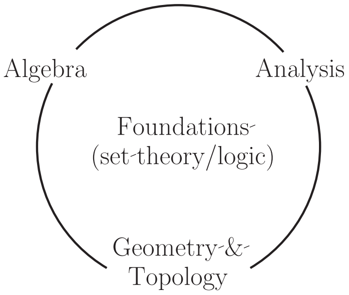
ABSTRACT ALGEBRA I

PAUL MELVIN
BRYN MAWR COLLEGE, FALL 2019

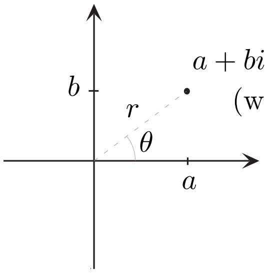
Pure Mathematics



$\boxed{\textbf{What is Algebra?}}$: the study of

- **Number systems**

$\mathbb{N} = \{1, 2, 3, \dots\}$: natural numbers
$\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$: integers
$\mathbb{Q} = \{\text{fractions}\}$: rationals
$\mathbb{R} = \{\text{decimals}\} = \text{points on the line}$: real numbers
$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\} = \text{points in the plane}$: complex numbers



$a + bi = re^{i\theta}$ polar form
(where $a = r\cos\theta$ and $b = r\sin\theta$)

Note $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, all proper inclusions, e.g. $\sqrt{2} \notin \mathbb{Q}$, as you're asked to show in the first writing assignment below.

Many other important number systems inside $\mathbb{C}$ will be encountered later in this course.

- **Structure** "binary operations" $+$ and $\cdot$

associative, commutative, and distributive properties (see WA#1)
identity elements 0 and 1 for $+$ and $\cdot$ resp.

Factoring and solving equations, e.g.

① $ax^2 + bx + c = 0$ has two solutions $x = (-b \pm \sqrt{b^2 - 4ac})\,/\,2a$ in $\mathbb{C}$
② $x^2 + y^2 = z^2$ has infinitely many solutions in $\mathbb{N}$, the "Pythagorian triples": (3,4,5), (5,12,13), ...
③ $x^n + y^n = z^n$ has no solutions in $\mathbb{N}$ for any fixed $n \geq 3$ [†]

- **Abstract systems** groups, rings, fields, vector spaces, modules, ...

A group is a set G with an associative "binary operation" $*$ (maybe $+$, $\cdot$, or something else) that has an identity (i.e. an element $e \in G$ such that $x*e = x = e*x$ for all $x \in G$) and inverses for each of its elements ($\forall\, x \in G, \exists\, y \in G$ such that $x * y = y * x = e$).

Examples $(\mathbb{Z}, +)$ is a group, while $(\mathbb{N}, +)$ is not (no identity). $(\mathbb{Z}, \cdot)$ and $(\mathbb{N}, \cdot)$ have identities but are not groups: some elements do not have inverses. $(\mathbb{Q}, \cdot)$ isn't either (0 doesn't have an inverse) but $(\mathbb{Q} - \{0\}, \cdot)$ is. $(\mathbb{Z}^n, +)$ and $(\mathbb{R}^n, +)$ are groups.

Focus of first semester: groups / intro to rings (sets with two operations satisfying ...)

Some history : theory of equations ($\rightsquigarrow$ modern algebra)

Quadratic equation (antiquity)

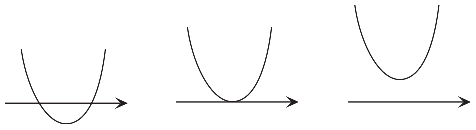
$$ax^2 + bx + c \;=\; 0$$

To solve for x, divide by a and complete the square, i.e. substitute $y = x + b/2a$ to eliminate the linear term. This gives the simpler quadratic

$$y^2 - p \;=\; 0$$

where $p = (b^2 - 4ac)/4a^2$ (verify this using the binomial expansion $(r+s)^2 = r^2 + 2rs + s^2$) whose roots are $y = \pm\sqrt{p}$. This yields the usual formula after substituting back for x.

Remark $\Delta = b^2 - 4ac$ is called the discriminant of the polynomial $ax^2 + bx + c$. If $a, b, c \in \mathbb{R}$, then the equation has 2, 1 or 0 real roots according to the sign of Δ:



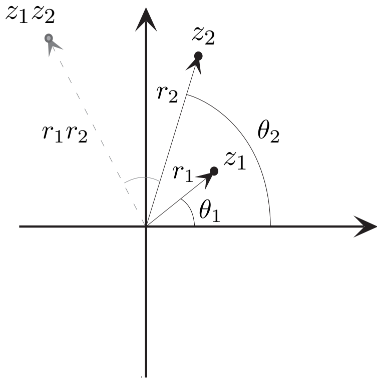
$\Delta > 0$ $\quad$ $\Delta = 0$ $\quad$ $\Delta < 0$

[†] This is Fermat's Last 'Theorem', conjectured in 1637 and finally proved in 1995 by Andrew Wiles. We'll give a proof for $n = 3$ at the end of the semester.

On complex multiplication, inverses and roots If $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$, then

$$z_1 z_2 \;=\; r_1 r_2\, e^{i(\theta_1+\theta_2)},$$

i.e. lengths multiply and angles add (prove this using trigonometry; note that it follows that for any u and v in the unit circle S^1, we have $uv, u^{-1} \in S^1$ so $(S^1, \cdot)$ is a group!).



It is now easy to see that each nonzero complex number $z = re^{i\theta}$ has inverse $z^{-1} = r^{-1}e^{-i\theta}$, and has two square roots, three cube roots, etc. In particular, the nth roots of z are

$$w = r^{1/n}e^{i\theta/n}\,,\;\; u_n w\,,\;\; \ldots\,,\;\; u_n^{n-1}w$$

where $u_n = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$. These points are equally distributed on a circle of radius $r^{1/n}$ about the origin (since multiplication by u_n rotates $\mathbb{C}$ about the origin by $2\pi/n$ radians).

Cubic equation (16th century: del Ferro, Tartaglia ⇝ Cardan, Viète)

$$\boxed{ax^3 + bx^2 + cx + d \;=\; 0}$$

To solve for x, divide by a and complete the cube, i.e. substitute $x = y - b/(3a)$ to eliminate the quadratic term, giving the "depressed" cubic

$$\boxed{y^3 + py + q \;=\; 0}$$

where p and q are found in practice by simplifying after the substitution (You will need to use the binomial expansion $(r+s)^3 = r^3 + 3r^2s + 3rs^2 + s^3$ to do so.) To find the roots of this cubic, use Viète's magical substitution $y = z - p/(3z)$, which leads to the sextic $z^6 + qz^3 - (p/3)^3 = 0$, and so a *quadratic* in $w = z^3$. So putting these together, substitute $y = w^{1/3} - p/(3w^{1/3})$ to get

$$\boxed{w^2 + qw - (p/3)^3 = 0}$$

with roots $w_\pm = -q/2 \pm \sqrt{(q/2)^2 + (p/3)^3}$. Now back substituting, if z_i (for $i = 1, 2, 3$) are the three cube roots[†] of w_+ or w_- (either will do) then $y_i = z_i - p/(3z_i)$ are the roots of the depressed cubic, and so

$$\boxed{x_i \;=\; z_i - p/(3z_i) - b/(3a)}$$

are the roots of the original equation. This is called Cardan's formula.

Question What is the significance of the sign of $\Delta = (q/2)^2 + (p/3)^3$? This number is called the discriminant of the cubic?

[†] Recall that if you find z_1, then $z_2 = uz_1$ and $z_3 = u^2 z_1$ where $u = u_3 = e^{2\pi i/3} = -1/2 + \sqrt{3}i/2$.

In examples, it is generally simpler to follow through the preceding derivation rather than trying to plug into a general formula. Or at least first find p and q by expanding the original cubic after the substitution $x = y - b/3a$, then one cube root z_1 of $-q/2 \pm \sqrt{\Delta}$, then $z_2 = uz_1$ and $z_3 = u^2 z_1$ (where $u = e^{2\pi i/3}$), and finally substitute in Cardan's formula.

Example Find the roots of $x^3 + 6x^2 + 9x + 2$.

Solution Substituting $y = x + 2$ gives $y^3 - 3y$, so $p = -3$ and $q = 0$, so $\Delta = -1$. Now choose $z_1 = i$ (a cube root of $-q/2 - \sqrt{\Delta} = -i$), so $z_2 = ui$ and $z_3 = u^2 i$. Cardan's formula now gives the roots of the cubic: $x_1 = i + i^{-1} - 2 = -2$, $x_2 = ui + (ui)^{-1} - 2 = -\sqrt{3} - 2$ and $x_3 = u^2 i + (u^2 i)^{-1} - 2 = \sqrt{3} - 2$.

Quartic equation 16th century: Ferrari

Quintic equation (and higher degree) 19th century: Abel proved, remarkably, that there's no general formula for the roots! Galois developed the general theory (we'll study this in the second semester) ⇝ birth of modern algebra. Spread the word ...!

Some arithmetic : Key Lemmas and the Fundamental Theorem

"Arithmetic" is the study of the natural numbers. For now, all unspecified variables $a, b, c, d, \ldots$ will represent elements of $\mathbb{N}$.

Definition Say d divides (or is a divisor of) a, written $d|a$, if $\exists\, m$ with $a = md$. For any a and b, write $\gcd(a, b)$ for the greatest common divisor of a and b.

Note that if $d|a$ then $d|ab$ for any b, and if $d|a$ and $d|b$ then $d|(a + b)$.

GCD Lemma *$\forall\, a, b \in \mathbb{N}$, $\exists\, m, n \in \mathbb{Z}$ such that $\gcd(a, b) = ma + nb$.*

Example $\gcd(10, 14) = 2 = 3 \cdot 10 + (-2) \cdot 14$. Note that in general, exactly one of m or n will be positive and the other will be ≤ 0; do you see why?

Proof of GCD Lemma Consider $S = \{ma + nb \mid m, n \in \mathbb{Z}\}$. Note that S is closed under subtraction, and under multiplication by *any* fixed integer; any nonempty such subset of $\mathbb{Z}$ is called an ideal in $\mathbb{Z}$.

Set $d = \min(S \cap \mathbb{N})$, the smallest positive element of S. We claim that $d = \gcd(a, b)$, which will prove the lemma. To prove this claim, we must show

$$\textcircled{1}\ d|a, d|b \qquad \textcircled{2}\ e|a, e|b \Longrightarrow e \leq d$$

$\textcircled{1}$ Dividing a by d gives a quotient q plus a remainder r less than d, that is $a = qd + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$. Thus $r = a - qd$, which lies in S since S is an ideal. The minimality of d shows that $r = 0$, and so $d|a$. Similarly $d|b$.

$\textcircled{2}$ $e|a, e|b \Longrightarrow e|(ma + nb)$ for all m, n, and in particular $e|d$. Thus $e \leq d$. □

Remark This proof used structural properties of $\mathbb{Z}$ (its arithmetic operations $+$ and $\cdot$ and its ordering $<$) and the following two axioms:

Well Ordering Principle (WOP) *Every non-empty subset of* $\mathbb{N}$ *has a smallest element* (or in symbols, $S \subset \mathbb{N}, S \neq \varnothing \implies \exists\, m \in S$ such that $m \leq s$ for all $s \in S$)

Note This principle applies equally well to subsets of $\mathbb{Z}_+ = \mathbb{N} \cup \{0\}$.

Division Algorithm (DA) $\forall\, a, d \in \mathbb{N}$, $\exists\, q, r \in \mathbb{Z}$ *with* $0 \leq r < d$ *such that* $a = qd + r$

In fact WOP $\implies$ DA: Set $S = \{a - md \mid m \in \mathbb{Z}_+, md \leq a\} \subset \mathbb{Z}_+$. By WOP, $\exists\, r = \min S \in \mathbb{Z}_+$, of the form $r = a - qd$, for some q. The minimality of r implies $r < d$, which proves DA. □

Where does the GCD Lemma lead?   To the ...

Fundamental Theorem of Arithmetic (FTAr) *Every natural number* $n > 1$ *is either prime (meaning it has exactly two natural number divisors, 1 and itself) or can be written uniquely as a product of primes (up to the order in which the primes appear in the product).*

via

Euclid's Lemma (EL) *If* p *is prime and* $p|ab$*, then* $p|a$ *or* $p|b$.

