Noetherian, e.g. $k[x_1, x_2, \ldots] \subset k(x_1, x_2, \ldots,)$.

Corollary. A finite direct sum of NRA A-modules is NRA.

Proof. By induction, it suffices to show the $n = 2$ case. Say $M_1 \oplus M_2$ where M_1, M_2 are NRA. The sequence

$$0 \to M_1 \hookrightarrow M_1 \oplus M_2 \twoheadrightarrow M_2 \to 0$$

is exact. ■

Proposition 6.6. Finite direct product of NRA rings is NRA.

Proof. Let A, B be Noetherian rings. Then any ideal in $A \times B$ is of the form $I \times J$ for I and ideal in A and J an ideal in B. So let $I_1 \times J_1 \subseteq \ldots$ be an increasing chain of ideals in $A \times B$. Then $I_1 \subseteq I_2 \ldots$ and $J_1 \subseteq J_2 \ldots$ both stabilize, so the direct product sequence stabilizes too. ■

Corollary. If A is an NRA ring and M is a finitely-generated A-module, then M is an NRA A-module. (In fact, A Noetherian ring, M f.g. A-module iff M is contained in a f.g. A-module)

Proof. Any f.g. A-module equals a factor module of $A \oplus \ldots \oplus A$. So A NRA ring, implies A^n is NRA as an A-module and any factor of A^n is a NRA A-module. ∎

Fact. If A Noetherian ring, any submodule of a f.g. module is f.g. *Note:* This is not true if A isn't Noetherian, e.g. view A as an A-module, it's f.g. as an A-module by $\{1\}$, but A isn't Noetherian.

Corollary. Let A be a Noetherian ring, B a ring containing A. View B as an A-module. Suppose B is contained in a f.g. A-module, then B is a Noetherian ring.

Proof. By the above fact, we have that B is a f.g. A-module. Thus B is a Noetherian A-module, by the corollary above. So B is Noetherian when considered as a B-module (as sub-B-modules are sub-A-modules). Hence B is a Noetherian ring. ∎

Converse isn't true. $B = \mathbb{Z}[x]$ is a Noetherian ring, i.e. it is a Noetherian B-module, but not a Noetherian $\mathbb{Z}$-module.

Fact. A is NRA ring and $I \subseteq A$ ideal implies A/I is NRA ring.

Proof. Let $I_1 \subseteq \ldots$ be an ascending chain of ideals in A/I. Lift them back to form an increasing chain of ideals in A. As A is Noetherian, this chain stabilizes, so the original must also. ∎

Corollary. If A is an Artin ring and $I \subseteq A$ is a prime ideal. Then A/I is a field, i.e. I is maximal.

Proposition 6.7. Let V be a vector space over the field k. TFAE

- V is finite-dimension
- Subspaces satisfy ACC
- Subspaces satisfy DCC.

Proof. Clearly $1 \to 2$ and $1 \to 3$. Assume $\neg 1$, i.e. V is infinite-dimensional. Then there exists a set $S = \{x_1, \ldots\}$ that is linearly independent over k. Then $\langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \ldots$ is a non-stabilizing ascending sequence and $\langle S \rangle \supsetneq \langle S - x_1 \rangle \ldots$ is a non-stabilizing descending sequence. ∎

Proposition 6.8. If A is a commutative ring with $1 \neq 0$ in which $(0) = m_1 \dots m_n$ is a product of maximal ideals. Then A is a Noetherian ring iff A is an Artin ring.

Proof. Recall in a Noeth. ring, all ideals contain a product of prime ideals. Thus, in a NR, (0) equals the product of prime ideals. Thus, in a NR in which all primes are maximal, (0) is the product of maximal ideals.

- Suppose $M = M_1 \supseteq M_2 \supseteq \dots \supseteq M_n = 0$ is a sequence of submodules of an A-module M. Then M has ACC (resp. DCC) iff each of the factor modules M_i/M_{i+1} has ACC (resp. DCC).

  Proof. Suppose M has ACC. Then M is a Noeth. A-module. So all submodules are Noeth., hence all factor modules of submodules are Noeth.

  Conversely, assume all M_i/M_{i+1} are Noeth. $M_n = 0$ and by hypothesis $M_{n-1}/M_n \cong M_{n-1}$ is Noeth. Then $0 \to M_{n-1} \to M_{n-2} \to M_{n-2}/M_{n-1} \to 0$ is exact and M_{n-1} and M_{n-2}/M_{n-1} are Noeth, so M_{n-2} is Noeth. Continuing in this way we get each M_i is Noeth. Hence $M_1 = M$ is Noeth. □

- Let M be an A-module. Then M has ACC (resp. DCC) as an A-module iff M has ACC (resp. DCC) as an $A/\operatorname{Ann}(M)$-module.

