

PCMI

ISAIAH DAILEY

CONTENTS

1. Groups	1
2. Exercises	13

1. GROUPS

Definition 1.1. A *semigroup* is a set with an associative operation. A *monoid* is a semigroup with an identity element. A *group* is a monoid with inverses. An *abelian* group is a commutative group.

Definition 1.2. For $n \geq 3$, write D_{2n} for the dihedral group of order $2n$ with presentation $\langle r, s \mid r^n, s^2, rsrs^{-1} \rangle$. The elements of D_{2n} are $e, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}$.

Definition 1.3. The quaternions group Q_8 has elements $\pm 1, \pm i, \pm j, \pm k$ with group structure given by

$$-1 \cdot x = -x \quad \forall x \in Q_8, \quad (-1)^2 = 1, \quad ij = k, \quad jk = i, \quad ki = j.$$

Definition 1.4. A subset H of a group G is a *subgroup* if H is nonempty and $xy^{-1} \in H$ whenever $x, y \in H$.

Definition 1.5. The *special linear group* of a field F is the subgroup $SL_n(F) \subseteq GL_n(F)$ of matrices A with $\det A = 1$.

Definition 1.6. The *alternating group* in n elements is the subgroup $A_n \leq S_n$ consisting of even permutations.¹ A_n has order $n!/2$.

Definition 1.7. Let $H \leq G$ be a subgroup, then we write G/H (resp. $H \backslash G$) for the set of left (resp. right) cosets of H in G .

Proposition 1.8. Let $H \leq G$.

- (1) For any $x, y \in G$, there is a bijection $xH \rightarrow yH$ given by $xh \mapsto yh$.
- (2) For any $x \in G$, there is a bijection $xH \rightarrow Hx^{-1}$ defined by $xh \mapsto h^{-1}x^{-1}$.
- (3) There is a bijection $G/H \rightarrow H \backslash G$ given by $xH \mapsto Hx^{-1}$.

Definition 1.9. Given a subgroup H of a group G , we define the index of H in G to be the quantity $|G : H| := |G/H| = |H \backslash G|$.

Proposition 1.10. Given a subgroup $H \leq G$, we have $|G| = |G : H| \cdot |H|$. More generally, if $K \leq H \leq G$, we have $|G : K| = |G : H| \cdot |H : K|$.

Date: July 19, 2024.

¹A permutation $\sigma \in S_n$ is said to be *even* if σ can be written as a composition of an even number of two-element swaps.

Theorem 1.11 (Lagrange's Theorem). *If G is a finite group and $H \leq G$, then $|H|$ and $|G : H|$ divide $|G|$. In particular, $|g| := |\langle g \rangle|$ divides $|G|$ for all $g \in G$.*

As a consequence of Lagrange's theorem, if $|G|$ is prime then G is cyclic.

Example 1.12. S_3 and D_6 are isomorphic, given by $\phi : D_6 \rightarrow S_3$ given by $\phi(r) = (1\ 2\ 3)$ and $\phi(s) = (1\ 2)$.

Definition 1.13. A subgroup $H \leq G$ is said to be *normal* if $xHx^{-1} = H$ for all $x \in G$, equivalently, if $xH = Hx$ for all $x \in G$. We write $H \trianglelefteq G$ to mean H is a normal subgroup of G .

Warning 1.14. The relation \trianglelefteq is NOT a transitive relation on subgroups!

Definition 1.15. If $H \trianglelefteq G$, then G/H becomes a group by the operation $xH \cdot yH = xyH$.

Proposition 1.16. *A subgroup $H \leq G$ is normal iff it is the kernel of some homomorphism.*

Proposition 1.17. *Let G be a group with subgroups $A, B \leq G$, then their intersection $A \cap B$ is also a subgroup.*

Definition 1.18. Let G be a group with subgroups $A, B \leq G$, then define

$$AB := \{ab \in G \mid a \in A, b \in B\}.$$

The set AB is *not* generally a subgroup.

Example 1.19. Consider $G = D_6$ generated by $\{r, s\}$ with $r^3 = s^2 = (sr)^2 = 1$. Let $A = \langle s \rangle$ and $B = \langle sr \rangle$, both subgroups of order 2. Then $AB = \{e, s, sr, r\}$, which is not a subgroup since $r^2 \notin AB$.

Exercise 1.20. Show that AB is a subgroup of G iff $AB = BA$.

Definition 1.21. Given a subset $S \subseteq G$, we write $N_G(S)$ for the *normalizer* of S in G , that is,

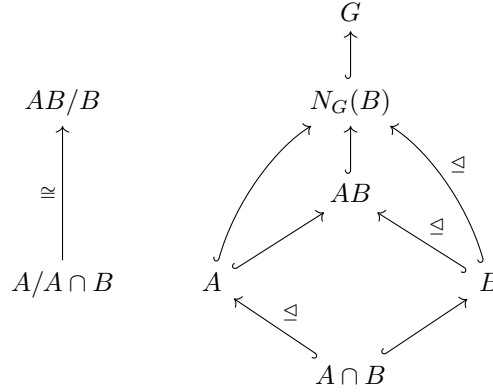
$$N_G(S) := \{g \in G \mid gSg^{-1} = S\}.$$

Proposition 1.22. *Let $S \subseteq G$, then*

- $N_G(S)$ is a subgroup of G .
- If $H \leq G$ is a subgroup, then $H \trianglelefteq N_G(H)$.
- $N_G(H)$ is the “largest” subgroup of G that H is normal inside of.
- $N_G(H) = G$ iff $H \trianglelefteq G$.

Theorem 1.23 (The Second (“Diamond”) Isomorphism Theorem). *Suppose $A, B \leq G$ and $A \leq N_G(B)$. Then*

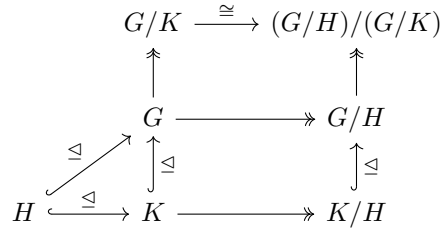
- (1) AB is a subgroup of G (equivalently, $AB = BA$).
- (2) $B \trianglelefteq AB$,
- (3) $A \cap B \trianglelefteq A$,
- (4) $A/(A \cap B) \cong AB/B$.



Corollary 1.24. *If $A \leq G$ and $B \trianglelefteq G$, then AB is a subgroup of G .*

Theorem 1.25 (The Third Isomorphism Theorem). *Let $H, K \trianglelefteq G$ with $H \leq K$. Then*

- (1) $K/H \trianglelefteq G/H$, and
- (2) $G/K \cong (G/H)/(K/H)$ via the assignment $xK \mapsto (xH)\overline{K}$ (where $\overline{K} = K/H \subseteq G/H$).



Intuitively, the following theorem says the following: Let $N \trianglelefteq G$ be a normal subgroup, then the quotient map $\pi : G \twoheadrightarrow G/N$ induces a lattice isomorphism (an inclusion-preserving bijection) between the set of subgroups of G containing N , and the set of subgroups of G/N . Moreover, this isomorphism restricts to an isomorphism on the normal subgroups, and given subgroups $A, B \leq G$ with $N \leq A \cap B$, we have $(A \cap B)/N = (A/N) \cap (B/N)$.

Theorem 1.26 (The Fourth (“Lattice”) Isomorphism Theorem). *Let $N \trianglelefteq G$ be a normal subgroup. Then we have inverse bijections*

$$\{A \leq G \mid N \leq A\} \xleftrightarrow{\sim} \{\overline{A} \leq G/N\}$$

$$A \longmapsto A/N$$

$$\pi^{-1}\overline{A} \longleftarrow \overline{A}$$

where $\pi^{-1}\overline{A} = \{g \in G \mid \pi(g) \in \overline{A}\}$. Furthermore, for $A, B \leq G$ with $N \leq A \cap B$, we have

- (1) $A \leq B$ iff $A/N \leq B/N$.
- (2) If $A \leq B$ then $|B : A| = |B/N : A/N|$.
- (3) $(A \cap B)/N = (A/N) \cap (B/N)$.
- (4) $A \trianglelefteq G$ iff $A/N \trianglelefteq G/N$.

Definition 1.27. A **group presentation** is a pair (S, R) consisting of a set S and a subset $R \subseteq F(S)$ (where $F(S)$ denotes the free group on S). The group *presented* by this data is defined to be

$$\langle S \mid R \rangle := F(S)/N,$$

where N is the *normal closure* of R in $F(S)$, that is, the smallest normal subgroup of $F(S)$ containing R .