Proof of EL If $p \,|\, a$ we're done. If $p \nmid a$, then $\gcd(a,p) = 1$ (since p is prime) and so by the GCD Lemma, $1 = ma + np$ for some integers m, n. But then $p \,|\, b$. Indeed $b = 1 \cdot b = (ma + np)b = m(ab) + npb$, which is divisible by p since $m(ab)$ and npb are. □

Summarizing the logic so far: WOP $\implies$ EL (via DA and GCD Lemma). For FTAr, also need induction, which we use informally in the following proof.

Proof of FTAr (existence) If n is not prime, then $n = ab$ for some $a, b < n$. But then by induction, each of a, b has a prime decomposition. Put these together to get one for n.

(uniqueness) Suppose

$$p_1 \cdots p_r \;=\; q_1 \cdots q_s$$

(all p_i's and q_j's are prime). Clearly

$$p_1 \,|\, p_1 \cdots p_r \quad \text{and so} \quad p_1 \,|\, q_1 q_2 \cdots q_s.$$

By EL and induction, p_1 divides at least one of the q_j's; can assume $p_1|q_1$ by reordering. But this implies $p_1 = q_1$ since q_1 is prime. Thus $p_2 \cdots p_r = q_2 \cdots q_s$. The result follows by induction. □

Induction

Principle of Induction *If* $S \subset \mathbb{N}$ *satisfies*

$$\textcircled{1}\;\; 1 \in S \qquad \text{and} \qquad \textcircled{2}\;\; n \in S \implies n + 1 \in S$$

then $S = \mathbb{N}$.

It can be shown that the Principal of Induction is equivalent to the WOP. The proof is not given here, but you're asked to prove WOP $\implies$ Induction in HW #2, which implies that FTAr actually follows just from WOP and the structural properties of $\mathbb{Z}$!

We conclude with an example of proof by induction. You're asked to give three more (slighltly harder) such proofs in the homework.

- Prove by induction on n that $1 + \cdots + n = n(n+1)/2$.

Proof Let $S = \{k \in \mathbb{N} \mid 1 + \cdots + k = k(k+1)/2\}$. We must show $S = \mathbb{N}$. Clearly $1 \in S$, since $1 = 1(2)/2$. So now assume that $n \in S$, that is, assume that

$$1 + \cdots + n = n(n+1)/2.$$

We must then show that $n+1 \in S$. But adding $n+1$ to both sides gives

$$\begin{aligned} 1 + \cdots + n + (n+1) &= n(n+1)/2 + (n+1) \\ &= (n(n+1) + 2(n+1))/2 \\ &= (n+1)(n+2)/2 = (n+1)((n+1)+1)/2. \end{aligned}$$

Hence $n+1 \in S$ as desired. Thus by induction $S = \mathbb{N}$. □

1. Foundations

Sets Assume familiarity with basics of set theory:

sets $S = \{\cdots \mid \cdots\}$
elements $x \in S$
subsets $A \subset S$
proper subset $A \subsetneqq S$
union $S \cup T = \{x \mid x \in S \text{ or } x \in T\}$
intersection $S \cap T = \{x \mid x \in S \text{ and } x \in T\}$
difference $S - T = \{x \mid x \in S \text{ and } x \notin T\}$
cartesian product $S \times T = \{(s,t) \mid s \in S, t \in T\}$
cardinality $|S| = \#$ elements in S (if S is finite)

Notation: $\forall, \exists, \Longrightarrow, \Longleftrightarrow$ (if and only if, or iff), $\Longrightarrow\Longleftarrow$ (contradiction), ! (unique).

Functions

Definition A function $f : S \to T$ (also written $S \xrightarrow{f} T$) consists of a pair of sets S and T, referred to as the domain and codomain of the function, and a "rule" $s \mapsto f(s)$ assigning to each element s in S an element $f(s)$ in T.[†]

Remark The domain and codomain must be specified when defining a function. For example the two squaring functions $\mathbb{R} \to \mathbb{R}$ and $\mathbb{R} \to \mathbb{R}^+$ (the real numbers ≥ 0), both given by the rule $x \mapsto x^2$, are distinct (cf. the exercise above Proposition 1.2 below).

Examples ① identity functions $\text{id}_S : S \to S$, $s \mapsto s$.

② inclusion of a subset $A \subset S$: $A \hookrightarrow S$, $a \mapsto a$.

③ restriction of $f : S \to T$ to a subset $A \subset S$: $f|A : A \to T$, $a \mapsto f(a)$.

④ projections $S \leftarrow S \times T \to T$, $s \mapsfrom (s,t) \mapsto t$.

⑤ constant functions $S \to T$, $s \mapsto t_0$, where t_0 is a fixed elt of T.

⑥ composition of functions Given $f : S \to T$ and $g : R \to S$, define $f \circ g : R \to T$ by $(f \circ g)(r) = f(g(r))$. Thus $f \circ g$ (also written fg) is defined by requiring that the diagram

$$\begin{tikzcd} R \arrow[rr, "f \circ g"] \arrow[dr, "g"'] & & T \\ & S \arrow[ur, "f"'] & \end{tikzcd}$$

Definition Given $f : S \to T$, define the image of a subset S_0 of S under f to be

$$f(S_0) \ := \ \{f(s) \mid s \in S_0\} \subset T$$

and the preimage of a subset T_0 of T under f to be

$$f^{-1}(T_0) \ := \ \{s \in S \mid f(s) \in T_0\} \subset S.$$

(give examples and pictures) Call $f(S)$ the image of f, also denoted $\text{Im}(f)$.

[†] To be precise, a "rule" consists of a subset $R \subset S \times T$ satisfying $\forall s \in S$, $\exists!\ t \in T$ such that $(s,t) \in R$, so a function is really a triple $(S, T, R \subset S \times T) \ldots$

1.1 Proposition $\textcircled{a}$ $f^{-1}(P \cup Q) = f^{-1}(P) \cup f^{-1}(Q)$

$\textcircled{b}$ $f^{-1}(P \cap Q) = f^{-1}(P) \cap f^{-1}(Q)$

Proof $\textcircled{a}$ (Note: often prove $=$ of sets in two steps, $\subset$ and $\supset$, though sometimes done simultaneously) $x \in f^{-1}(P \cup Q) \iff f(x) \in P \cup Q \iff f(x) \in P$ or $f(x) \in Q \iff x \in f^{-1}(P)$ or $x \in f^{-1}(Q) \iff x \in f^{-1}(P) \cup f^{-1}(Q)$ $\textcircled{b}$ Same as $\textcircled{a}$ with $\cup$ and "or" replaced with $\cap$ and "and". □

Definition A function $f : S \to T$ is one-to-one (or monic or injective, also written 1-1) if it maps *at most* one element of S to each element of T. In other words, $f(x) = f(y) \implies x = y$, or equivalently $|f^{-1}(t)| \leq 1$ for all $t \in T$. It is onto (or epic or surjective) if it maps *at least* one element of S to each element of T. In other words $\text{Im}(f) = T$, or equivalently $\forall t \in T$, $\exists\, s \in S$ with $f(s) = t$, or equivalently $|f^{-1}(t)| \geq 1$ for all $t \in T$.

Exercise Determine which of the squaring functions $\mathbb{R} \to \mathbb{R}$, $\mathbb{R}^+ \to \mathbb{R}$, $\mathbb{R} \to \mathbb{R}^+$ and $\mathbb{R}^+ \to \mathbb{R}^+$ (i.e. all are given by the same rule $x \mapsto x^2$, but with different domains and codomains) are 1-1 and which are onto.[†]

1.2 Proposition *$f : S \to T$ is*

$\textcircled{a}$ 1-1 $\iff$ it has a left inverse, i.e. $\exists\, \ell : T \to S$ with $\ell \circ f = \text{id}_S$

$\textcircled{b}$ *onto $\iff$ it has a right inverse, i.e.* $\exists\, r : T \to S$ *with* $f \circ r = \text{id}_T$

Proof $\implies$'s : ($\textcircled{a} \implies$) For $t \in \text{Im}(f)$, define $\ell(t)$ to be the (unique) $s \in f^{-1}(t)$, and define $\ell(t)$ arbitrarily for $t \notin \text{Im}(f)$. ($\textcircled{b} \implies$) Define $r(t) =$ any $s \in f^{-1}(t)$. □

Exercise Prove the converses $\textcircled{a} \Longleftarrow$ and $\textcircled{b} \Longleftarrow$.

Definition A bijection is a function that is both one-to-one and onto. Any bijection $f : S \to T$ has an inverse function $f^{-1} : T \to S$, mapping each $t \in T$ to the unique $s \in S$ for which $f(s) = t$, and characterized by the two conditions $f \circ f^{-1} = \text{id}_T$ and $f^{-1} \circ f = \text{id}_S$.

Equivalence relations

Definition A partition of a set S is a division of S into non-overlapping subsets, i.e. a collection of nonempty disjoint subsets S_i of S (for i in some possibly infinite indexing set) whose union is S. We write $S = \sqcup S_i$

Examples (including Banach-Tarski Paradox) $\mathbb{Z} = \{\text{evens}\} \sqcup \{\text{odds}\}$, $\{\text{BMC undergrads}\} = \{\text{freshmen}\} \sqcup \{\text{sophomores}\} \sqcup \{\text{juniors}\} \sqcup \{\text{seniors}\}$, $\mathbb{N} = \{\text{prime numbers}\} \sqcup \{\text{composites}\}$

Definition A relation on S is a subset $\sim$ of $S \times S$; we write $x \sim y$ to indicate $(x, y) \in \sim$. Call $\sim$ an equivalence relation if it is

$\textcircled{R}$ reflexive : $x \sim x$ (for all $x \in S$),

$\textcircled{S}$ symmetric : $x \sim y \implies y \sim x$, and

$\textcircled{T}$ transitive : $x \sim y$ and $y \sim z \implies x \sim z$

The equivalence class of $x \in S$ is the subset $\overline{x} := \{y \in S \mid x \sim y\}$ of S.

[†] The first is neither, the second is 1-1 but not onto, the third is onto but not 1-1, and the last is both.

1.3 Proposition *The collection of equivalence classes of an equivalence relation on S form a partition of S. Conversely, any partition $S = \sqcup S_i$ gives rise to a unique equivalence relation $\sim$ whose equivalence classes are the S_i's, namely $x \sim y \iff \exists\, i$ with $x, y \in S_i$.*

Proof Exercise

Definition The set of all equivalence classes of an equivalence relation $\sim$ is called the quotient set of S by $\sim$:

$$S/\!\sim\; := \;\{E \subset S \mid E = \overline{x} \text{ for some } x \in S\}\,.$$

Note that the elements of $S/\!\sim$ are themselves subsets of S. The map $S \to S/\!\sim$ that sends x to $\overline{x}$ is called the natural projection of S onto $S/\!\sim$.

Examples ① (very important example: **the integers mod n**) Fix $n \in \mathbb{N}$. Then the "congruence modulo n" relation $\equiv_n$ on the set $\mathbb{N}$ is defined by

$$a \equiv_n b \quad\iff\quad a - b \;\text{ is divisible by }\; n\,,$$

or equivalently, a and b differ by a multiple of n.[†] You should verify that is an equivalence relation, i.e. that $a \equiv_n a$, $a \equiv_n b \Longrightarrow b \equiv_n a$, and $a \equiv_n b$ and $b \equiv_n c \Longrightarrow a \equiv_n c$.

The equivalence class

$$\overline{a} \;=\; \{a + kn \mid k \in \mathbb{Z}\} \;=\; \{\ldots, a - n, a, a + n, a + 2n, \ldots\}$$

is sometimes called the residue class of a (mod n). The quotient set $\mathbb{Z}/\!\equiv_n$, also denoted $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$, is called the integers mod n :

$$\mathbb{Z}_n \;=\; \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

For example, in $\mathbb{Z}_2$ the element $\overline{0} = \{\text{all even integers}\}$ and $\overline{1} = \{\text{all odd integers}\}$, whereas $\overline{1} \in \mathbb{Z}_3$ is the subset $\{\cdots, -2, 1, 4, \cdots\}$, etc. Thus the meaning of $\overline{0}, \overline{1}, \ldots$ depends on the context. Also there are (infinitely) many ways to write the same element, e.g. in $\mathbb{Z}_2$, have $\cdots = \overline{-2} = \overline{0} = \overline{2} = \cdots$.