Consider $M = A \supseteq m_1 \supseteq m_1m_2 \supseteq \dots \supseteq m_1 \dots m_n = 0$. A Noetherian ring iff A is Noetherian A-module iff each $M_i = m_1 \dots m_i / m_1 \dots m_{i+1}$ is a Noetherian A-module iff each M_i is a Noetherian A/m_{i+1}-module ($\operatorname{Ann}(M_i) = m_{i+1}$) iff each of the M_i is Noetherian as a A/m_{i+1}-vector space iff each of the M_i is Artin as a A/m_{i+1}-vector space iff each of the M_i is Artin as an A-module iff A is Artin as an A-module iff A is an Artin ring. ■

- In an Artin ring, all primes are maximal. *Proof.* A/p is an Artin ID, hence a field. Thus p is maximal.

- An Artin ring has a finite number of maximal ideals.

  Proof. Let Σ be the set of all ideals that can be written as a finite intersection of maximal ideals. Σ is clearly nonempty. So Σ has a minimal element, $\mathfrak{m} = m_1 \cap \dots \cap m_n$. Suffices to show m_i are all the maximal ideals. Let m be an arbitrary maximal ideal. Note $\mathfrak{m} \cap m \in \Sigma$ and $\mathfrak{m} \cap m \subseteq \mathfrak{m}$. By minimality, $\mathfrak{m} = \mathfrak{m} \cap m$. So $\mathfrak{m} \subseteq m$. By the homework, $m_i \subseteq m$ for some i. As m_i is maximal, so $m = m_i$. ■

- Let A be a commutative ring with $1 \neq 0$. Let $\mathcal{N} = \{x \in A : x^n = 0 \text{ for some } n\}$ (**nilradical**). Then $\mathcal{N} = \bigcap_{\text{prime}} \mathfrak{p}$.

Proof. If $x \in \mathcal{N}$, then $x^n = 0$, so $x^n \in \mathfrak{p}$, implies $x \in \mathfrak{p}$.

Conversely, assume $x \notin \mathcal{N}$, i.e. $x^n \neq 0$ for any n. Let Σ be the set of ideals of A not containing any power of x. Σ is nonempty as $(0) \in \Sigma$. By Zorn's lemma, Σ has a maximal element, J. Suffices to show J is a prime ideal. Suppose not, then there exists $a, b \in A$ such that $a, b \notin J$ but $ab \in J$. Then $J + (a)$, $J + (b)$ properly contain J. As J is maximal, it follows these aren't in Σ. Hence they both contain a power of x. Thus $(J + (a))(J + (b)) \subseteq J + (ab) \subseteq J$ contains a power of x, a contradiction. ∎

Proof. Let $S = \{1, x, x^2, \dots\}$. S is a MCS. Then $S^{-1}A \neq 0$, so it contains a maximal (hence prime) ideal. Thus there exists a prime ideal of A disjoint from S. ∎

- In an Artin ring, $\mathcal{N}^k = (0)$.

Proof. $\mathcal{N} \supseteq \mathcal{N}^2 \supseteq \dots$ is descending, so by DCC, $I = \mathcal{N}^k = \mathcal{N}^{k+1}$. Assume $I \neq 0$. Let Σ be the set of ideals $\mathcal{I} \subseteq A$ such that $\mathcal{I}I \neq 0$. Σ is nonempty as $I \in \Sigma$. So Σ has a minimal element, J. There exists $x \in J$ such that $(x)I \neq 0$. Then $(x) \subseteq J$ and $(x) \in \Sigma$, so $J = (x)$. Note $(x)II = (x)I \neq 0$, so $(x)I \in \Sigma$ and $(x)I \subseteq J$. Thus $J = (x)I$. Thus $x = xy$ for some $y \in I$. Thus $x = xy = xy^2 = \dots$. Since $y \in I \subseteq \mathcal{N}$, some power of y is 0. Hence $x = 0$, a contradiction.

∎

- Thus in an Artin ring, $\mathcal{N}^k = (0)$ and $\mathcal{N} = m_1 \cap m_n$ (as finitely many maximal ideals and all primes are maximal). The m_i are pairwise coprime. Thus $\mathcal{N} = m_1 m_2 \dots m_n$, so $\mathcal{N}^k = (m_1 \dots m_n)^k$, the product of maximal ideals. (0) **is the product of maximal ideals in** A**. Hence Artin ring implies Noetherian ring.**
- In an Artin local ring, $(0) = m^n$.
- Any Artin ring is a finite direct product of Artin local rings. Unique up to isomorphism/rearranging.
- Powers of distinct maximal ideals are coprime.
- In an Artin local ring, let d be the smallest integer such that $m^d = 0$. Let e be the stabilization point of $m \supset m^2 \dots$. Then $e = d$.

  Not necessarily true in non-local rings. $(0) = \prod m_i^{k_i}$ (k_i as small as possible). Choose e_i analogously. We have $e_i = d_i$.

Contents