Given a group G , we say that (S, R) is a *presentation* of G if there exists an isomorphism $G \cong \langle S \mid R \rangle$ of groups. We say that G is *finitely presentable* if it has a presentation (S, R) , where S and R are both finite.

Example 1.28. The dihedral group D_{2n} of order $2n$ has presentation $\langle r, s \mid r^n, s^2, sr sr \rangle$.

Proposition 1.29. For $n \geq 1$, we have

$$S_n \cong \langle s_1, \dots, s_{n-1} \mid R \rangle,$$

where R consists of the relations

$$\begin{aligned} s_i^2 &= 1, & \text{for } i = 1, \dots, n-1, \\ (s_i s_j)^2 &= 1, & \text{when } |i - j| \geq 2, \\ (s_i s_{i+1})^3 &= 1, & \text{for } i = 1, \dots, n-1. \end{aligned}$$

Definition 1.30. Given an object X in a category \mathcal{C} and a group G , a *left group action* of G on X is a group homomorphism $\phi : G \rightarrow \text{Aut}(X)$, denoted by $G \curvearrowright X$. A *right group action* is a group homomorphism $\phi : G^{\text{op}} \rightarrow \text{Aut}(X)$.

Definition 1.31. A set equipped with a G -action is called a G -set.

Example 1.32. For any object X and group G , the trivial map $G \rightarrow \text{Aut}(X)$ yields the *trivial action* of G on X , in which G simply acts via identities on X .

Example 1.33. Given $H \leq G$, the set G/H of left cosets of H admits a natural G action by

$$g \cdot xH := gxH.$$

Similarly, the set $H \backslash G$ of right cosets of H admits a natural G action by the rule

$$g \cdot Hx := Hxg^{-1}.$$

Example 1.34. Every group acts on itself by conjugation via the map $\text{conj} : G \rightarrow \text{Aut}(G)$ defined by

$$\text{conj}_g(x) := gxg^{-1}.$$

Definition 1.35. Let $\phi : G \rightarrow \text{Aut}(X)$ be a left G -action on an object X .

- (1) The *kernel* of the action is the kernel of the homomorphism ϕ , i.e., it is the set $\{g \in G \mid \phi_g = \text{id}_X\}$.
- (2) The action is *faithful* if the kernel is trivial.

If X is a set, then we have the following further definitions.

- (1) Given $x \in X$, the *stabilizer* of x (denoted by $\text{Stab}(x)$ or just G_x) is the set $\{g \in G \mid g \cdot x = x\}$.
- (2) The action is *free* if all the stabilizers G_x are trivial.

Proposition 1.36. Suppose X is a G -set, and $x, y \in X$ satisfying $y = g \cdot x$ for some $g \in G$. Then

$$G_y = gG_xg^{-1}.$$

Example 1.37. Consider the tautological action of $G = S_n$ on $X = \{1, \dots, n\}$, so the corresponding homomorphism $G \rightarrow \text{Sym}(X)$ is the identity. We have that:

- The kernel of the action is trivial, so it is a faithful action.
- The action is free iff $n \geq 3$.
- If $n > 1$, each G_x is isomorphic to S_{n-1} , but each is a *distinct* subgroup of S_n .
- The G_x are conjugate to each other: if $\sigma \in S_n$ such that $\sigma(x) = y$, then $G_y = \sigma G_x \sigma^{-1}$.

Theorem 1.38 (Cayley's Theorem). *Every group is isomorphic to a subgroup of some permutation group $\text{Sym}(X)$.*

Proof. Given G , it suffices to provide a faithful action on some set X , so that the induced homomorphism $\phi : G \rightarrow \text{Sym}(X)$ is injective, and therefore identifies G with a subgroup of $\text{Sym}(X)$. This is easy: equip $X = G$ with the natural left G action given by $g \cdot x := gx$. Then this action is faithful, since $gx = x$ for all $x \in X$ certainly implies $g = e$. \square

Proposition 1.39. *If G is a finite group and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal. In particular, index 2 subgroups of finite groups are always normal.*

Proof. Let $H \leq G$ be a subgroup of index p , and consider the left action of G on $X = G/H$, which gives a homomorphism $\phi : G \rightarrow \text{Sym}(G/H) \cong S_p$. Let $K = \ker \phi$ of this action. We know K is normal, since it is a kernel, so it suffices to show that $K = H$. Note that clearly $K \leq H$, so it further suffices to show that $|H : K| = 1$. By the first isomorphism theorem, G/K is isomorphic to a subgroup of S_p , so that $|G : K|$ divides $|S_p| = p!$, by Lagrange's theorem. We have that $|G : K| = |G : H||H : K| = p|H : K|$, so $|H : K|$ divides $p!/p = (p-1)(p-2) \cdots 2 \cdot 1$. However, since $|H : K|$ divides $|G|$, we know that no prime smaller than p divides $|H : K|$. Thus $|H : K| = 1$, as desired. \square

Definition 1.40. Consider a group action $G \curvearrowright X$, where X is a set. Define a relation \sim on X by

$$x \sim y \iff \exists g \in G, g \cdot x = y.$$

This is an equivalence relation on X , and the equivalence classes of this relations are called *orbits*. We write $\text{Orb}(x)$, Gx , or $G \cdot x$ for the orbit which contains x , so that $\text{Orb}(x) = \{g \cdot x \mid g \in G\}$.

An action is *transitive* if it has exactly one orbit.

Example 1.41. G acts transitively on G/H .

Theorem 1.42 (The Orbit/Stabilizer Theorem). *Suppose X is a G -set, and $x \in X$. Then there is a bijection*

$$G/\text{Stab}(x) \xrightarrow{\sim} \text{Orb}(x), \quad g\text{Stab}(x) \mapsto g \cdot x.$$

Thus for an orbit \mathcal{O} , we have $|\mathcal{O}| = |G : \text{Stab}(x)|$ for any $x \in \mathcal{O}$.

Corollary 1.43. *Let G act on a finite set X . Then we have*

$$|X| = \sum_{k=1}^r |G : \text{Stab}(x_k)|,$$

where $x_1, \dots, x_r \in X$ are representatives of the orbits of the action (that is, $\text{Orb}(x_i) \cap \text{Orb}(x_j) = \emptyset$ when $i \neq j$, and $\bigcup_{k=1}^r \text{Orb}(x_k) = X$),

Theorem 1.44 (Cauchy's Theorem). *Let G be a finite group. If a prime p divides $|G|$, then G has an element of order p .*

Definition 1.45. A group G is *simple* if its only normal subgroups are $\{e\}$ and G . By convention the trivial group is *not* simple.

Example 1.46. Let p be a prime. Then the cyclic group $G = C_p$ of order p is simple.

Proposition 1.47. *The alternating group A_n on n elements is simple for $n \geq 5$.*

Proof sketch. Elements of A_n are the even permutations, and it is straightforward to check that A_n is also generated by its subset of 3-cycles. Then one checks that any normal subgroup N of A_n which contains some 3-cycle contains every 3-cycle, and therefore satisfies $N = A_n$.

Thus, in order to prove A_n is simple, it suffices to show that if $N \trianglelefteq A_n$ is a non-trivial normal subgroup, it must contain at least one 3-cycle. This is where the assumption that $n \geq 5$ is needed. \square

Example 1.48. The group A_4 is not simple: the subgroup $N = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ generated by the products of disjoint 2-cycles is normal.

Definition 1.49. Consider the conjugation action of G on itself: $\cong_g (x) = gxg^{-1}$.

- The *orbits* for the conjugation action are the conjugacy classes; we denote the conjugacy class of an element $x \in G$ by $\text{Cl}(x) := \{gxg^{-1} : g \in G\}$.
- The *stabilizer* of $x \in G$ under the conjugation action is the *centralizer subgroup* of x :

$$C_G(x) := \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}.$$

- The kernel of the conjugation action is precisely the *center*

$$Z_G := \{g \in G \mid gx = xg \ \forall x \in G\}.$$

- Note that $\text{Cl}(e) = \{e\}$ and $C_G(e) = G$, so that the conjugation action is neither free nor transitive (unless $G = \{e\}$).

Theorem 1.50 (The Class Equation). *For a finite group G , we have*

$$|G| = |Z_G| + \sum_{k=1}^r |G : C_G(g_k)|,$$

where g_1, \dots, g_r are representatives of the distinct conjugacy classes of G not contained in the center Z_G .

Moreover, each term on the right divides $|G|$.

Definition 1.51. Let p be a prime. A p -group is a non-trivial finite group whose order is a power of p .