② $S = \mathbb{R}^2 - 0$, and $x \sim y \iff x = \lambda y$ for some nonzero real number λ (picture). The quotient set $\mathbb{R}^2/\!\sim$, usually denoted $\mathbb{R}P^1$ and called the real projective line, is a circle!

Binary operations

Definition A binary operation on a set S is a function

$$* : S \times S \longrightarrow S.$$

Write $a * b$ for $*(a, b)$ ("infix" notation). It is associative if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$ and commutative if $a * b = b * a$ for all $a, b \in S$.

Examples ① $+$ and $\cdot$ are associative and commutative binary operations on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$. What about $-$? It's not even a binary operation on $\mathbb{N}$ (why?), and although it is a binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, it's neither associative nor commutative there.

② $+$ and $\cdot$ of $n \times n$ matrices (both are associative; $+$ is commutative but $\cdot$ is not)

[†] This is also commonly written $a \equiv b \pmod{n}$

③ + and $\cdot$ on $\mathbb{Z}_n$ (“modular arithmetic”) defined by

$$\overline{a}+\overline{b} \;:=\; \overline{a+b} \qquad \text{and} \qquad \overline{a}\cdot\overline{b} \;:=\; \overline{a\cdot b}$$

(in each case the RHS defines the LHS). Must show these operations are “well-defined”[†], and it is then straightforward to verify that they are associative and commutative, and that $\cdot$ distributes over $+$. For example, in $\mathbb{Z}_{12}$ (‘clock arithmetic’) we have

$$\overline{7}+\overline{8} \;=\; \overline{15}=\overline{3} \qquad \text{and} \qquad \overline{7}\cdot\overline{8}=\overline{56}=\overline{8}.$$

Morphisms

Definition A morphism (a.k.a. homomorphism) $f:(S,*)\to(S',*')$ of sets with binary operations is a function $f:S\to S'$ satisfying

$$f(a*b)=f(a)*'f(b)$$

for all $a,b\in S$. We call f a monomorphism if it is 1-1, and an epimorphism if it is onto. An isomorphism is a morphism which has an inverse which is also a morphism.

Remark Any morphism f which has an inverse (i.e. any bijective morphism) is in fact an isomorphism. You are asked to show this in the homework. This entails showing that

$$f^{-1}(x*'y) \;=\; f^{-1}(x)*f^{-1}(y)$$

for any $x,y\in S'$. To do this, start by noting $x=f(a)$, $y=f(b)$ for some $a,b\in S$, since f is onto. Now plug in ...

Examples ① The “exponential map”

$$(\mathbb{R},+)\longrightarrow(\mathbb{R},\cdot)\;, \quad x\mapsto e^x$$

is a morphism since $e^{x+y}=e^xe^y$.

② The “determinant map”

$$(M_n(\mathbb{R}),\cdot)\longrightarrow(\mathbb{R},\cdot)$$

is a morphism since $\det(AB)=\det(A)\det(B)$.

[†] For example, for $+$ suppose that $a\equiv a'$ and $b\equiv b'$, i.e. $n|(a-a'), n|(b-b')$. Then $n|[(a-a')+(b-b')]\Longrightarrow n|[(a+b)-(a'+b')]$. Thus $\overline{a+b}=\overline{a'+b'}$.

2. Groups

Basic definitions and properties

Definition A group is a set G with a binary operation $*$ satisfying three axioms:

Ⓐ associativity : $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$

Ⓔ identity : $\exists\, e \in G$ s.t. $e * a = a = a * e$ for all $a \in G$

Ⓘ inverses : $\forall\, a \in G$, $\exists\, b \in G$ s.t. $a * b = e = b * a$.

If $*$ is commutative, say G is abelian. The order of G is the number of elements in G, written $|G|$. If $|G| < \infty$, say G is finite; otherwise G is infinite. The order of an element $a \in G$, written $|a|$ (not to be confused with $|G|$) is the least positive integer n such that $a * \cdots * a$ (n times) $= e$. If no such n exists, then $|a| = \infty$ by convention.

Remarks ① Identities and inverses are unique

Proof If e_1 and e_2 are both identities, then in fact $e_1 \underset{\text{E}}{=} e_1 * e_2 \underset{\text{E}}{=} e_2$.
If b_1, b_2 are both inverses of a, then

$$b_1 \underset{\text{E}}{=} b_1 * e \underset{\text{I}}{=} b_1 * (a * b_2) \underset{\text{A}}{=} (b_1 * a) * b_2 \underset{\text{I}}{=} e * b_2 \underset{\text{E}}{=} b_2$$

② Multiplicative Convention: we usually write

$\cdot$ for $*$ and $a \cdot b$ or ab for $a * b$
1 (or 1_G) for e
a^{-1} for the inverse of a
a^n for $a * \cdots * a$ (n times) (so $|a| =$ smallest $n \in \mathbb{N}$ such that $a^n = 1$)
a^0 for 1 and a^{-n} for $(a^n)^{-1}$

If G is abelian, however, we often adopt the additive convention, writing $+$ for $*$ and $a + b$, 0, $-a$, and na for $a * b$, e, the inverse of a, and $a * \cdots * a$ (n times). With this notation, $|a| =$ smallest n such that $na = 0$.

③ Other important algebraic structures

- semigroups Ⓐ only (set with an associative binary operation)

- monoids Ⓐ and Ⓔ only (semigroup with an identity)

- rings abelian group $(R, +)$ with another associative binary operation $R \times R \overset{\cdot}{\to} R$ which distributes over $+$, i.e. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$. We call R a commutative ring if $\cdot$ is commutative, and a ring with identity if $\exists 1$.

- fields commutative ring $(F, +, \cdot)$ with identity $1 \neq 0$ such that each nonzero element has a multiplicative inverse, e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$ for prime n (HW).

2.0 Cancellation Property *If elements a, b, c in a group satisfy $ab = ac$, then $b = c$.*

Proof Idea: *multiply by a^{-1} on the left.* More precisely (supply reasons): $ab = ac \implies a^{-1}(ab) = a^{-1}(ac) \implies (a^{-1}a)b = (a^{-1}a)c \implies 1b = 1c \implies b = c$. □

Examples of groups

① $\mathbb{Z}$ is an infinite abelian group under $+$, called the infinite cyclic group. In fact $(\mathbb{Z},+,\cdot)$ is a commutative ring with 1, but not a field ($\nexists$ inverses in general)

② $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are infinite abelian groups under $+$, as are $\mathbb{Q}-0$, $\mathbb{R}-0$, $\mathbb{C}-0$ under $\cdot$

③ $\mathbb{Z}_n = \{\overline{0},\overline{1},\cdots,\overline{n-1}\}$ is a finite abelian group under $+$, called the (additive) finite cyclic group of order n. In fact $(\mathbb{Z}_n,+,\cdot)$ is a commutative ring with 1.

Application (Linear Diophantine Equations) For $a,b,c\in\mathbb{Z}$, find all integer solutions to

$$ax+by \;=\; c$$

Solution First reduce to the case $d:=\gcd(a,b)=1$ (a and b relatively prime): If $d\neq 1$, then either $d\nmid c$ in which case $\nexists$ integer solutions, or $d\mid c$ in which case we simply divide through by d. So we may assume $d=1$. Then working in $\mathbb{Z}_b$ the equation becomes $\overline{a}\,\overline{x}=\overline{c}$. To solve this, we would like to multiply on the left by the inverse of $\overline{a}$ in $\mathbb{Z}_b$, if we knew it existed. This is where $d=1$ is used: By the GCD lemma we have $ma+nb=1$ for suitable integers m,n, and so in $\mathbb{Z}_b$ we have $\overline{m}\,\overline{a}=\overline{1}$, i.e. $\overline{a}^{-1}=\overline{m}$. Thus the unique solution to the equation in $\mathbb{Z}_b$ is $\overline{x}=\overline{m}\,\overline{c}$, and consequently one solution in $\mathbb{Z}$ is $x_0=mc$, $y_0=nc$.

To get all the solutions, we can add any multiple kb of b to x_0, which will change y_0 by subtracting ka. Thus the full set of solutions is $\{(mc+kb,nc-ka)\,|\,k\in\mathbb{Z}\}$.

Example Solve $6x+10y=14$, or equivalently, $3x+5y=7$. Working in $\mathbb{Z}_5$

$$\overline{3}\overline{x} \;=\; \overline{2} \;\Longrightarrow\; \overline{x} \;=\; \overline{3}^{-1}\overline{2} \;=\; \overline{2}\cdot\overline{2} \;=\; \overline{4}$$

so one solution is $(4,-1)$, and the full solutions set is $\{(x,y)=(4+5k,-1-3k)\mid k\in\mathbb{Z}\}$.

④ The (multiplicative) finite cyclic group of order n

$$C_n \;=\; \{z\in\mathbb{C}\mid z^n=1\} \;=\; \{1,u,u^2,\dots,u^{n-1}\} \qquad \text{(under multiplication)}$$

where $u=e^{2\pi i/n}$. This group is ‘isomorphic’ to $(\mathbb{Z}_n,+)$ via $u^k\leftrightarrow\overline{k}$. Note that each C_n is a ‘subgroup’ of the circle group $\mathbb{S}^1=\{z\in\mathbb{C}\mid |z|=1\}$ (under multiplication), which is an infinite abelian group (in fact a Lie group: a group which is also a ‘manifold’ …)

⑤ The Klein 4-group $V_4=\{1,a,b,c\}$ with $a^2=b^2=c^2=1$ (from which follows[†] that the product of any two of a,b,c equals the third). This is a finite abelian group that is not isomorphic to C_4 (e.g. since only two elements in C_4 have square 1). C_4 and V_4 are the only two groups of order 4, up to isomorphism (seen by showing[†] that, up to relabeling the elements, there are only two possible multiplication tables for groups of order 4).

⑥ The finite quaternion group $Q_8=\{\pm1,\pm i,\pm j,\pm k\}$ with $i^2=j^2=k^2=-1$, $ij=k=-ji$, $jk=i=-kj$, $ki=j=-ik$, and $-1x=-x$ for any $x\in Q_8$. This is a finite nonabelian group of order 8. It is one of exactly five such groups (up to isomorphism, as you will show later). It is a subgroup of the infinite quaternion group

$$\mathbb{S}^3 \;=\; \{a+bi+cj+dk\,|\,a,b,c,d\in\mathbb{R},\;\; a^2+b^2+c^2+d^2=1\}$$

which in turn is a subset of the ring of quaternions

$$\mathbb{H} \;=\; \{a+bi+cj+dk\mid a,b,c,d\in\mathbb{R}\}.$$

[†] Helpful observation The cancelation property in groups implies that their multiplication tables are like Sudokus: any row or column contains all the elements in the group, each appearing exactly once.

Remark Multiplication in $\mathbb{H}$ is related to the dot and cross products in $\mathbb{R}^3$: Writing a quaternion $a+bi+cj+dk$ as $a+(b,c,d)=a+\vec{v}$, we have

$$(a+\vec{v})(b+\vec{w}) = (ab - \vec{v}\bullet\vec{w}) + (a\vec{w}+b\vec{v}+\vec{v}\times\vec{w}).$$

⑦ **Products** If G and H are groups, then $G\times H$ is as well under the operation $(g,h)\cdot(g',h') := (gg',hh')$. For example, $C_2\times C_2 = \{(1,1),(1,-1),(-1,1),(-1,-1)\}\cong V_4$.

Remarks ⓐ The product of abelian groups is abelian ⓑ $|G\times H| = |G||H|$.

⑧ **Units** Let $(R,\cdot)$ be a monoid (e.g. ignore $+$ in any ring R). Set

$$R^\bullet = \{a\in R \mid \exists\, b\in R \text{ with } ab=ba=1\},$$

that is, the set of all invertible elements in R. These are called the units in R.

Claim $(R^\bullet,\cdot)$ is a group Proof: First note that the inverse of any $a\in R^\bullet$ is unique (by the same argument we used for groups) and is also in $R^\bullet$; we denote it by a^{-1}. It is easy to see that $\cdot$ induces a binary operation on $R^\bullet$, i.e. that $R^\bullet$ is closed under multiplication: $a,b\in R^\bullet \implies (ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab) \implies ab\in R^\bullet$. Furthermore, associativity is inherited, $1\in R$ (since $1\cdot 1=1$) and any $a\in R^\bullet$ has an inverse in $R^\bullet$ (namely a^{-1}).