Proposition 1.52. *Every p -group has a non-trivial center.*

Proof. The class equation for G gives

$$p^d = |Z_G| + \sum_{k=1}^r |G : C_G(g_k)|.$$

Since $C_G(g_k) \neq G$, we have that p divides each $|G : C_G(g_k)|$. Therefore p divides $|Z_G|$. Since $|Z_G| \geq 1$ we may conclude that p divides $|Z_G|$. \square

Corollary 1.53. *If $|G| = p^2$ for some prime p then G is abelian.*

Proof. First we note a general fact: If G/Z_G is cyclic, then G is abelian. To see this, pick $g \in G$ which projects to a generator of G/Z_G . Then every element in G can be written as $g^k x$ for some $k \in \mathbb{Z}$ and $x \in Z_G$. Then every element in G can be written as $g^k x$ for some $k \in \mathbb{Z}$ and $x \in Z_G$. Since $(g^i x)(g^j y) = g^{i+j} xy$ whenever $x, y \in Z_G$, we see that G is abelian.

If $|G| = p^2$, then by the previous result $|Z_G| \in \{p, p^2\}$, whence $|G/Z_G| \in \{1, p\}$ and thus is cyclic. \square

Definition 1.54. Given a group G , the image of the homomorphism $\text{conj} : G \rightarrow \text{Aut}(G)$ is the group

$$\text{Inn}(G) := \{\text{conj}_g \mid g \in G\} \leq \text{Aut}(G),$$

and its elements are called *inner automorphisms* of G . The first isomorphism theorem then gives an isomorphism

$$G/Z_G \cong \text{Inn}(G).$$

Proposition 1.55. $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$.

Definition 1.56. The group of *outer automorphisms* of G is given by the quotient

$$\text{Out}(G) := \text{Aut}(G)/\text{Inn}(G).$$

Definition 1.57. Given a subgroup $H \leq G$, its *centralizer* is the subgroup $C_G(H) := \{g \in G \mid gh = hg \ \forall h \in H\}$.

Proposition 1.58. Let $N \trianglelefteq G$ be a normal subgroup, then the conjugation action of G on N yields a group homomorphism $\kappa : G \rightarrow \text{Aut}(N)$. Then

$$\kappa^{-1}(\text{Inn}(N)) = C_G(N)N,$$

which is a normal subgroup of G .

Remark 1.59. In the language of the above proposition, we know that κ induces an injective homomorphism

$$\bar{\kappa} : G/C_G(N)N \hookrightarrow \text{Out}(N),$$

so any elements of $G \setminus C_G(N)N$ give rise to non-inner automorphisms of N .

Proposition 1.60. $|\text{Aut}(C_n)| = \phi(n)$, where ϕ is the Euler ϕ function for which $\phi(n)$ is the number of integers in $\{1, \dots, n\}$ which are relatively prime to n .

Definition 1.61. A *p-Sylow subgroup* of a finite group G is a subgroup $P \leq G$ which is a p -group, and is such that $|G : P|$ is prime to p . Equivalently, if $G = p^a m$ with $(p, m) = 1$ and $a \geq 1$, then a p -Sylow subgroup is a subgroup of order p^a .

Note: With this convention, the trivial subgroup is not p -Sylow for any prime p .

Write $\text{Syl}_p(G)$ for the set of p -Sylow subgroups of G , and write $n_p(G) := |\text{Syl}_p(G)|$. Note that G acts on $\text{Syl}_p(G)$ by conjugation: if $P \leq G$ is a p -Sylow subgroup, so is gPg^{-1} for any $g \in G$.

In the following three theorems, p will be a chosen prime, and G will be a finite group of order $p^a m$, where $a \geq 1$ and $p \nmid m$.

Theorem 1.62 (Sylow 1). *The group G has a p -Sylow subgroup, i.e., $\text{Syl}_p(G) \neq \emptyset$.*

Theorem 1.63 (Sylow 2). *Any two p -Sylow subgroups of G are conjugate, i.e., G acts transitively on $\text{Syl}_p(G)$ by conjugation.*

Theorem 1.64 (Sylow 3). *If P is any p -Sylow subgroup of G , then $n_p = |G : N_G(P)|$. Furthermore, $n_p \mid m$ and $n_p \equiv 1 \pmod{p}$.*

Lemma 1.65. *Let P, Q be subgroups of a group G with $|P| = p$ and $|Q| = q$ prime and distinct. Further suppose that PQ is a subgroup of G (for example, if $P \subseteq N_G(Q)$ or $Q \subseteq N_G(P)$) and $ab = ba$ for all $a \in P$ and $b \in Q$. Then PQ is isomorphic to the cyclic group C_{pq} of order pq .*

Proof. Since P and Q have prime order, we can write $P = \langle x \rangle$ and $Q = \langle y \rangle$ where $|x| = p$ and $|y| = q$. Set $z = xy$. If $z^k = e$, then $x^k = y^{-k}$ because x and y commute, so that $x^k \in P \cap Q$, which is trivial, since $|P \cap Q|$ has to divide both p and q , which are distinct primes. Hence we must have $x^k = e = y^k$, meaning $|z| = pq$, and we see that PQ is cyclic. \square

Proposition 1.66. *If $p < q$ are primes and $q \not\equiv 1 \pmod{p}$, then every group of order pq is cyclic.*

Proof. By Sylow 3, $n_q|p$ and $n_q \equiv 1 \pmod q$. If $n_q > q$, then $n_q > p$, a contradiction of the fact that $n_q|p$. Hence we must have $n_q = 1$. Let $Q \leq G$ be the unique q -Sylow subgroup of G . Note that since $n_q = 1$ and any conjugate of Q is also a q -Sylow subgroup, we have that Q is a normal subgroup of G . Since $|Q| = q$ is prime, we can write $Q = \langle y \rangle$, where y has order q . Pick any subgroup $P \leq G$ of order p , and write $P = \langle x \rangle$. P acts on Q via conjugation, yielding a map $\kappa : P \rightarrow \text{Aut}(Q)$; the order of $\kappa(P)$ must divide both $|P| = p$ and $|\text{Aut}(Q)| = q - 1$ by Lagrange's, and clearly $|\kappa(P)| \leq |P| = p$, so that $|\kappa(P)| \in \{1, p\}$. Since $q \not\equiv 1 \pmod p$, p does not divide $q - 1$, so that we must have $|\kappa(P)| = 1$, meaning $\kappa(P) = \{e\}$. Therefore $ab = ba$ for all $a \in P$ and $b \in Q$. It then follows by [Proposition 1.39](#) and [Lemma 1.65](#) that PQ is a subgroup of G which is isomorphic to C_{pq} . Since $|G| = pq$, it follows that $G = PQ \cong C_{pq}$, as desired. \square

Proposition 1.67. *If $|G| = 30$, G has unique 3- and 5-Sylow subgroups and contains a normal subgroup isomorphic to C_{15} .*

Proof. By the Sylow theorems, $n_3|10$, $n_3 \equiv 1 \pmod 3$, $n_5|6$, and $n_5 \equiv 1 \pmod 5$. Thus $n_3 \in \{1, 10\}$ and $n_5 \in \{1, 6\}$. If $n_3 = 10$ and $n_5 = 6$, then since each subgroup in Syl_3 and Syl_5 are cyclic of prime order, there would be at least $2 \cdot 10 = 20$ distinct order 3 elements in G , and $4 \cdot 6 = 24$ distinct order 5 elements in G , an impossibility since $|G| = 30 < 44$. Thus, one of n_3 and n_5 is 1. Let $P \in \text{Syl}_3$ and $Q \in \text{Syl}_5$, so that since $n_3 = 1$ or $n_5 = 1$, at least one of P or Q is normal in G , so that by the second isomorphism theorem we know that PQ is a subgroup of G . Moreover, $|PQ| \leq 15$ and 3 and 5 divide $|PQ|$, so we must have $|PQ| = 15$. Thus PQ is an index 2 subgroup of G , so PQ is normal in G . By [Proposition 1.66](#), since $|PQ| = 15 = 3 \cdot 5$ and $5 \not\equiv 1 \pmod 3$, we have that PQ is cyclic, as desired. Sylow 3 directly gives that $n_3(PQ) = n_5(PQ) = 1$, so that P and Q are the unique 5- and 3-Sylow subgroups in PQ . We claim this implies $n_3(G) = n_5(G) = 1$. If we had $n_3(G) = 10$, then G would have at least $2 \cdot 10 = 20$ distinct order 3 elements, so that in particular PQ would have to contain at least 5 elements of order 3, meaning PQ would have to contain at least $\lceil 5/2 \rceil = 3$ subgroups of order 3, a contradiction of the fact that $n_3(PQ) = 1$. A similar argument yields that $n_5(G) = 1$, as desired. \square

Proposition 1.68. *Let G be a group of order 12. If G does not have a normal 3-Sylow subgroup, then $G \cong A_4$.*

Proof. We have that $n_3|4$ and $n_3 \equiv 1 \pmod 3$ by the third Sylow theorem, so either $n_3 = 1$ or $n_3 = 4$. Since G does not have a normal 3-Sylow subgroup, we must have that $n_3 = 4$. The group G acts on $\text{Syl}_3(G)$ by conjugation, yielding a homomorphism

$$\phi : G \rightarrow \text{Sym}(\text{Syl}_3(G)) \cong S_4.$$

First we aim to show this map is injective, so that G is isomorphic to a subgroup of order 12 of S_4 .

If $P \in \text{Syl}_3(G)$, then $|G : N_G(P)| = n_3 = 4$, meaning $|N_G(P)| = 3$, so that $P = N_G(P)$. The kernel of ϕ consists of the elements of g which normalize all 3-Sylow subgroups of G , and so are in the intersection of all 3-Sylow subgroups. This implies $\ker \phi$ is trivial, so ϕ is injective, as desired.

It remains to show that $\phi(G) = A_4$, which can be done in a number of ways. For instance, G must contain exactly 8 elements of order 3, while there are exactly 8 elements of order 3 in S_4 , and they generate A_4 . \square

Proposition 1.69. *Suppose $|G| = 60$ and $n_5(G) > 1$. Then G is simple.*

Proof. By the third Sylow theorem, we have $n_5 \in \{1, 6\}$, so $n_5 = 6$ by assumption. Now, let H be a non-trivial proper normal subgroup of G . We split into cases.

Case 1. If 5 divides $|H|$, then H contains a 5-Sylow subgroup; being normal, it must contain every 5-Sylow subgroup of G . Thus $|H| \geq 1 + 4 \cdot 6 = 25$, so $|H| = 30$. But we have shown above that every group of order 30 has a unique 5-Sylow subgroup, so this is not possible.

Case 2. If 5 does not divide $|H|$, then $|H|$ divides 12. Now we claim that G must contain a normal subgroup of order 3 or 4. If H itself is not of one of these orders, then $|H| = 6$ or $|H| = 12$. If $|H| = 6$ (resp. $|H| = 12$), then Sylow 3 yields $n_3(H) = 1$ (resp. $n_4(H) = 1$), so H admits a normal 3-Sylow subgroup (resp. a normal 4-Sylow subgroup). Since H is normal, it follows that $n_3(G) = 1$ (resp. $n_4(G) = 1$) as well, so indeed G contains a normal subgroup of order 3 or 4, call it K .

Now G/K has order 15 or 20, and in each case Sylow 3 yields $n_5(G/K) = 1$, so G/K has a normal 5-Sylow subgroup. By the fourth (lattice) isomorphism theorem, the preimage of such a 5-Sylow subgroup will be a normal subgroup of G with order divisible by 5, contradicting the above. \square

In general, subgroups of f.g. groups are not f.g.!

Example 1.70. Let $G = F(a, b)$ be the free group on two generators. Write $x_n := a^n b a^{-n} \in G$, and let $H = \langle x_n, n \in \mathbb{Z} \rangle$. Then H is not finitely generated.

Definition 1.71. A poset (P, \leq) has the *ascending chain condition* (*acc*) if, for every countable sequence $(x_k)_{k \in \mathbb{N}}$ with $x_k \leq x_{k+1}$, there exists m such that $x_k = x_m$ for all $k \geq m$.

A group G has the *ascending chain condition for subgroups* if the set of subgroups ordered by inclusion has the acc.

Proposition 1.72. *TFAE*

- (1) G has the acc for subgroups
- (2) All subgroups of G are f.g.

Proposition 1.73. *Let $N \trianglelefteq G$. TFAE*

- (1) G has the acc for subgroups
- (2) Both N and G/N have the acc for subgroups.

Proposition 1.74. *Every f.g. abelian group has the acc for subgroups. In particular, every subgroup of a f.g. abelian group is also f.g.*

Definition 1.75. Let G be a group. We say that an element $a \in G$ is *torsion* if it has finite order, and write $G_{\text{tors}} \subseteq G$ for the subset of torsion elements. A group G is *torsion free* if $G_{\text{tors}} = \{e\}$. A group G is *torsion* if $G_{\text{tors}} = G$.

Proposition 1.76. *If G is an abelian group then G_{tors} is a subgroup of G .*

Proposition 1.77. *If G is abelian, then G/G_{tors} is torsion free.*

Proposition 1.78. *Every f.g. torsion abelian group is finite.*

Proposition 1.79 (Product Recognition). *Let G be a group, and suppose $G_1, \dots, G_n \trianglelefteq G$ are normal subgroups such that*

- (1) $G_1 \cdots G_n = G$, and
- (2) $G_k \cap (G_1 \cdots G_{k-1} G_{k+1} \cdots G_n) = \{e\}$ for $k = 1, \dots, n$.

Then the function

$$\phi : G_1 \times \cdots \times G_n \rightarrow G \quad (g_1, \dots, g_n) \mapsto g_1 \cdots g_n$$

is an isomorphism of groups.

Proposition 1.80. *If $G = G_1 \times \cdots \times G_n$ and $N_k \trianglelefteq G_k$ for $k = 1, \dots, n$, then $N = N_1 \times \cdots \times N_n$ is a normal subgroup of G , and there is an isomorphism*

$$G/N \cong (G_1/N_1) \times \cdots \times (G_n/N_n).$$

Theorem 1.81. *Every f.g. abelian group G is isomorphic to one of the form*

$$G \cong F \times \mathbb{Z}^r, \quad |F| < \infty, \quad \mathbb{Z}^r = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ copies}}, \quad r \geq 0.$$

The factors are unique, in the sense that if G admits two such isomorphisms $G \cong F \times \mathbb{Z}^r \cong F' \times \mathbb{Z}^{r'}$, then $F \cong F'$ and $r = r'$.

Theorem 1.82. *Every finite abelian group G is isomorphic to one of the form*

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

where

- $s \geq 0$, each $n_i \geq 2$, $n_{i+1} \mid n_i$ for all $i = 1, \dots, s-1$.

Furthermore, the decomposition is unique up to isomorphism of the factors.

Definition 1.83. A complete set of invariants for a f.g. abelian group

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

are the free rank r and the list n_1, \dots, n_s of invariant factors. G is finite iff $r = 0$.

Theorem 1.84 (Elementary divisor decomposition). *For every finite abelian group G of order $n = p_1^{a_1} \cdots p_k^{a_k}$, where the $p_1 < \cdots < p_k$ are distinct primes, there is*

- (1) *an isomorphism $G \cong A_1 \times \cdots \times A_k$, with $|A_i| = p_i^{a_i}$ and $a_i \geq 1$, such that*
- (2) *for each A_i , there is an isomorphism*

$$A_i \cong \mathbb{Z}/p_i^{b_{i1}} \times \cdots \times \mathbb{Z}/p_i^{b_{is_i}},$$

with $b_{i1} \geq \cdots \geq b_{is_i}$ and $b_{i1} + \cdots + b_{is_i} = a_i$.

Furthermore, this decomposition is unique, in the sense that if G admits isomorphisms $G \cong B_1 \times \cdots \times B_\ell$ with $|B_i| = q_i^{a_i}$ with q_i prime and $a_j \geq 1$, then $k = \ell$, $p_i = q_i$, and $A_i \cong B_i$.

Definition 1.85. The decomposition described in (1) above is called the *primary decomposition* of G . Part (2) is just giving the invariant factor decomposition of each A_i .

The list of numbers $p_1^{b_{11}}, \dots, p_{ks_k}^{b_{ks_k}}$ are the *elementary divisors* of the group G . The list of elementary divisors is a complete isomorphism invariant of a finite abelian group G .

Definition 1.86. Let H, K, G be groups. We say that G is an *extension* of K by H if there exists a normal subgroup $H' \trianglelefteq G$ and isomorphisms $H \cong H'$ and $K \cong G/H'$, equivalently, an exact sequence of groups

$$0 \rightarrow H \rightarrow G \rightarrow K \rightarrow 0.$$

The extension is *split* if there is additionally a subgroup $K' \leq G$ such that the map $K' \rightarrow G/H'$ sending $x \mapsto xH'$, equivalently, if there is a homomorphism $s : K \rightarrow G$ such that $p \circ s = \text{id}_K$ (in which case $K' = s(K)$).

Example 1.87. Given groups K and H , you can always extend K by H via the *trivial extension*, defined by

$$G := H \times K, \quad H' := H \times \{e\}.$$

The trivial extension is always split, by $K' = \{e\} \times K$.