Examples ⓐ $\mathbb{Z}^\bullet = \{+1,-1\} = C_2$

ⓑ $\mathbb{Z}_n^\bullet \underset{\text{def}}{=} \{\bar{a}\in\mathbb{Z}_n \mid \exists\,\bar{b} \text{ with } \bar{a}\bar{b}=\bar{1}\} \underset{\text{claim}}{=} \{\bar{a}\in\mathbb{Z}_n \mid \gcd(a,n)=1\}$

(Proof: $\bar{a}\in\mathbb{Z}_n^\bullet \iff \exists\, x,y$ s.t. $ax+ny=1 \underset{\text{GCD}}{\iff} \gcd(a,n)=1$). Thus

$$\mathbb{Z}_n^\bullet = \{\bar{a} \mid 0<a<n,\ \gcd(a,n)=1\}.$$

For example $\mathbb{Z}_8^\bullet = \{\bar{1},\bar{3},\bar{5},\bar{7}\}$ is a group of order 4 with multiplication table

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

As noted above, there are exactly two groups of order 4, C_4 and V_4. Which one is $\mathbb{Z}_8^\bullet$ isomorphic to? Answer: to V_4, via $\bar{1}\leftrightarrow 1$, $\bar{3}\leftrightarrow a$, $\bar{5}\leftrightarrow b$ and $\bar{7}\leftrightarrow c$.

The order $|\mathbb{Z}_n^\bullet|$ is called the Euler phi function of n, denoted $\varphi(n)$.

Fact Let $n = p_1^{e_1}\cdots p_k^{e_k}$ where $p_1,\dots,p_k$ are distinct primes. Then

$$\varphi(n) = p_1^{e_1}(1-1/p_1)\cdots p_k^{e_k}(1-1/p_k) = n\,(1-1/p_1)\cdots(1-1/p_k)\,.$$

For example: $\varphi(152) = \varphi(2^3\cdot 19) = 152(1-1/2)(1-1/19) = 152(9/19) = 8\cdot 9 = 72$. This is proved by first showing

$$\mathbb{Z}_n^\bullet \cong \mathbb{Z}_{p_1^{e_1}}^\bullet \times\cdots\times \mathbb{Z}_{p_k^{e_k}}^\bullet$$

and then $\mathbb{Z}_{p^e}^\bullet \cong C_{p^e(1-1/p)}$ for odd primes p, and $\mathbb{Z}_2^\bullet = 1$, $\mathbb{Z}_{2^e}^\bullet \cong C_2\times C_{2^{e-2}}$ for $e\geq 2$.

For example, $\mathbb{Z}_{152}^\bullet \cong C_2\times C_2\times C_{18}$.

Important families of groups

Cyclic groups C_n for $n = 1, 2, 3, \ldots$ (defined above)

Dihedral groups $D_{2n} := \{\text{symmetries of } P_n\}$

where P_n is the regular n-gon in $\mathbb{C}$, with vertices at $e^{2\pi ik/n}$, and a symmetry of P_n is a rigid motion (i.e. distance preserving map $f : \mathbb{C} \to \mathbb{C}$) sending P_n to itself setwise (i.e. $f(P_n) = P_n$). Each symmetry is either a rotation about 0, or a reflection across a line through 0. D_{2n} consists of n rotations and n reflections, so $|D_{2n}| = 2n$. The group operation is composition. (Note: Can view $C_n \subset D_{2n}$ as the set of rotations of P_n.)

Can write each element of D_{2n} in terms of r (counterclockwise rotation by $2\pi/n$ radians, i.e. multiplication by ζ_n) and s (reflection through the x-axis, i.e. conjugation):

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$$

Note the "relations" $r^n = s^2 = 1$ and $sr = r^{-1}s$ (since $\overline{\zeta_n z} = \overline{\zeta_n}\,\overline{z}$). These relations can be used to reduce any word in the letters r, s, r^{-1} and s^{-1} to the unique form $r^p s^q$, for some $p \in \{0, \ldots, n-1\}$ and $q \in \{0, 1\}$, so we say D_{2n} is generated by r, s with relations $r^n = s^2 = 1$, $sr = r^{-1}s$, written

$$D_{2n} = (r, s \mid r^n = s^2 = 1,\ sr = r^{-1}s).$$

One useful consequence of these relations is that $sr^k = r^{-k}s = r^{n-k}s$ for any k.

Remark $D_4 \cong V_4$. Also think about D_6 and D_8, symmetries of the equilateral triangle and the square, and T_{12}, O_{24} and I_{60}, symmetries of the (solid) tetrahedron, octahedron (or cube) and icosahedron (or dodecahedron).

Symmetric groups $S_n := \{\text{bijections } \underline{n} \to \underline{n}\}$

where $\underline{n} = \{1, \ldots, n\}$, with composition as the group operation. This group is called the symmetric group of degree n, and its elements are generally referred to as permutations (of n symbols or letters). Note that S_n is a finite group, nonabelian iff $n \geq 3$, of order

$$|S_n| \;=\; n! \qquad \text{(why?)}$$

(What about S_1 and S_2? Exercise $S_3 \cong D_6$)

More generally, for any set A (possibly infinite), the set S_A of bijections $A \to A$ is a group under composition, the symmetric group on A.

Notation for elements $\sigma \in S_n$ ⓐ two-row notation – write the numbers $1, \ldots, n$ in the first row and their images $\sigma(1), \ldots, \sigma(n)$ in the second.

ⓑ cycle notation (more efficient) : break $\sigma \in S_n$ into disjoint 'cycles'. The k-cycle

$$(i_1\ i_2\ i_3\ \cdots\ i_k)$$

is the permutation which sends each i_j to the next i_{j+1} in the list, sends i_k to i_1, and leaves all else fixed (draw circular picture). Note that "cyclic permutations" of the list, e.g. $(i_2\ i_3\ \cdots\ i_k\ i_1)$, represent the same cycle. A 2-cycle is also called a transposition

2.1 Disjoint cycle decomposition *Every $\sigma \in S_n$ can be written uniquely as a product of disjoint cycles (up to order and cyclic permutation within each cycle; generally suppress 1-cycles in the notation).* Proof: 'obvious' . . . think about it.

Examples ① $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} = (1\ 4)(2\ 5\ 3)$

② $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix} = (1\ 4)(2)(3\ 5) = (1\ 4)(3\ 5) = (3\ 5)(4\ 1)$

Exercise List all the elements of S_3 and S_4.

To multiply (i.e. compose) two permutations, first juxtapose their cycle decompositions. What results is a product of cycles that might not be disjoint. To rewrite this in disjoint cycle form, work from right to left (as with composition of functions) to see where each number $1, \ldots, n$ maps.

For example, to compute $\pi = \sigma\tau$ where $\sigma = (2\ 1\ 4\ 5\ 3)$ and $\tau = (1\ 5)(2\ 3)$, first see where 1 maps: we have $\tau(1) = 5$ and $\sigma(5) = 3$, and so $\pi(1) = 3$. Similarly $\pi(3) = 1$ (giving $(1\ 3)$ as one of the cycles in π), $\pi(2) = 2$ (giving the cycle (2)), $\pi(4) = 5$ and $\pi(5) = 4$ (giving the cycle $(4\ 5)$). Thus

$$(2\ 1\ 4\ 5\ 3) \cdot (1\ 5)(2\ 3) = (1\ 3)(2)(4\ 5) = (1\ 3)(4\ 5).$$

Remark The order (as an element of S_n) of any k-cycle is k, and in general the order of a permutation is the least common multiple (lcm) of the orders of the (disjoint) cycles in its cycle decomposition (why?). For example

$$|(2\ 1\ 4\ 5\ 3)(6\ 9)(7\ 8)| = 10 \qquad |(2\ 1\ 4\ 5\ 3)(1\ 5)(2\ 3)| = 2$$

(not 10 for the latter, since the cycles are not disjoint).

Alternating groups $A_n \subset S_n$. Later ...

Matrix groups Let R be a commutative ring with 1, e.g. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}$ or $\mathbb{Z}_n$.

For each $n \in \mathbb{N}$ have the group $GL_n(R)$ of invertible $n \times n$ matrices with entries in R, called the general linear group (over R). This is just the group of units in $M_n(R)$ (the ring of $n \times n$ matrices/R).

Note A is invertible iff $\det(A)$ is invertible, i.e. in $R^\bullet$ ($= R - 0$ for a field).

Example $GL_2(\mathbb{Z}_2) = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\}$

Exercise Show that for p prime $|GL_n(\mathbb{Z}_p)| \ = \ \prod_{k=0}^{n-1} (p^n - p^k)\,.$

There are many important subgroups of $GL_n(R)$, e.g. the special linear group

$$SL_n(R) = \{A \in GL_n(R) \mid \det(A) = 1\}.$$

For $R = \mathbb{R}$ we have the orthogonal and special orthogonal groups

$$O(n) \ = \ \{A \in GL_n(\mathbb{R}) \mid AA^T = I\} \qquad SO(n) \ = \ \{A \in SO(n) \mid \det(A) = 1\}$$

and for $R = \mathbb{C}$, the unitary and special unitary groups

$$U(n) \ = \ \{A \in GL_n(\mathbb{R}) \mid AA^* = I\} \qquad SU(n) \ = \ \{A \in U(n) \mid \det(A) = 1\}$$

Tricky exercise: Show $SU(2) \cong \mathbb{S}^3 :=$ the 'unit' quaternions.

Group Morphisms

Definition A function $f : G \to H$ between groups is a morphism (a.k.a. homomorphism) if $f(xy) = f(x)f(y)$ for all $x, y \in G$. The kernel and image of f are the subsets

$$\ker(f) := \{x \in G \mid f(x) = 1\} \subset G \qquad \text{and} \qquad \operatorname{im}(f) := \{f(x) \mid x \in G\} \subset H\,^{\dagger}$$

Define mono, epi, and iso-morphisms in usual way (mono = 1-1, epi = onto, iso = both). Say G and H are isomorphic if $\exists$ and isomorphism $G \to H$. A morphism from a group to itself (i.e. $G = H$) is called an endomorphism, and an automorphism if it is bijective.

Examples ① The trivial morphism $G \to H$, by definition, sends every $x \in G$ to 1_H.

② $\exp : (\mathbb{R}, +) \to (\mathbb{R}^{\bullet}, \cdot)$ is a monomorphism.

③ $\det : GL_n(\mathbb{R}) \to \mathbb{R}^{\bullet}$ is an epimorphism (where it is understood that the operation is multiplication in both groups).

④ For any abelian group G, the map $\phi_- : G \to G$, $x \mapsto x^{-1}$ is a homomorphism since $\phi_-(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi_-(x)\phi_-(y)$. In fact ϕ_- is an automorphism which is its own inverse! If G is nonabelian, then ϕ_- is not a morphism: for any $a, b \in G$ with $ab \neq ba$, have $\phi_-(ab) = (ab)^{-1}$ and $\phi_-(a)\phi_-(b) = a^{-1}b^{-1} = (ba)^{-1}$, but $(ab)^{-1} \neq (ba)^{-1}$ since inverses are unique.