Example 1.88. Let $H = K = C_2$. Then both $G_1 = C_2 \times C_2$ and $G_2 = C_4$ are extensions of K by H

$$H' := \{e, a\} \trianglelefteq G_1 = C_2 \times C_2 = \langle a \mid a^2 \rangle \times \langle b \mid b^2 \rangle = \{e, a, b, ab\}, \quad G_1/H' = \{\bar{e}, \bar{b}\},$$

and

$$H' = \{e, c^2\} \trianglelefteq G_2 = C_4 = \langle c \mid c^4 \rangle = \{e, c, c^2, c^3\}, \quad G_2/H' = \{\bar{e}, \bar{c}\}.$$

The first extension is split, using $K' = \{e, b\} \leq G_1$, but the second extension is not split.

Definition 1.89. The *extension problem* for groups is to classify, for given H and K , all possible extensions of K by H , up to isomorphism.

Theorem 1.90. Let H, K be groups, and $\alpha : K \rightarrow \text{Aut}(H)$ a homomorphism. Let G be the set $H \times K$, and define a product on G by the rule

$$(h_1, k_1)(h_2, k_2) := (h_1\alpha(k_1)(h_2), k_1k_2).$$

Then we have the following

- (1) G is a group, with identity element (e, e) and inverses $(h, k)^{-1} := (\alpha(k^{-1})(h^{-1}), k^{-1})$.
- (2) The subsets $H' = H \times \{e\}$ and $K' = \{e\} \times K$ are subgroups, and there are isomorphisms $H \xrightarrow{\sim} H'$ and $K \xrightarrow{\sim} K'$ defined by $h \mapsto (h, e)$ and $k \mapsto (e, k)$ respectively.

We now identify H with H' and K with K' via these isomorphisms in the following.

- 3. $H \trianglelefteq G$.
- 4. $H \cap K = \{e\}$ and $G = HK$.
- 5. We have $khk^{-1} = \alpha(k)(h)$ for all $h \in H$ and $k \in K$.

We denote this group G by $H \rtimes K$, or by $H \rtimes_{\alpha} K$ if we want to make the action of K on H explicit.

Example 1.91. Let $H = F(a)$ and $K = \langle b \mid b^2 \rangle$. Let $\phi : K \rightarrow \text{Aut}(H)$ be the homomorphism defined by $\phi(b)(a) = a^{-1}$. We obtain a semi-direct product $G = H \rtimes K$. If we identify H and K with the obvious subgroups of G , this means that

$$G = \{a^n \mid n \in \mathbb{Z}\} \amalg \{a^n b \mid n \in \mathbb{Z}\}, \quad bab^{-1} = a^{-1}.$$

In fact, G is the infinite dihedral group.

Example 1.92. Let $G \subseteq \text{Sym}(\mathbb{R}^n)$ be the set of all functions $\phi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ of the form

$$\phi(x) = Ax + b, \quad A \in \text{GL}_n(\mathbb{R}), \quad b \in \mathbb{R}^n.$$

This can be shown to be a subgroup. It is a semi-direct product of its subgroups

$$H = \{\phi \mid \phi(x) = x + b, b \in \mathbb{R}^n\}, \quad K = \{\phi \mid \phi(x) = Ax, A \in \text{GL}_n(\mathbb{R})\}.$$

Definition 1.93. A *composition series* for a group G is a finite chain of subgroups

$$\{e\} = M_0 \leq M_1 \leq \cdots \leq M_{r-1} \leq M_r = G, \quad r \geq 0,$$

such that

- (1) M_{k-1} is a normal subgroup of M_k , for each $k = 1, \dots, r$, and
- (2) the quotient M_k/M_{k-1} is a simple group.

The groups $M_1/M_0, M_2/M_1, \dots, M_r/M_{r-1}$ are called the *composition factors* of the composition series.

Proposition 1.94. Every finite group has a composition series.

Theorem 1.95 (Jordan-Hölder). Suppose G is a group with a composition series. Then the composition factors of a composition series are unique up to change of permutation. That is, if

$$\{e\} = M_0 \leq \cdots \leq M_r = G, \quad \{e\} = N_0 \leq \cdots \leq N_s = G$$

are two composition series, then $r = s$ and there exists $\sigma \in S_r$ such that $M_k/M_{k-1} \cong N_{\sigma(k)}/M_{\sigma(k)-1}$ for all $k = 1, \dots, n$.

Definition 1.96. A group G is *solvable* if it admits a finite chain of subgroups

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

with each $G_k \trianglelefteq G_{k+1}$, such that each quotient G_k/G_{k-1} is abelian. In particular, a finite group G is solvable if its composition factors are abelian, i.e., all cyclic of prime order.

Definition 1.97. Given elements $x, y \in G$, we write

$$[x, y] := xyx^{-1}y^{-1} \in G$$

for the *commutator* of x and y . For subsets $S, T \subseteq G$, we write

$$[S, T] := \langle [x, y], x \in S, y \in T \rangle$$

for the subgroup generated by such commutators. In particular, the *commutator subgroup* of G is the subgroup $[G, G]$ generated by all commutators.

Remark 1.98. $[G, G]$ is a normal subgroup of G . The quotient group $G/[G, G]$ is abelian, and is called the *abelianization* of G .

Proposition 1.99. If $H \trianglelefteq G$, then G/H is abelian iff $[G, G] \leq H$.

Definition 1.100. The *derived series* of a group G is the sequence of subgroups $G^{(k)}$ defined by

- $G^{(0)} = G$,
- $G^{(1)} = [G, G]$,
- $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$, $k \geq 2$.

We obtain a descending chain of subgroups, each of which is normal in the previous:

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots$$

Proposition 1.101. G is solvable iff $G^{(s)} = \{e\}$ for some s .

Corollary 1.102. If G is solvable, then so is any subgroup or quotient group of G .

Definition 1.103. Given a group G , its *upper central series* is defined by

- $Z_0(G) = \{e\}$,
- $Z_1(G) = Z(G)$,
- $Z_{k+1}(G)$ is the preimage under the quotient map $\pi : G \rightarrow G/Z_k(G)$ of $Z(G/Z_k(G))$, for all $k \geq 1$.

We obtain a possibly infinite sequence of subgroups

$$\{e\} = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq G,$$

each of which is normal in G .

Definition 1.104. A group G is *nilpotent* if there exists a c such that $Z_c(G) = G$. The smallest such c is called the *nilpotence class* of G .

Proposition 1.105. If G is nilpotent, so is any quotient group G/N , and the nilpotence class of G is \geq the nilpotence class of G/N .

Proposition 1.106. $Z_k(G_1 \times \cdots \times G_s) = Z_k(G_1) \times \cdots \times Z_k(G_s)$. In particular, if G_1, \dots, G_s are nilpotent, then so is $G = G_1 \times \cdots \times G_s$.

Proposition 1.107. Let p be a prime and G a p -group of order p^a , $a \geq 1$. Then G is nilpotent, and if $a \geq 2$, it has nilpotence class $\leq a - 1$.

Theorem 1.108. Let G be a finite group with p_1, \dots, p_s the distinct primes dividing its order. Then TFAE.

- (1) G is nilpotent.

- (2) If $H < G$, then $H < N_G(H)$ (i.e., every proper subgroup of G is proper in its normalizer, or equivalently, G is the only subgroup which is its own normalizer).
- (3) $|\text{Syl}_{p_i}(G)| = 1$ for all $i = 1, \dots, s$ (or equivalently, G has a normal p_i -Sylow subgroup for all $i = 1, \dots, s$).
- (4) $G \cong P_1 \times \dots \times P_s$, where $P_i \in \text{Syl}_{p_i}(G)$.

Corollary 1.109. Any finite abelian group is a product of its Sylow subgroups.

2. EXERCISES

Lemma 2.1. Let G be a p -group for some prime p . Then p divides $|Z(G)|$, and in particular $Z(G)$ is nontrivial.

Proof. Since G is a p -group, we may write $|G| = p^a$ for some $a \in \mathbb{N}$, i.e., $a \geq 1$. Then by the class equation, we have that

$$|G| = |Z(G)| + \sum_{j=1}^r [G : C_G(g_j)],$$

where g_1, \dots, g_r are representatives of the conjugacy classes of G , and each $[G : C_G(g_j)]$ is > 1 and divides $|G|$, say $[G : C_G(g_j)] = p^{m_j}$, where $1 < m_j$. Thus, we have

$$p^a = |Z(G)| + \sum_{j=1}^r p^{m_j} \implies |Z(G)| = p^a - \sum_{j=1}^r p^{m_j},$$

and the RHS is clearly divisible by p , so that p divides $|Z(G)|$ as well, yielding the desired result. \square

Lemma 2.2. Let p_1, \dots, p_r be distinct primes, and m_1, \dots, m_r be positive integers. Set $m := p_1^{m_1} \dots p_r^{m_r}$. Then

$$\mathbb{Z}/m \cong \bigoplus_{j=1}^r \mathbb{Z}/p_j^{m_j}.$$

Proof. Let

$$G := \bigoplus_{j=1}^r \mathbb{Z}/p_j^{m_j},$$

and for $j = 1, \dots, r$, let $a_j \in G$ be a generator of the j^{th} summand, so that $|a_j| = p_j^{m_j}$. Let $x := a_1 \dots a_r$, so that

$$|x| = \text{lcm}(a_1, \dots, a_r) = \text{lcm}(p_1^{m_1}, \dots, p_r^{m_r}).$$

Since each of the p_j 's are distinct primes, it follows that $|x| = p_1^{m_1} \dots p_r^{m_r} = m$. Thus G has an element of order $m = |G|$, so G is cyclic of order m , as desired. \square

Lemma 2.3. Let G be a finite group acting on a finite set X , and suppose $x, y \in X$. Then $\text{Orb}(x) = \text{Orb}(y) \iff |\text{Stab}(x)| = |\text{Stab}(y)|$.

Proof. If $|\text{Orb}(x)| = |\text{Orb}(y)|$, then by the Orbit/Stabilizer Theorem we have

$$|\text{Stab}(x)| = |G|/[G : \text{Stab}(x)] = |G|/|\text{Orb}(x)| = |G|/|\text{Orb}(y)| = |G|/[G : \text{Stab}(y)] = |\text{Stab}(y)|.$$

On the other hand, if $|\text{Stab}(x)| = |\text{Stab}(y)|$, we have

$$|\text{Orb}(x)| = [G : \text{Stab}(x)] = |G|/|\text{Stab}(x)| = |G|/|\text{Stab}(y)| = [G : \text{Stab}(y)] = |\text{Orb}(y)|. \quad \square$$

Lemma 2.4 (Burnside's Lemma). *Let G be a finite group acting on a finite set X . Then*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|,$$

where X/G denotes the collection of G -orbits in X , and given $g \in G$, $X^g := \{x \in X \mid g \cdot x = x\}$.

Proof. First of all, note that

$$\sum_{g \in G} |X^g| = |\{(g, x) \in G \times X \mid g \cdot x = x\}| = \sum_{x \in X} |\text{Stab}(x)|,$$

By the Orbit/Stabilizer theorem, we have $|\text{Stab}(x)| = |G|/|\text{Orb}(x)|$, so that

$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{|G|} \sum_{x \in X} \frac{|G|}{|\text{Orb}(x)|} = \sum_{x \in X} \frac{1}{|\text{Orb}(x)|}.$$

Finally, writing X as the disjoint union of its orbits in X/G , we have

$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \sum_{A \in X/G} \sum_{x \in A} \frac{1}{|A|} = \sum_{A \in X/G} 1 = |X/G|. \quad \square$$

Lemma 2.5. *let P and Q be finite groups of coprime order. Then $\text{Aut}(P \times Q) \cong \text{Aut}(P) \times \text{Aut}(Q)$.*

Proof. There is a canonical map

$$\text{Aut}(P) \times \text{Aut}(Q) \rightarrow \text{Aut}(P \times Q)$$

sending a pair (σ, τ) to the automorphism $\sigma \times \tau$ defined by $(\sigma \times \tau)(p, q) = (\sigma(p), \tau(q))$. It is straightforward to verify that $\sigma \times \tau$ is an automorphism of $P \times Q$ and that this assignment is an injective homomorphism. It remains to show the assignment is surjective.

Now, let $x \in P$, and write $\eta(x, e) = (p, q)$, where $p \in P$ and $q \in Q$. Then since η is a homomorphism, we have

$$(e, e) = \eta(e, e) = \eta((x, e)^{|x|}) = (p^{|x|}, q^{|x|}),$$

so that $q^{|x|} = e$. Thus $|q|$ divides $|x|$, say $|x| = n|q|$. By Lagrange's, $|x| = n|q|$ divides $|P|$ and $|q|$ divides $|Q|$, so $|q|$ is a common factor of $|P|$ and $|Q|$. Yet $|P|$ and $|Q|$ are coprime, so it follows that $|q| = 1$, which means $q = e$. Thus we've shown that $\eta(P \times \{e\}) \subseteq P \times \{e\}$. A similar argument yields that $\eta(\{e\} \times Q) \subseteq \{e\} \times Q$. Now let σ and τ denote the compositions which fit into the following diagram

$$\begin{array}{ccccc} P & \hookrightarrow & P \times Q & \hookleftarrow & Q \\ \sigma \downarrow & & \eta \downarrow & & \downarrow \tau \\ P & \twoheadleftarrow & P \times Q & \twoheadrightarrow & Q \end{array}$$

where the top arrows denote the identifications $P \cong P \times \{e\}$ and $Q \cong \{e\} \times Q$. Then given $p \in P$ and $q \in Q$, it follows that

$$\eta(p, q) = \eta(p, e)\eta(e, q) = (\sigma(p), e)(e, \tau(q)) = (\sigma(p), \tau(q)),$$

where the middle equality is where we used the fact that $\eta(P \times \{e\}) \subseteq P \times \{e\}$ and $\eta(\{e\} \times Q) \subseteq \{e\} \times Q$. Thus we've shown that $\eta = \sigma \times \tau$. It is straightforward to see that η is not injective (resp. surjective) unless σ and τ are, so we have shown the desired result. \square

Lemma 2.6. *Suppose G and H are finite groups and p a prime dividing $|G|$ but not $|H|$. Then there is a bijection*

$$\text{Syl}_p(G) \xrightarrow{\sim} \text{Syl}_p(G \times H) \quad \text{given by} \quad K \mapsto K \times \{e\}.$$

In particular $n_p(G) = n_p(G \times H)$.

Proof. Let $K \in \text{Syl}_p(G)$, and identify K with $K \times \{e\} \leq G \times H$. Since p does not divide $|H|$, K is also a p -Sylow subgroup of $G \times H$. Thus by Sylow 2, every p -Sylow subgroup of $G \times H$ is conjugate to K . Clearly any conjugate of $K \times \{e\}$ by an element of $G \times H$ lands in $G \times \{e\}$, so every element of $\text{Syl}_p(G \times H)$ is of the form $L \times \{e\}$ for a unique $L \in \text{Syl}_p(G)$, as desired. \square

Lemma 2.7. *Suppose G is a finite group, p is a prime number, and n is a positive integer. Then there is a bijection*

$$\text{Syl}_p(G) \rightarrow \text{Syl}_p(G \times \mathbb{Z}/p^n) \quad \text{given by} \quad K \mapsto K \times \mathbb{Z}/p^n.$$

In particular $n_p(G) = n_p(G \times \mathbb{Z}/p^n)$.

Proof. Clearly if K is a p -Sylow subgroup of G then $K \times \mathbb{Z}/p^n$ is a p -Sylow subgroup of $H := G \times \mathbb{Z}/p^n$. Thus by Sylow 2 every p -Sylow subgroup of H is a conjugate of $K \times \mathbb{Z}/p^n$, and clearly any conjugate of $K \times \mathbb{Z}/p^n$ is of the form $L \times \mathbb{Z}/p^n$ for some subgroup $L \leq G$ satisfying $|L| = |K|$ (since conjugating $A \times B$ by (a, b) is the same as first conjugating A by a and B by b and then taking their product). \square

1. (May 2022 Q1)

- (a) Let H be a subgroup of a group G . Then G acts on the set $G/H = \{gH \mid g \in G\}$ by left multiplication. This action naturally determines a homomorphism $\alpha : G \rightarrow S(G/H)$, where $S(X)$ is the group of permutations on a set X . Prove that the kernel of α is contained in H .

Proof. If $H = G$ we are done, so suppose H is a proper subgroup of G . Then it suffices to show that if $x \in G \setminus H$, then $x \notin \ker \alpha$. This is clear, as if $x \notin H$, then $xH \neq H$, so that in particular $\alpha(x)(eH) = xH \neq eH$, meaning $\alpha(x)$ is not trivial, so $x \notin \ker \alpha$. \square

- (b) Let L be a subgroup of a finite group K such that $[K : L] = p$, where p is the smallest prime that divides the order $|K|$ of K . Prove that L is normal in K . Hint: Use part (a).

Proof. This is [Proposition 1.39](#). \square

- (c) Describe all finite groups of order p^2 , where p is a prime, up to isomorphism. Prove your answer.

We claim that there are two finite groups of order p^2 : \mathbb{Z}/p^2 and $\mathbb{Z}/p \oplus \mathbb{Z}/p$.