2.2 Properties of morphisms

ⓐ *Any composition of morphisms is a morphism.*

ⓑ *If $f : G \to H$ is a group morphism, then*

i) f is onto $\iff \operatorname{im}(f) = H$
ii) $f(1) = 1$
iii) $f(x^{-1}) = f(x)^{-1}$
iv) f is 1-1 $\iff \ker(f) = \{1\}$
v) *If $x \in G$ has finite order n, then $f(x)$ has finite order that is a divisor of n*

Proof ⓐ Straightforward from the definition. ⓑ i) is true for all functions; ii) $f(1) = f(1 \cdot 1) = f(1)f(1)$. Now multiply by $f(1)^{-1}$; iii) HW; iv) $\Longrightarrow$ is clear, $\Longleftarrow$ HW; v) $f(x)^n = f(x^n) = f(1) = 1$. Now appeal to:

2.3 Order Lemma *Let a be an element of order n in a group. If n is finite, then $a^i = a^j \iff i \equiv j \pmod{n}$. In particular $a^k = 1 \iff k$ is a multiple of n. If n is infinite, then $a^i \neq a^j$ unless $i = j$.*

Proof If n is finite, then for any i and j we can write $i - j = qn + r$ with $0 \leq r < n$. Thus $a^i = a^j \iff a^{i-j} = 1 \iff a^r = 1$ (since $a^{qn+r} = (a^n)^q a^r = a^r$) $\iff r = 0$ (since $r < n$) $\iff i \equiv j \pmod{n}$. If n is infinite, then $a^i = a^j \Longrightarrow a^{i-j} = 1 \Longrightarrow i - j = 0 \Longrightarrow i = j$. $\square$

2.4 Properties of isomorphisms *If $f : G \to H$ is an isomorphism of groups, then*

ⓐ $|G| = |H|$, ⓑ *G is abelian $\iff$ H is abelian, and* ⓒ $|f(x)| = |x| \;\; \forall x \in G$ *(so G and H have the same number of elements of any given order)*

Proof ⓐ and ⓑ are exercises. ⓒ is HW.

[†] Equivalently $\ker(f) = f^{-1}(1)$ and $\operatorname{Im}(f) = f(G)$

Can use these properties to prove two groups are not isomorphic. For example:

ⓐ $C_m \ncong C_n$ for $m \neq n$ since they have different orders.

ⓑ $C_6 \ncong S_3$ since C_6 is abelian and S_3 is not.

ⓒ $\mathbb{Z}^\bullet_{24} \ncong C_8$ since C_8 has elements of order 8, but $\mathbb{Z}^\bullet_{24}$ doesn't. Similarly $D_{24} \ncong S_4$ since D_{24} has thirteen elements of order 2 while S_4 has nine (exercise).

Open Problem : Classify all groups (up to isomorphism)

Facts ① There is only one of any given prime order (prove later)

② There are two of order 4 ($C_4, C_2 \times C_2 \cong V_4$), two of order 6 ($C_6, S_3 \cong D_6$), five of order 8 ($C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8, Q_8$), two of order 9 ($C_9, C_3 \times C_3$), two of order 10, five of order 12, fourteen of order 16, fifty-one of order 32 . . . (see p. 168 in text)

③ All finite groups have been classified (circa 1980), but not the infinite ones.

Group Actions

(a central theme in the course)

Definition An action of a group G on a set A is a map $G \times A \to A$, $(g, a) \mapsto g \bullet a$ satisfying

(A1) $g \bullet (h \bullet a) = (gh) \bullet a$ (A2) $1 \bullet a = a$

for all $g, h \in G$, $a \in A$. The associated permutation representation is the function $\sigma : G \to S_A$ (the symmetric group on A) defined by

$$(*) \qquad \sigma(g)(a) = g \bullet a.$$

Note that σ is a group homomorphism, and conversely any homomorphism $G \xrightarrow{\sigma} S_A$ gives rise to a group action given by $(*)$ which has σ as its permutation representation (exercise).

The kernel of the action is $\ker(\sigma) = \{g \in G \mid g \bullet a = a \text{ for all } a \in A\}$. The action is said to be faithful if it has trivial kernel ($\Longrightarrow \sigma$ is one-to-one), i.e. $g \bullet a = g \bullet b \Longrightarrow a = b$.

Examples ① trivial action $g \bullet a = a$ for all $a \in A$ (i.e. σ is the trivial homomorphism). This is not faithful (unless $G = \{1\}$).

② The (faithful) action of D_{2n} on the set of vertices of the n-gon.

③ The actions of any group G on itself by left multiplication $g \bullet a = ga$, right multiplication ag^{-1}, or conjugation $g \bullet a = gag^{-1}$ (you're asked to verify the last one in HW).

Definition Two elements a and b in a group G are conjugate, written $a \sim b$, if there exists $g \in G$ such that $gag^{-1} = b$. We call gag^{-1} the conjugate of a by g.

Remark $\sim$ is an equivalence relation, i.e. $a \sim a$, $a \sim b \Longrightarrow b \sim a$, and $a \sim b$, $b \sim c \Longrightarrow a \sim c$. The equivalence class of $a \in G$, denoted $[a]$, is called the conjugacy class of a. Thus two elements a and b are conjugate if and only if $[a] = [b]$. Note that if G is abelian, then $[a] = \{a\}$ for every $a \in G$ (i.e. the only conjugate of a is a itself).

Exercise Show that the conjugacy classes in Q_8 are $[1] = \{1\}$, $[-1] = \{-1\}$, $[i] = \{i, -i\}$, $[j] = \{j, -j\}$ and $[k] = \{k, -k\}$. Find the conjugacy classes in S_3 and D_8.

Subgroups

Definition A subset H of a group G is a subgroup of G, written $H < G$, if it contains the identity element 1 of G, and is a group under the operation induced from G, or equivalently it is 'closed' under

Ⓢ1 multiplication : $x, y \in H \implies xy \in H$

Ⓢ2 inversion : $x \in H \implies x^{-1} \in H$ (associativity is automatic)

Examples ① Every group G has the trivial subgroups $\{1\}$ and G. Any subgroup H other than G itself is called a proper subgroup, written $H \lneqq G$.

② (Subgroups of $\mathbb{Z}$) For $k = 0, 1, 2, \ldots$, the set $k\mathbb{Z} = \{nk \mid n \in \mathbb{Z}\}$ of all multiples of k is a subgroup of $\mathbb{Z}$, and there are no others. (Note that + is the operation in $\mathbb{Z}$, so (S2) reads $0 \in k\mathbb{Z}$.) $0\mathbb{Z} = \{0\}$ and $1\mathbb{Z} = \mathbb{Z}$ are trivial, $2\mathbb{Z}$ = evens, etc.

③ $\{1, r, \ldots, r^{n-1}\}$ and $\{1, s\}$ are subgroups of D_{2n}; there are others (find them)

④ $\{1, -1\}$ and $\{1, i, -1, -i\}$ are subgroups of Q_8; there are others (find them)

⑤ $C_n < S^1 < \mathbb{C}^\bullet$ ⑥ Kernels and images of homomorphisms are subgroups (why?)

2.5 Subgroup Criterion *A subset H of a group G is a subgroup if and only if* ⓐ H is nonempty and ⓑ H is closed under 'division', i.e. $x, y \in H \implies xy^{-1} \in H$.

Proof ($\implies$) $H \neq \varnothing$ since $1 \in H$. If $x, y \in H$, then $y^{-1} \in H$ by Ⓢ3 so $xy^{-1} \in H$ by (S1). Thus ⓑ holds.

($\impliedby$) $\exists h \in H$ by ⓐ, so $1 = hh^{-1} \in H$ by ⓑ. Now verify

Ⓢ2 : $x \in H \implies x^{-1} = 1 \cdot x^{-1} \in H$ by ⓑ, and finally

Ⓢ1 : $x, y \in H \implies y^{-1} \in H$ by Ⓢ2 $\implies xy = x(y^{-1})^{-1} \in H$ by ⓑ. □

Remark If H is finite, ⓑ can be replaced by Ⓢ1 , since $x \in H \implies x^n = 1$ for some n (since G is finite) $\implies 1 = x^n \in H$ and $x^{-1} = x^{n-1} \in H$.

Normal subgroups

Definition A subgroup H of G is called a normal subgroup of G (written $H \lhd G$) if

$$h \in H,\, g \in G \implies ghg^{-1} \in H$$

or in words, if H is "closed under conjugation" by any element in G. Equivalently, this says that $gHg^{-1} = H$ (i.e. $gH = Hg$) for every $g \in G$.

Examples ① Every subgroup of an abelian group is normal (why?)

② $\ker(f) \lhd G$ for any morphism $f : G \to H$ (why?)

③ Any $H < G$ with $|H| = \frac{1}{2}|G|$ (say H is of index 2 in G) is normal in G

Proof of ③ For any $x \notin H$, the set xH is disjoint from H (if $xh = h'$ for some $h, h' \in H$ then $x = h^{-1}h' \in H \implies\impliedby$). So $xH = G - H$. Similarly $Hx = G - H$. Thus $xH = Hx \implies xHx^{-1} = H \implies H \lhd G$. □

More examples of subgroups (some but not all are normal)

$\textcircled{1}$ Any subgroup of a subgroup of a group G is a subgroup of G, and any intersection of subgroups of G is a subgroup of G (convince yourself that this is true). Warning This is not necessarily true for normal subgroups : $K \lhd H \lhd G \not\Longrightarrow K \lhd G$ (HW: show $\exists$ examples with $|G| = 8$), but intersections of normal subgroups are still normal.

$\textcircled{2}$ (Centers, centralizers and normalizers) Let G be a group. The center of G is the set Z_G of all the elements in G that commute with every element of G :

$$Z_G \ := \ \{x \in G \mid xg = gx \text{ for all } g \in G\}$$

In general, Z_G is a normal subgroup of G.

Proof $1 \in Z_G$ since $1g = g = g1$ for all g. For $x, y \in Z_G$ and $g \in G$, have $xyg = xgy = gxy \Longrightarrow xy \in Z_G$ (proving $\textcircled{S1}$)and $xg^{-1} = g^{-1}x \Longrightarrow$ (by taking inverses) $gx^{-1} = x^{-1}g \Longrightarrow x^{-1} \in Z_G$ (proving $\textcircled{S2}$). □

Exercise Give an alternative proof using the subgroup criterion and the observation that $xg = gx \Longleftrightarrow x = gxg^{-1}$

Examples If G is abelian, then $Z_G = G$, and otherwise it is a proper subgroup of G. For example: $Z_{S_3} = \{1\}$, $Z_{Q_8} = \{1, -1\}$, $Z_{D_8} = \{1, r^2\}$ (exercise).

More generally, for any subset $A \subset G$, define the centralizer of A in G to be the set of all elements of G that commute with every element in A :

$$Z_G(A) \ := \ \{x \in G \mid xa = ax \text{ for all } a \in A\}$$

(so $Z_G = Z_G(G)$), also written $Z_G(a)$ when $A = \{a\}$. The normalizer of A in G to be the set of all elements in G that commute 'set wise' with A :

$$N_G(A) \ := \ \{x \in G \mid xA = Ax\}$$

where $xA = \{xa \mid a \in A\}$ and $Ax = \{ax \mid a \in A\}$. In general, $Z_G(A)$ and $N_G(A)$ are subgroups of G (general proof given in $\textcircled{9}$ below), but not necessarily normal subgroups.

Example For $A = \{1, -1, i, -i\} < Q_8$, have $ji \neq ij$, $ki \neq ik$, etc. and so $Z_{Q_8}(A) = A$. However $jA = \{j, -j, -k, k\}$ is the same set as $Aj = \{j, -j, k, -k\}$, so $N_{Q_8}(A) = Q_8$.

Remark In general, for any nonempty subsets $A_1, \ldots, A_n$ of a group G, define

$$A_1 \cdots A_n = \{a_1 \cdots a_n \mid a_i \in A_i \text{ for each } i = 1, \ldots n\}.$$

Special cases are $xA = \{x\}A$, $Ax = A\{x\}$ and $xAx^{-1} = \{x\}A\{x^{-1}\} = \{xax^{-1} \,|\, a \in A\}$. Note that the conditions $xa = ax$ and $xA = Ax$ defining $Z_G(a)$ and $N_G(A)$ can be rewritten as $xax^{-1} = a$ and $xAx^{-1} = A$.

$\textcircled{3}$ (Stabilizers) If a group G acts on a set A and $a \in A$, then the stabilizer of a is

$$G_a = \{x \in G \mid x \cdot a = a\}$$

G_a subgroup of G for each a. (Proof: $1 \in G_a$ by (A2), so $G_a \neq \varnothing$. Thus for any $x \in G_a$, $x^{-1} \cdot a = x^{-1} \cdot (x \cdot a) = (x^{-1}x) \cdot a = 1 \cdot a = a$ so $x^{-1} \in G_a$. If $x, y \in G_a$ then $(xy) \cdot a = x \cdot (y \cdot a) = x \cdot a = a$ so $xy \in G_a$.)

Examples

ⓐ The stabilizer of $1 \in \mathbb{C}$ under the usual action of the dihedral group D_{2n} is $\{1, s\}$.