Proof. Since $|G| = p^2$, $|G|$ is abelian ([Corollary 1.53](#)). Now, by the classification theorem for f.g. abelian groups, we can write

$$G \cong \bigoplus_{i=1}^r \mathbb{Z}/p_i^{m_i}$$

for some unique collection of primes p_1, \dots, p_r (not necessarily distinct) and positive integers m_1, \dots, m_r . Given any such decomposition, we must have $p_1^{m_1} \cdots p_r^{m_r} = |G| = p^2$. Then the desired result follows. \square

- (d) Describe all finite groups of order $425 = 25 \cdot 17$ up to isomorphism. Prove your answer.

There are two:

$$\mathbb{Z}/17 \oplus \mathbb{Z}/5 \oplus \mathbb{Z}/5 \quad \text{and} \quad \mathbb{Z}/17 \oplus \mathbb{Z}/25.$$

Proof. Let G be a group of order 425. By the third Sylow theorem, $n_{17} \mid 25$ and $n_{17} \equiv 1 \pmod{17}$, so $n_{17} \in \{1, 5, 25\} \cap \{1, 18, 35, \dots\} = \{1\}$. Similarly, $n_5 \mid 17$ and $n_5 \equiv 1 \pmod{5}$, so that $n_5 \in \{1, 17\} \cap \{1, 6, 11, 16, 21, \dots\} = \{1\}$. Thus G contains precisely one subgroup P of order 17 and one subgroup Q of order 25, and they are both normal by the second Sylow theorem. Moreover, $P \cap Q$ is a subgroup of both P and Q , and $|P \cap Q|$ must divide both 17 and 25, which are coprime, so we must have $|P \cap Q| = 1$, meaning $P \cap Q = \{e\}$. Finally, we have that PQ is a subgroup of G (since Q is normal) by the second isomorphism theorem, and P and Q are both subgroups of PQ , so that 17 and 25 must both divide the order of PQ . Moreover, since $PQ \subseteq G$, we have $|PQ| \leq |G| = 25 \cdot 17$. It follows that $PQ = G$. Thus since P, Q are normal, $P \cap Q = \{e\}$, and $PQ = G$, we have that $G = P \times Q$, by the product recognition theorem ([Proposition 1.79](#)).

Now, since $|P| = 17$ is prime, P is cyclic of order 17. Moreover, since $|Q| = 25 = 5^2$, we showed above that either $Q = \mathbb{Z}/5 \oplus \mathbb{Z}/5$ or $Q = \mathbb{Z}/25$. Thus we are done. \square

2. (May 2022 Q4)

- (a) Let G be a finite subgroup of the multiplicative group K^* of a field K . Prove that G is cyclic.

Proof. First of all, we claim that each Sylow subgroup of G is cyclic. To that end, let P be a p -Sylow subgroup of G (where p is some prime dividing the order of G), and let $a \in P$ have maximal order, say $|a| = m$, so $m = p^n$ for some positive integer n . Then $\{1, a, a^2, \dots, a^{m-1}\}$ are m distinct roots of the polynomial $f := x^m - 1 \in K[x]$, which is of degree m , so they are the only roots of f . Now, let $b \in P$. Then since P is a p -group, b has order p^k for some $k \in \mathbb{Z}_{\geq 0}$. Moreover, by assumption $k \leq n$, so that $b^m = b^{p^n} = (b^{p^k})^{p^{n-k}} = 1$. Thus b is a root of f , meaning $b \in \{1, a, a^2, \dots, a^{m-1}\}$. Our choice of $b \in P$ was arbitrary, and we showed $b \in \langle a \rangle$, so $P = \langle a \rangle$, as desired.

Now, since G is a finite abelian group, it can be written as a product of its Sylow subgroups, each of which we've shown is cyclic. Thus, G can be written as

$$G = \bigoplus_{i=1}^r \mathbb{Z}/p_i^{m_i},$$

where each of the p_i 's are distinct primes (since G is abelian, given a fixed prime p dividing G , each p -Sylow subgroup of G is normal, so by the second Sylow theorem $n_p = 1$), so by [Lemma 2.2](#), G is cyclic, as desired. \square

- (b) Let $k = \mathbb{Z}/p\mathbb{Z}$ be the finite field of order p , p a prime. Let K/k be a finite field extension of degree m . Prove that the elements of K are the roots of the polynomial $X^{p^m} - X$ over k .

Proof. **TODO.** \square

- (c) Prove that every irreducible polynomial $f(x) \in k[x]$ is separable.

Proof. **TODO.** \square

3. (August 2021 Q1) Let G be a non-trivial finite group acting on a finite set X . We assume that for all $g \in G \setminus \{e\}$ there exists a unique $x \in X$ such that $g \cdot x = x$.

- (a) Let $Y = \{x \in X \mid G_x \neq \{e\}\}$, where G_x denotes the stabilizer of x . Show that Y is stable under the action of G .

Proof. Let $y \in Y$ and $g \in G$. Then by [Lemma 2.3](#), since $\text{Orb}(g \cdot y) = \text{Orb}(y)$ (by definition), it follows that $|\text{Stab}(g \cdot y)| = |\text{Stab}(y)| \geq 2$, so that $g \cdot y$ has a nontrivial stabilizer, as desired. \square

- (b) Let y_1, y_2, \dots, y_n be a set of orbit representatives of Y/G (with $|Y/G| = n$), and let $m_i = |G_{y_i}|$. Show that

$$1 - \frac{1}{|G|} = \sum_{i=1}^n \left(1 - \frac{1}{m_i}\right).$$

Proof. Note that $|G|/m_i = |\text{Orb}(y_i)|$ by the Orbit/Stabilizer theorem. Thus

$$|G| \sum_{i=1}^n \left(1 - \frac{1}{m_i}\right) = n|G| - \sum_{i=1}^n \frac{|G|}{m_i} = n|G| - \sum_{i=1}^n |\text{Orb}(y_i)| = n|G| - |Y|.$$

Thus, it suffices to show that

$$|G| - 1 = n|G| - |Y|.$$

This follows by Burnside's Lemma ([Lemma 2.4](#)), as

$$\begin{aligned} n|G| - |Y| &= |Y/G||G| - |Y| \\ &= \sum_{g \in G} |Y^g| - |Y| && (Y^g := \{y \in Y \mid g \cdot y = y\}) \\ &= |Y^e| + \sum_{g \in G \setminus \{e\}} |Y^g| - |Y| \\ &\stackrel{(*)}{=} |Y| + |G \setminus \{e\}| - |Y| \\ &= |G| - 1, \end{aligned}$$

where $(*)$ denotes where we used the assumption that $|Y^g| = 1$ for all $g \in G \setminus \{e\}$. \square

- (c) Show that X has (at least) a fixed point under the action of G .

Proof. By part (ii), we have

$$|G| - 1 = n|G| - |Y|$$

which yields

$$(1) \quad |Y| = (n-1)|G| + 1.$$

We claim that Y has at least $n-1$ orbits of size $|G|$. Assuming this were true, since Y has n orbits and $|Y| = (n-1)|G| + 1$, it would follow that the remaining orbit of Y must have order 1, so that the action of G fixes a point of Y , and therefore a point of X , as desired.

Now, to see the claim, note that the order of each orbit of Y divides $|G|$, so if there were two orbits of size $< |G|$, the sum of their orders would be at most $|G|$, which would yield

$$|Y| \leq |G| + (n-2)|G| = (n-1)|G| < (n-1)|G| + 1,$$

a contradiction of [Equation 1](#), as desired. \square

4. (January 2021 Q1) Let G be a group of order 2057.

- (a) Show that $G \simeq P \times Q$, where P is a group of order 17 and Q is a group of order 121. Determine all groups of order 2057 up to isomorphism.

There are two.

$$\mathbb{Z}/17 \oplus \mathbb{Z}/121 \quad \text{and} \quad \mathbb{Z}/17 \oplus \mathbb{Z}/11 \oplus \mathbb{Z}/11.$$

Proof. Observe that $2057 = 17 \cdot 121 = 17 \cdot 11^2$, and use the exact same argument given in [May 2022, Q1\(d\)](#). \square

- (b) Show that $\text{Aut}(G) \simeq \text{Aut}(P) \times \text{Aut}(Q)$.

Proof. This is [Lemma 2.5](#). \square

- (c) Show that if Q is cyclic, then so is $\text{Aut}(Q)$. What is the order of $\text{Aut}(Q)$ in this case?