ⓑ Normalizers are examples of stabilizers for a suitable action: Let G act by conjugation on the set of all subsets of G,

$$x \cdot A = xAx^{-1} \quad (= \{xax^{-1} \mid a \in A\}\ ).$$

Then for any $A \subset G$,

$$N_G(A) = \{x \in G \mid xA = Ax\} = \{x \in G \mid xAx^{-1} = A\} = G_A.$$

Similarly centralizers can viewed in terms of actions: For $A \subset G$, the normalizer $N_G(A)$ acts on A by conjugation, and $Z_G(A)$ is the kernel of this action (do you see why?).

Thus the fact that normalizers and centralizers are subgroups can be deduced from the fact that stabilizers and kernels of homomorphisms are.

Cyclic groups and their subgroups

Definition For any element x in a group G, let $\langle x \rangle$ denote the set of all powers of x (or multiples of x if G is an additive group) :

$$\langle x \rangle \;=\; \{x^k \mid k \in \mathbb{Z}\} \qquad \text{(with repetitions deleted)}$$

This is a subgroup of G (verify this) called the cyclic subgroup generated by x. In general, a group G is called a cyclic group if it can be generated by one of its elements, i.e. if

$$G \;=\; \langle x \rangle \qquad \text{for some } x \in G.$$

Any such x is called a generator of G (there may be many).

Remark if $|G| = n$, then G cyclic $\iff$ G has an element of order n.

Examples ① $(\mathbb{Z}, +)$ (or its multiplicative analogue $C_\infty = \{u^k \mid k \in \mathbb{Z}\}$[†]) is cyclic with generator 1 (or u). Alternatively, -1 (resp. u^{-1}) is a generator.

② C_n is cyclic with generator $u = e^{2\pi i/n}$ (or u^k for any k rel prime to n)

③ D_{2n} is not cyclic for $n > 1$: $\langle r^k \rangle \subset \langle r \rangle \neq D_{2n}$ and $\langle r^k s \rangle = \{1, r^k s\} \neq D_{2n}$

2.6 Proposition *The order n of any element x in a group is equal to the order of the cyclic subgroup it generates: $|x| = |\langle x \rangle|$.*

Proof This is clear if if $n = \infty$. If $n < \infty$ then $x^i = x^j \iff i \equiv_n j$ (by the order lemma) so $\langle x \rangle$ consists of the n distinct elements $1, x, \ldots, x^{n-1}$. □

2.7 Classification Theorem for Cyclic Groups *Every cyclic group $C = \langle x \rangle$ is isomorphic to C_n for some $n = 1, 2, \cdots, \infty$. Thus there is up to isomorphism exactly one cyclic group of each finite order and one infinite cyclic group.*

Proof If $|C| = n$, then the function $C \to C_n$ mapping x^k to u^k (for each $k \in \mathbb{Z}$) is a well defined isomorphism (why?). □

[†] where u is an indeterminant

2.8 <u>Classification Theorem for Subgroups of Cyclic Groups</u> *Let C be a cyclic group, generated say by $x \in C$. Then*

ⓐ *Every subgroup H of C is cyclic. In particular if H is nontrivial, then it is generated by x^m where m is the <u>smallest</u> positive integer for which $x^m \in H$.*

ⓑ *If C is finite of order n, then it has a unique subgroup of order k for each divisor k of n, and no other subgroups.*

<u>Proof</u> ⓐ HW ⓑ If $H < C$ is nontrivial, then $H = \langle x^m \rangle$ for m as in ⓐ. The division algorithm gives $n = km + r$ for a unique positive integer k and nonnegative integer $r < m$. Thus $1 = x^n = x^{km}x^r$, so $x^r = x^{-km} \in H$. The minimality of m shows $r = 0$. Hence $k|n$ and $H = \langle x^{n/k} \rangle$ has order k, and is the unique subgroup of order k. □

This theorem gives a complete picture of the "lattice" of subgroups of any cyclic group (draw pictures, cf. §2.5 in the text).

<u>Remarks</u> ① $\exists$ groups with non-planar lattices, e.g. D_{16}

② $\exists$ pairs of nonisomorphic groups with the same subgroup lattice, e.g. $C_2 \times C_8$ and the "modular group" of order $16 = (r, s \mid r^8 = 1 = s^2,\ rs = sr^5)$.

<u>Question</u> Does Theorem 2.8b generalize to other finite groups G?

<u>Answer</u> $\Longrightarrow$ of the first statement does (Lagranges's theorem, below), but $\Longleftarrow$ does not. An example is provided by the tetrahedral group T_{12} of symmetries of the tetrahedron:

2.9 <u>Proposition</u> *The group T_{12} of order 12 has no subgroup of order 6.*

<u>Proof</u> T_{12} contains 8 distinct $2\pi/3$-rotations, about the lines joining the 4 vertices to the centers of their opposite faces in the tetrahedron, and 4 other elements. If there were a subgroup H of T_{12} with 6 elements, then H would have to contain at least one of these rotations r, since $4 < 6$. But then it would contain all of them (since they are all conjugate to r or r^{-1}, and $H \lhd G$ as shown above) which is clearly impossible since $8 > 6$. □

As for the last statement in 2.8b, this is rarely true. For example the symmetric groups S_n contain many subgroups of order k for each $k < n$; do you see why?

Lagrange's Theorem and Applications

2.10 Lagrange's Theorem *The order of any subgroup H of a finite group G divides $|G|$.*

We give the proof below. The idea is to chop G into pieces, all of the same size as H:

Definition[†] If $H < G$, then any subset of G of the form

$$xH = \{xh \mid h \in h\}$$

for $x \in G$, is called a left coset of H in G. (for example $1H = H$ itself). Similarly define the right cosets $Hx \subset G$. Note that if G is an additive group, then cosets (right or left) are of the form $x + H = \{x + h \,|\, h \in H\}$.

Remark Now in general, the left (resp. right) cosets of H partition G into equal sized subsets, the total number of which is called the index of H in G, denoted $|G : H|$:

2.11 Coset Lemma *Let $H < G$. Then G is the union of all the left cosets of H in G, and any two such cosets $\textcircled{a}$ have the same size, and $\textcircled{b}$ coincide if they intersect at all.* (Similarly for right cosets)

Proof The first statement follows from the fact that each $x \in G$ lies in xH. Now given two cosets xH and yH, the map $xH \to yH$ sending xh to yh is a bijection, by cancellation (check this), proving $\textcircled{a}$. If xH and yH intersect, then $xi = yj$ for some $i, j \in H$, so $xh = xii^{-1}h = yji^{-1}h \in yH$ for any $h \in H \implies xH \subset yH$. Similarly $yH \subset xH$, so $xH = yH$. This proves $\textcircled{b}$. □

Example of coset decomposition: The subgroup $H = \{1, (1\ 2)\}$ of S_3 has cosets H, $(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$ and $(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}$.

Proof of Lagrange's Theorem The coset lemma shows that

$$|G| \;=\; |G : H||H|$$

which shows that $|H|$ divides $|G|$. □

Remark The set of all left cosets is (sometimes) denoted by G/H, so

$$|G/H| \;=\; |G : H| \;=\; |G|/|H|.$$

Similarly for the set $H\backslash G$ of right cosets.

2.12 Coset Recognitiion *Let $H < G$. Then two elements x and y in G lie in the same coset of H if and only if either of the following two equivalent conditions holds:*

$$\textcircled{a}\;\; x^{-1}y \in H \qquad \textit{or} \qquad \textcircled{b}\;\; y = xh \textit{ for some } h \in H$$

and similarly for right cosets.

Proof HW □

[†] This definition applies to infinite groups as well.

Applications

① The order of any element x in a finite group G divides the order of G.

② Any group of prime order p is cyclic (and so there's only one up to isomorphism).

③ **Euler's Theorem** *If $a, n \in \mathbb{N}$ are relatively prime, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Recall here that $\varphi(n) = |\mathbb{Z}_n^{\bullet}|$, the Euler phi function of n. Note that if p is prime, then $\varphi(p) = p - 1$ so we have the following special case of Euler's theorem:

Fermat's Little Theorem *If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Example $3^4 = 81 \equiv 1 \pmod{5}$, $3^6 = 729 \equiv 1 \pmod{7}$

Proofs ① $|x| = |\langle x \rangle|$, which divides $|G|$ by Lagrange's Theorem.

② Any $x \neq 1$ in G has order dividing p by ①, and thus equal to p, since p is prime. Thus $G = \langle x \rangle$, so G is cyclic.

③ $\gcd(a, n) = 1 \Longrightarrow \overline{a} \in \mathbb{Z}_n^{\bullet}$ (by the GCD Lemma) $\Longrightarrow \overline{a}^{\varphi(n)} = \overline{1}$ (by ①, since $\mathbb{Z}_n^{\bullet}$ has order $\varphi(n)$), i.e. $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Products and Finite Abelian Groups

Recall that the product of two groups H and K is

$$H \times K = \{(h, k) \mid h \in H,\ k \in K\}$$

with componentwise multiplication $(h, k)(h', k') = (hh', kk')$. It turns out that every finite abelian group is a product of cyclic groups. More precisely,

2.13 Fundamental Theorem of Finite Abelian Groups (Primary Form) *Every finite abelian group is isomorphic to a product of cyclic groups, each of prime power order. This product is unique except for possible rearrangement of the cyclic factors.*

The prime powers that appear are called the primary factors or elementary divisors of the group. This theorem leads to

Algorithm for finding all abelian groups of a given order n :

- If $n = p^k$, a pure prime power, then there is (up to isomorphism) exactly one abelian group of order n for each partition of k (a sequence $k_1 \geq \cdots \geq k_s$ of natural numbers such that $k = k_1 + \cdots + k_s$), namely

$$C_{p^{k_1}} \times \cdots \times C_{p^{k_n}}.$$

For example, there are three abelian groups of order $125 = 5^3$

$$C_{125} \qquad C_{25} \times C_5 \qquad C_5 \times C_5 \times C_5$$

corresponding to the three partitions 3, $2 + 1$ and $1 + 1 + 1$ of 3.

- For general $n = p_1^{k_1} p_2^{k_2} \cdots$, there's one group for each list of partitions of $k_1,\ k_2, \ldots$.

Example How many abelian groups are there of order $1500 = 2^2 \cdot 3 \cdot 5^3$? Answer: $6 = 2 \cdot 1 \cdot 3$) List them: $C_4 \times C_3 \times C_{125}$, $C_2 \times C_2 \times C_3 \times C_{125}$, $C_4 \times C_3 \times C_{25} \times C_5$, $C_2 \times C_2 \times C_3 \times C_{25} \times C_5$, $C_4 \times C_3 \times C_5 \times C_5 \times C_5$, $C_2 \times C_2 \times C_3 \times C_5 \times C_5 \times C_5$.

There's another standard form for finite abelian groups: Using the fact from HW that

$$C_m \times C_n \cong C_{mn}$$

if m and n are relatively prime, can start with the primary form, then group the largest factors associated with each prime in the primary form, then the next largest, etc. to get a unique form for any finite abelian group

$$G \cong C_{n_1} \times C_{n_2} \times \cdots$$

where $n = n_1 \cdot n_2 \cdots$ and n_i is divisible n_{i+1} for each i; the numbers $n_1, n_2, \ldots$ are called the invariant factors of G. For example

$$C_4 \times C_2 \times C_3 \times C_5 \times C_5 \cong C_{60} \times C_{10}$$

has invariant factors $60, 10$. The group $C_8 \times C_2 \times C_{28} \times C_{25} \times C_{14}$ has inv factors $1400, 28, 2, 2$ (exercise). In summary

2.14 Fundamental Theorem of Finite Abelian Groups (Invariant Form) *Any finite abelian group G is isomorphic to a product $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$ where each n_i is divisible by n_{i+1}. The numbers $n_1, \ldots, n_k$, called the invariant factors of G, are unique.*

We'll prove the first statement in the fundamental theorem (primary form). Need

2.15 Product Recognition Theorem (PRT) *If H and K are normal subgroups of a group G satisfying $H \cap K = 1$ and $HK = G$, then $G \cong H \times K$.*

Proof Consider the function $f : H \times K \to G$ given by $f(h, k) = hk$, which is onto since $HK = G$. We claim that f is a homomorphism. First note that for any $h \in H$ and $k \in K$, $hkh^{-1}k^{-1} \in H \cap K$ (it can be written as $h(kh^{-1}k^{-1}) \in H$ since $H \lhd G$, or as $(hkh^{-1})k^{-1} \in K$ since $K \lhd G$). Since $H \cap K = 1$, it follows that $hkh^{-1}k^{-1} = 1$, i.e. $hk = kh$, so the elts of H commute with the elements of K. Now $f((h, k)(h', k')) = f(hh', kk') = hh'kk' = hkh'k' = f(h, k)f(h', k')$.

Finally observe that $\ker(f) = 1$ (since $f(h, k) = 1 \implies hk = 1 \implies h = k^{-1} \in H \cap K = 1$, i.e. $(h, k) = (1, 1)$) so f is 1-1. □

Now let G be a nontrivial finite abelian group. We wish to show that G is a product of cyclic groups of prime power orders. First consider an element a in G of order $n > 1$, and choose a prime divisor p of n. Then G has an element of order p, namely $b = a^{n/p}$ (by the Order Lemma 2.3). Thus $|G| = p^k q$ for some $k > 0$ and q not divisible by p. Set

$$P = \{x \in G \mid x^{p^k} = 1\} \qquad \text{and} \qquad Q = \{x \in G \mid x^q = 1\}.$$

Then $P \neq 1$ (since it contains b) and Q are subgroups (since G is abelian) with $P \cap Q = 1$ (since $p \nmid q$) and $PQ = G$: $\exists\, a, b$ with $aq + bp^k = 1$, so for any $x \in G$

$$x = x^{aq + bp^k} = x^{aq} x^{bp^k} \in PQ$$

(do you see why?) Thus $G \cong P \times Q$ by the PRT. It remains (by induction on $|G|$) to prove that P is a product of cyclic groups. This is the content of the following theorem:

2.16 p-Group Theorem *If P is an abelian p-group for some prime p* (meaning that each element in P has order a power of p) *then P is a product of cyclic groups.*

Proof Let H be the cyclic subgroup of P generated by an element h of maximal order (say p^s) in P, and K be a largest possible subgroup of P for which $H \cap K = 1$. If the subgroup $HK = P$, then $P \cong H \times K$ by the PRT, and the theorem follows by induction on $|P|$. So assume $HK \neq P$. We will show that this leads to a contradiction.

Claim $\exists\, x \in P$ such that $x \notin HK$ but $x^p \in K$.

Proof of claim First note that $\exists\, y \notin HK$ with $y^p \in HK$. (Indeed, for any $z \notin HK$, choose the smallest m such that $z^{p^m} \in HK$, and set $y = z^{p^{m-1}}$.) Now $y^p = h^n k$ for some $n \in \mathbb{Z}$, $k \in K$. By the maximality of $|h|$ we have

$$y^{p^s} = (h^n k)^{p^{s-1}} = h^{np^{s-1}} k^{p^{s-1}} = 1.$$

Thus $h^{np^{s-1}} = 1$, since $H \cap K = 1$, and so $p|n$. Set $x = h^{-n/p}y$. Clearly $x^p = k \in K$, but $x \notin HK$ since $y \notin HK$. This completes the proof of the claim.

Now let K' be the subgroup generated by x and K,

$$K' = \{x^n k \mid n \in \mathbb{Z},\, k \in K\}.$$

Observe that $H \cap K' = 1$, since $x^n k = h \in H \implies x^n = hk^{-1} \in HK \implies p|n \implies x^n \in K \implies h \in K \implies h = 1$. But $K' \supsetneqq K$, which contradicts the maximality of K. □

The Symmetric and Alternating Groups

The following famous result underscores the importance of the symmetric groups:

2.17 Cayley's Theorem *Every group G is isomorphic to a subgroup of the symmetric group S_G of all permutations of the set G. In particular, every finite group of order n is isomorphic to a subgroup of S_n.*

Proof Let G act on itself by left multiplication. Then the associated permutation homomorphism $\lambda : G \to S_G$ (i.e. $\lambda(g) =$ left multiplication by g) is one-to-one, by the cancellation property in G, and so $G \cong \mathrm{im}(\lambda) < S_G$. □

One important subgroup of S_n is the alternating group A_n of all "even" permutations, where the parity (even or odd) of a permutation $\sigma \in S_n$ is defined as follows: First note that σ can be written as a product of transpositions, since any cycle can be so written:

$$(*) \qquad (i_1\ \cdots\ i_k) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{k-1}\ i_k)$$

Definition A permutation is even if it can be written as a product of an even number of transpositions, and odd if it can be written as a product of an odd number of transpositions.

This decomposition is not unique, e.g. $1 = (1\ 2)(1\ 2) = (1\ 2)(3\ 4)(1\ 2)(3\ 4)$, but the parity of the number of transpositions is always the same:

2.18 Remarkable Fact *No permutation is both even and odd.*

There are many proofs (cf. pages 109–111 in Dummit and Foote, or the enlightening dance floor proof by Ty Cunningham in Math. Magazine **43** (1970) 154-5). Here is one:

Proof Consider the function $c : S_n \to \mathbb{N}$ that sends $\sigma \in S_n$ to the number of cycles in the disjoint cycle decompostion of σ, counting the 1-cycles (see §2.2). For example $c(k\text{-cycle}) = n - k + 1$. Readily verify

$$c(\sigma\tau) \;\equiv\; c(\sigma) + 1 \pmod 2$$

for any transposition $\tau = (i\ j)$: If i and j lie in the same cycle in σ then that cycle splits into two in $\sigma\tau$, and if they lie in distinct cycles in σ then those cycles are joined into one in $\sigma\tau$; the remaining cycles of σ and $\sigma\tau$ coincide. It follows that if σ is a product of m transpositions then

$$c(\sigma) \;\equiv\; c(1) + m \equiv n + m$$

so the parity of m is determined by σ. □

Therefore any permutation σ has a well-defined parity : even or odd. Since odd-length cycles are even and even-length cycles are odd (by $(*)$) this parity is just the parity of the number of even-length cycles in any cycle decomposition of σ; the number of odd-length cycles is irrelevant.[†] Thus even permutations are those with even number of even-length cycles, for example those with cycle structure

$$(\cdot\cdot\cdot)\ ,\ (\cdot\cdot)(\cdot\cdot)\ ,\ (\cdot\cdot\cdot\cdot\cdot)\ ,\ (\cdot\cdot\cdot)(\cdot\cdot\cdot)\ ,\ (\cdot\cdot\cdot\cdot)(\cdot\cdot)\ ,\ (\cdot\cdot)(\cdot\cdot)(\cdot\cdot)(\cdot\cdot)\ ,\ \text{etc.}$$

Noting that even·even = odd·odd = even, and even·odd = odd·even = odd, we have a group morphism

$$\text{sgn} : S_n \to C_2 = \{\pm 1\}$$

sending even permutations to $+1$ and odd ones to -1. The kernel of sgn, consisting of all even permutations, is called the alternating group of degree n, denoted A_n. It is a normal subgroup of S_n, since it is the kernel of a morphism, and is clearly of index 2 in S_n, i.e.

$$|A_n| \;=\; n!/2 \qquad \text{for } n > 1$$

Do you see why?

Examples A_1 and A_2 are trivial groups (exercise). It can be shown without too much difficulty that $A_3 \cong C_3$, $A_4 \cong T_{12}$ and $A_5 \cong I_{60}$. But beyond that, these are 'new' groups, which have the exceptional property (Abel's Theorem below) of being 'simple':

Definition A group G is simple if it has no nontrivial proper normal subgroups.

Example Any group of prime order is simple. Indeed such a group has no proper subgroups whatsoever, by Lagrange's Theorem.

To prove Abel's Theorem (which is the key to showing that there is no quintic formula!) we will need to understand some basic characteristics of S_n and A_n. First note that by the cycle structure observation above, one can easily list the elements in A_n. For example

$$A_3 \;=\; \{1, (1\ 2\ 3), (3\ 2\ 1)\} \qquad \text{and} \qquad A_4 \;=\; \{1, (1\ 2\ 3), \cdots, (1\ 2)(3\ 4), \cdots\}.$$

We now discuss some deeper properties.

[†] The parity of σ can also be computed geometrically from a picture of σ obtained by connecting the n points $x_1 = (1,0), \ldots, x_n = (n,0)$ in the plane to the n points $y_1 = (1,1), \ldots, y_n = (n,1)$ directly above them with a 'transverse' collection of arcs $\alpha_1, \ldots, \alpha_n$, where α_i joins x_i to $y_{\sigma(i)}$. Here the 'transverse' condition means that we only allow only pairwise intersections between the arcs, where one crosses another. Now the parity of σ is simply the parity of the number of intersection points of the arcs.

Conjugation in S_n and A_n Given $\sigma, \tau \in S_n$, we compute $\sigma\tau\sigma^{-1}$ as follows: Write τ as a product $(i\,j\,\cdots)$ of cycles. Then

$$\sigma\,(i\,j\,\cdots)\,\sigma^{-1} \;=\; (\sigma(i)\,\sigma(j)\cdots)$$

i.e. replace each number in τ by its image under σ. This is easy to see if τ is a single cycle, and generalizes using the trick

$$\sigma\tau_1\tau_2\cdots\tau_r\sigma^{-1} \;=\; (\sigma\tau_1\sigma^{-1})(\sigma\tau_2\sigma^{-1})\cdots(\sigma\tau_r\sigma^{-1}).$$

It follows that two elements in S_n are conjugate $\iff$ they have the same cycle structure. For $\Longleftarrow$, note that one can easily write down a σ for which $\sigma\tau\sigma^{-1} = \tau'$ for any τ and τ' which have the same cycle structure; indeed it is not hard to determine all such σ's.

Conjugation in A_n is more complicated: A pair of ermutations iin A_n that are conjugate in A_n are certainly conjugate in S_n, but the converse need not be true; one must check whether any of the possible conjugating permutations is even.

Example $\tau = (2\ 3\ 4)$ and $\tau' = (4\ 3\ 2)$ are conjugate in S_4 since they have the same cycle structure $(\cdots)$, but not in A_4, since $\sigma\tau\sigma^{-1} = \tau' \Longrightarrow \sigma$ maps the ordered triple $(2,3,4)$ to either $(4,3,2)$, $(3,2,4)$ or $(2,4,3)$, which forces $\sigma = (2\ 4)$, $(2\ 3)$ or $(3\ 4)$, all of which are odd. This is explored further in the HW.

Normal subgroups of S_n and A_n Recall that $A_n \lhd S_n$. In fact:

2.19 Lemma *If $n \geq 5$, then A_n is the only nontrivial proper normal subgroup of S_n*

Proof First note that A_n is generated by 3-cycles. Indeed each element of A_n can be written as a product of an even number of transpositions, which pairwise can be rewritten in terms of 3-cycles: $(i\ j)(j\ k) = (i\ j\ k)$, $(i\ j)(k\ \ell) = (i\ j\ k)(j\ k\ \ell)$.

Now consider any $H \lhd S_n$ with $H \neq 1$. We must show $H = A_n$ or S_n. Choose any $\sigma \neq 1$ in H with disjoint cycle decomposition $(i\,j\,\cdots)$. Then σ does not commute with the transposition $\tau = (j\,k)$, for any chosen $k \neq i, j$ (here we are using $n \geq 3$). Indeed $\sigma\tau(i) = j$ whereas $\tau\sigma(i) = k$. Now consider the "commutator"

$$[\sigma,\tau] \;:=\; \sigma\tau\sigma^{-1}\tau^{-1} \neq 1.$$

Clearly $[\sigma,\tau] \in H$ (since $[\sigma,\tau] = \sigma(\tau\sigma^{-1}\tau^{-1})$ and H is normal) and $[\sigma,\tau]$ is a product $(\sigma\tau\sigma^{-1})(\tau^{-1})$ of two distinct transpositions. If these transpositions overlap, then $[\sigma,\tau]$ is a 3-cycle $\Longrightarrow H$ contains all 3-cycles (since it is normal) $\Longrightarrow A_n \subset H$ (since A_n is generated by 3-cycles) $\Longrightarrow H = A_n$ or S_n. If they don't overlap, then H contains all products of pairs of disjoint transpositions (since it is normal), and in particular $(1\ 2)(3\ 4)$ and $(3\ 4)(2\ 5)$ (here we're using $n \geq 5$) whose product is the 3-cycle $(1\ 2)(2\ 5) = (1\ 2\ 5) \Longrightarrow H$ contains all 3-cycles and so again $H = A_n$ or S_n. □

Remark We have repeatedly used the fact that a normal subgroup that contains an element h must contain the entire conjugacy class of h (i.e. all elements conjugate to h), a fortiori: *A subgroup $H < G$ is normal in G if and only if it is a union of conjugacy classes in G.* In general, one can understand a lot about the structure of a group from a knowledge of its normal subgroups, and consequently from a knowledge of its conjugacy classes.