Proof. This is proven in class — if $G \cong \langle a \mid a^n \rangle$, then there is an isomorphism of monoids

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \text{End}(G) \quad \text{given by} \quad [k] \mapsto (a^m \mapsto a^{mk})$$

(this is easily proven via the universal property of free groups). Thus there is an isomorphism of groups

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \text{Aut}(G).$$

We know that $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$, where $\phi(n)$ is the number of positive integers less than or equal to n that are coprime to n .

It is straightforward to see that $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$ if p is prime: given $1 \leq m < p^k$, the only way to have $\gcd(p^k, m) > 1$ is if m is a multiple of p , that is, $m \in \{p, 2p, 3p, \dots, p^{k-1}p = p^k\}$, and there are p^{k-1} such multiples not greater than p^k . Therefore, the other $p^k - p^{k-1}$ numbers are all relatively prime to p^k . Thus if $Q \cong \mathbb{Z}/121 = \mathbb{Z}/11^2$, we have that $|\text{Aut}(Q)| = |(\mathbb{Z}/11^2)^\times| = 11^2 - 11 = 110$. \square

- (d) If Q is not cyclic, find an isomorphic description of $\text{Aut}(Q)$ and compute its order.

Proof. If Q is not cyclic, then $Q \cong \mathbb{Z}/11 \oplus \mathbb{Z}/11 = \mathbb{F}_{11}^2$, so that $\text{Aut}(Q) = \text{GL}_2(\mathbb{F}_{11})$. The group $\text{GL}_n(\mathbb{F}_p)$ has order $(p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$. (The first row u_1 of the matrix can be anything but the 0-vector, so there are $p^n - 1$ possibilities for the first row. The second row can be anything but a multiple of the first row, giving $p^n - p$ possibilities. For any choice u_1, u_2 of the first rows, the third row can be anything but a linear combination of u_1 and u_2 . The number of linear combinations $a_1u_1 + a_2u_2$ is just the number of choices for the pair (a_1, a_2) , and there are p^2 of these. It follows that there are $p^n - p^2$ for the third row. And so on.) Thus $\text{Aut}(Q)$ has order $(11^2 - 1)(11^2 - 11) = 120 \cdot 110 = 13200$. \square

5. (August 2020 Q1)

- (a) A finite group G is called *cool* if G has precisely four Sylow subgroups (over all primes p). The order $|G|$ of a cool group is called a *cool number*. For example, S_3 is a cool group and 6 is a cool number. Describe the set of all cool numbers. Hint: Use prime factorization in your description.

We claim there are two types of cool numbers:

- **Type I.** Numbers of the form $p^n q^m r^k s^\ell$, where p, q, r, s are distinct prime numbers, and n, m, k, ℓ are positive integers. I.e., numbers with exactly four distinct prime factors.
- **Type II.** Numbers of the form $2^n 3^m$, where n and m are any positive integers.

Proof. To start, we will show any Type I or II number is cool. First, let p, q, r, s be distinct prime numbers, and n, m, k, ℓ be positive integers, and consider the group

$$G = \mathbb{Z}/p^n \oplus \mathbb{Z}/q^m \oplus \mathbb{Z}/r^k \oplus \mathbb{Z}/s^\ell.$$

Because G is abelian, every subgroup of G is normal. Thus we have $n_p = n_q = n_r = n_s = 1$ by the second Sylow theorem, so that G has 4 Sylow subgroups as desired.

Now, let n and m be positive integers and consider the group

$$G = S_3 \times \mathbb{Z}/2^{n-1} \times \mathbb{Z}/3^{m-1}.$$

Clearly $|G| = 6 \cdot 2^{n-1} \cdot 3^{m-1} = 2^n 3^m$. Now we claim that $n_2(G) = 3$ and $n_3(G) = 1$. To see this, note first that $n_3(S_3) = 1$ and $n_2(S_3) = 3$. Then $n_3(S_3 \times \mathbb{Z}/2^{n-1}) = 1$ by [Lemma 2.6](#), since 3 does not divide $|\mathbb{Z}/2^{n-1}|$, and $n_2(S_3 \times \mathbb{Z}/2^{n-1}) = n_2(S_3) = 3$, by [Lemma 2.7](#). A similar argument yields that $n_3(G) = 1$ and $n_2(G) = 3$, as desired.

Now, let G be a group. Then we claim that in order for G to be cool, its order must be Type I or II as defined above. If $|G|$ has more than four distinct prime factors, then G has more than four Sylow subgroups by Sylow 1, so G isn't cool. We showed above that any number with precisely four distinct prime factors is cool. Clearly the trivial group is not cool. Thus, it suffices to consider the cases that $|G|$ has one, two, or three prime factors. In what follows, let p, q , and r be distinct primes, and let n, m , and k be positive integers.

Case 1. $|G| = p^n$. By the third Sylow theorem, we have $n_p \mid 1$, which implies $n_p = 1 \neq 4$, so no p -group is cool.

Case 2. $|G| = p^n q^m$. In order for G to be cool, we must have $n_p + n_q = 4$, so suppose this holds. Then we claim $\{p, q\} = \{2, 3\}$. If $n_p = n_q = 2$, then by Sylow 3 we'd have $n_p = 2 \equiv 1 \pmod{p}$, i.e., $1 \equiv 0 \pmod{p}$, but 1 is not a multiple of any prime, so we can't have $n_p = n_q = 2$.

Now, suppose $\{n_p, n_q\} = \{1, 3\}$, say WLOG $n_p = 3$ and $n_q = 1$. Then by Sylow 3, we have $n_p = 3 \equiv 1 \pmod{p}$, i.e., $2 \equiv 0 \pmod{p}$, which is only possible if $p = 2$. We'd also have $n_p = 3 \mid q^m$, which is only possible if $q = 3$. Hence $|G| = 2^n 3^m$, so $|G|$ is Type II, as desired.

Case 3. $|G| = p^n q^m r^\ell$. Again, if G is cool, then we can assume WLOG that $n_p = 2$ and $n_q = n_r = 1$. Then by Sylow 3, $n_p = 2 \equiv 1 \pmod{p}$, i.e., $1 \equiv 0 \pmod{p}$, an impossibility since $p \neq 1$. Thus if G has 3 prime factors then it is lame. \square

- (b) For each cool number n that you found in part (a), determine whether every group of order n is nilpotent.

Proof. First, let G be a Type I cool group, so that $|G| = p_1^{n_1} p_2^{n_2} p_3^{n_3} p_4^{n_4}$ where each p_i is a distinct prime and each n_i is a positive integer. Then since G is cool, for each $i = 1, 2, 3, 4$ there exists a unique normal subgroup $H_i \trianglelefteq G$ of order $p_i^{n_i}$. Since each H_i is normal, $K := H_1 H_2 H_3 H_4$ is a subgroup of G , and $|H_i| = p_i^{n_i}$ divides $|K|$ for each $i = 1, 2, 3, 4$. Since the p_i 's are distinct primes, it follows that $|K| = p_1^{n_1} p_2^{n_2} p_3^{n_3} p_4^{n_4} = |G|$, so that $K = G$. Moreover, if $L_1 := H_1 \cap (H_2 H_3 H_4)$, Then $|L_1|$ must divide $|H_1| = p_1^{n_1}$ and $|H_2 H_3 H_4|$, which has order $|H_2| |H_3| |H_4| = p_2^{n_2} p_3^{n_3} p_4^{n_4}$ (since $|H_2 H_3 H_4| \leq |H_2| |H_3| |H_4|$, and $|H_i|$ must divide $|H_2 H_3 H_4|$ for $i = 2, 3, 4$). Since $|L_1|$ divides both $p_1^{n_1}$ and $p_2^{n_2} p_3^{n_3} p_4^{n_4}$ and the p_i 's are distinct primes, it follows that $|L_1| = 1$, so $L_1 = \{e\}$. The exact same argument yields that $L_2 := H_2 \cap H_1 H_3 H_4$, $L_3 := H_3 \cap H_1 H_2 H_4$, and $L_4 := H_4 \cap H_1 H_2 H_3$ are trivial as well. Thus by the product recognition theorem, it follows that $G \cong H_1 \times H_2 \times H_3 \times H_4$. We

know p -groups are nilpotent ([Proposition 1.107](#)) and a product of nilpotent groups is nilpotent ([Proposition 1.106](#)), so G is nilpotent, as desired.

Now, suppose G is a Type II cool group, so that $|G| = 2^n 3^m$, $n_2 = 3$, and $n_3 = 1$. □

- (c) For each cool number n that you found in part (a), determine whether every cool group of order n is solvable.

Proof. □

6. (August 2020 Q2) Suppose a finite group G acts on a set A so that for every nontrivial $g \in G$ there exists a unique fixed point (i.e., there is exactly one $a \in A$, depending on g , such that $g(a) = a$). Prove that this fixed point is the same for all $g \in G$.

Proof. □