2.20 Abel's Theorem *A_n is simple for all $n \geq 5$.*

Proof If A_n is not simple, then it contains a nontrivial proper normal subgroup H of *maximal* order, and we show that this leads to a contradiction: By Lemma 2.19, $H \ntriangleleft S_n$, so for some odd σ, the subgroup $K = {}^{\sigma}H := \sigma H \sigma^{-1}$ of A_n is distinct from H.[†] We claim

$$\textcircled{a}\ \ K \lhd A_n\ ,\quad \textcircled{b}\ \ H \cap K \ = \ \{1\} \qquad \text{and} \qquad \textcircled{c}\ \ HK = A_n$$

To see this, note that for $\tau \in S_n$, we have ${}^{\tau}H = H$ if τ is even (since $H \lhd A_n$) and ${}^{\tau}H = K$ if τ is odd (since $\tau^{-1}\sigma$ is even $\Longrightarrow H = {}^{\tau^{-1}\sigma}H \Longrightarrow {}^{\tau}H = {}^{\sigma}H = K$). Since ${}^{\tau}K = {}^{\tau\sigma}H$. and τ and $\tau\sigma$ have opposite parity, it follows that ${}^{\tau}K = K$ if τ is even (proving $\textcircled{a}$) and ${}^{\tau}K = H$ if τ is odd. Also $H \cap K \lhd S_n$ (since ${}^{\tau}(H \cap K) = {}^{\tau}H \cap {}^{\tau}K = H \cap K = K \cap H$) and $H \cap K \subsetneqq A_n$, so in fact $H \cap K = \{1\}$ by Lemma 2.19 again. This proves $\textcircled{b}$. Finally, $H \subsetneqq HK \lhd A_n \Longrightarrow HK = A_n$ by the maximality of H, proving $\textcircled{c}$.

It follows by the Product Recognition Theorem 2.15 that $A_n \cong H \times K$, and every element of H commutes with every element of K (cf. the proof of 2.15). But if $\tau \in H$ is of order > 2 (there exists such an τ, since otherwise $\tau^2 = 1$ for every $\tau \in H \cup K$, and thus every $\tau \in HK = A_n$, but A_n clearly contains odd order elements, e.g. 3-cycles), then $\tau = (i\ j\ k, \cdots)$ (in disjoint cycle form) and $\kappa = (k\ m)\tau(k\ m)^{-1} = (i\ j\ m, \cdots) \in K$ do not commute (e.g. $\tau\kappa(i) = k$ whereas $\kappa\tau(i) = m$), which is a contradiction. □

Challenging Exercise Give an alternative proof of Abel's Theorem for $n = 5$ as follows: Show that A_5 splits into six conjugacy classes, namely the 'trivial class' containing only the identity element, two classes of 3-cycles with 10 elements each, two classes of 5-cycles with 12 elements each, and one class with all 15 products of pairs of 2-cycles. Now observe that the total number of elements in any union of these classes including the trivial one together with at least one but not all of the remaining ones, will never divide $|A_5| = 60$, and thus that A_5 does not contain a nontrivial proper normal subgroup.

Quotient Groups

Recall that the normality of a subgroup $H < G$ can be characterized in a variety of ways, e.g. H is closed under conjugation, or $xHx^{-1} = H$ for all $x \in G$, or $xH = Hx$ for all $x \in G$, or H is a union of conjugacy classes. Here is another important characterization:

2.21 Normality Lemma *A subgroup H of G is normal in $G \Longleftrightarrow (xH)(yH) = (xy)H$ for all $x, y \in G$.*

Proof $\Longrightarrow$ is trivial using the aforementioned characterizations: $(xH)(yH) = x(Hy)H = x(yH)H = (xy)H$ (note that $HH \subset H$ since H is a subgroup, and $HH \supset H$ since $1 \in H$). For $\Longleftarrow$, take $y = x^{-1}$ to get $(xH)(x^{-1}H) = H \Longrightarrow xHx^{-1} \subset H$ since $1 \in H$. □

This lemma says that the "obvious" operation $xH \cdot yH \ = \ (xy)H$ on the set G/H of all left cosets of H in G is well defined $\Longleftrightarrow$ H is normal in G. This operation can be described more invariantly as follows: given two cosets H_1, H_2 in G/H, choose $h_1 \in H_1$ and $h_2 \in H_2$, and let H_1H_2 be the coset containing h_1h_2. The lemma shows that this coset is independent of which elements you chose. Furthermore, it turns out that this operation then makes the set G/H into a group, called the quotient group of G by H, explaining why normality is such an important notion:

[†] This subgroup ${}^{\sigma}H = \sigma H \sigma^{-1}$ is called the conjugate of H by σ. Note that in general, ${}^{\alpha}({}^{\beta}H) = {}^{\alpha\beta}H$ for any $\alpha, \beta \in S_n$.

2.22 Theorem *If $H \lhd G$, then G/H is a group under the operation defined by $xH \cdot yH = (xy)H$. Furthermore the map $p : G \to G/H$ defined by $p(x) = xH$, called the natural projection of G onto G/H, is an epimorphism.*

Proof The operation is well defined (by the lemma), associative, with identity element $1H = H$ and $(xH)^{-1} = x^{-1}H$ (verify). Clearly p is a morphism, since $p(xy) = xyH = xHyH = p(x)p(y)$, and is onto since every coset is the image of any element in it. $\square$

Remarks ① Any quotient group G/H of an abelian group G is abelian, since $xHyH = xyH = yxH = yHxH$, for any $x, y \in G$.

② Be very careful when G is an "additive" group, i.e. the operation is $+$. Then cosets of $H < G$ are of the form $x + H = \{x + h \mid h \in H\}$, and the operation in G/H is addition: $(x + H) + (y + H) = (x + y) + H$. For example, if $H = n\mathbb{Z} = \{\text{multiples of } n\} < \mathbb{Z}$, then $\mathbb{Z}/n\mathbb{Z} = \{k + n\mathbb{Z} \mid k = 0, \ldots, n-1\}$.

Note If G' is another additive group, then the product $G \times G'$ will be often be called the direct sum, written $G \oplus G' = \{(g, g') \mid g \in G,\ g' \in G'\}$ with the operation $(g, g') + (h, h') = (g + g', h + h')$. In other words $G \oplus G'$ is the same group as $G \times G'$, but written additively (cf. example ② below).

Examples ① $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, via the isomorphism $k + n\mathbb{Z} \mapsto \overline{k}$.

② Let $H := \langle 4 \rangle = \{0, 4, 8\} \lhd \mathbb{Z}_{12}$. Then H has order 3 $\Longrightarrow \mathbb{Z}_{12}/H = \{H, 1 + H, 2 + H, 3 + H\}$ has order 4 $\Longrightarrow \mathbb{Z}_{12}/H \cong C_4$ or V_4. Since $1 + H$ has order 4 (why?) we have in fact $\mathbb{Z}_{12}/H \cong C_4$.

③ Let $S := \langle (0, 1) \rangle \lhd G := \mathbb{Z}_2 \oplus \mathbb{Z}_4$. Note that $|S| = 4$ (since $(0, 1)$ has order 4) so G/S has order $|G/S| = |G|/|S| = 8/4 = 2$, and therefore $G/S \cong \mathbb{Z}_2$. G also has three subgroups of order two, $H = \langle (1, 0) \rangle$, $J = \langle (1, 2) \rangle$ and $K = \langle (0, 2) \rangle$, with $G/H \cong H/J \cong \mathbb{Z}_4$ and $G/K \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$; verify this by computing the orders of elements in the quotient, e.g. $(0, 1) + H$ has order 4 in G/H.

④ Let H be the cyclic subgroup of S_3 generated by the 3-cycle $(1\ 2\ 3)$, $H = \langle (1\ 2\ 3) \rangle = \{1, (1\,2\,3), (1\,3\,2)\} \lhd S_3$. Then H has two cosets, H and $H' = (1\,2)H = \{(1\,2), (2\,3), (1\,3)\}$, so $S_3/H = \{H, H'\} \cong C_2$.

⑤ $Z(D_8) = \{1, r^2\} \lhd D_8$, and $D_8/Z(D_8) \cong C_2 \times C_2$ (compute orders again).

Most of the important properties of quotient groups follow from the

2.23 Universal Property of Quotient Groups (UPQG) *Let K be a normal subgroup of G and $p : G \to G/K$ be the natural projection. Then for any morphism $f : G \to H$ whose kernel contains K, there exists a unique morphism $g : G/K \to H$ such that $f = g \circ p$, i.e. the following diagram commutes*

$$\begin{tikzcd} G \arrow[r, "p"] \arrow[dr, "f"'] & G/K \arrow[d, dotted, "g"] \\ & H \end{tikzcd}$$

In particular $g(xK) = f(x)$, i.e. $g(\text{coset}) = f(\text{any element in the coset})$. Also $\ker(g) = \ker(f)/K$ and $\text{im}(g) = \text{im}(f)$.

Proof First check that g is well defined (and thus unique by the commutativity of the diagram): if x, y lie in the same coset, then $x^{-1}y \in K$. But $K \subset \ker(f)$, by hypothesis, so $f(x^{-1}y) = 1 = f(x)^{-1}f(y) \implies f(x) = f(y)$. It is now straightforward to show g is a morphism ($g(xKyK) = g(xyK) = f(xy) = f(x)f(y) = g(xK)g(yK)$) with $\ker(g) = \{xK \mid f(x) = 1\} = \ker(f)/K$ and $\operatorname{im}(g) = \{f(x) \mid x \in G\} = \operatorname{im}(f)$. □

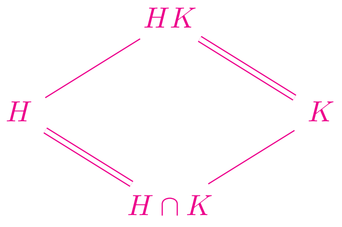
The UPQG can be used to construct morphisms *from* quotient groups. For example, you can show that $\mathbb{Z}_2 \oplus \mathbb{Z}_4/\langle(0,2)\rangle$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (see example $\textcircled{2}$ above) by constructing an explicit isomorphism., arising from the UPQG via the morphism $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ (a,b) \mapsto (a,b)$.

It has the following important consequences:

2.24 The Isomorphism Theorems

a) (First Isomorphism Theorem) *If $f : G \to H$ is a morphism, then $G/\ker(f) \cong \operatorname{im}(f)$.*

b) (Diamond Isomorphism Theorem) *If $H < G$ and $K \lhd G$, then $HK < G$, $H \cap K \lhd H$ and $H/H\cap K \cong HK/K$:*



c) If $H, K \lhd G$ with $H \subset K$, then $K/H \lhd G/H$ and $G/K \cong (G/H)/(K/H)$.

Proof Apply the Universal Property to

a)
$$\begin{tikzcd} G \arrow[r] \arrow[dr, "f"'] & G/\ker(f) \arrow[d, dotted] \\ & \operatorname{im}(f) \subset H \end{tikzcd}$$

b)
$$\begin{tikzcd} H \arrow[r] \arrow[d, hook] & H/H\cap K \arrow[d, dotted] \\ HK \arrow[r] & HK/K \end{tikzcd}$$

c)
$$\begin{tikzcd} G \arrow[r] \arrow[dr] & G/H \arrow[d, dotted] \\ & G/K \end{tikzcd}$$

← Now apply the First Isomorphism Theorem to this.

2.25 The Correspondence Theorem *Let $f : G \to H$ be a group morphism, $\mathcal{G}$ be the set of all subgroups of G containing $K = \ker(f)$, and $\mathcal{H}$ be the set of all subgroups of H contained in $I = \operatorname{im}(f)$. Then the map*

$$f : \mathcal{G} \to \mathcal{H}\ , \quad S \mapsto f(S)$$

is a bijection which respects containment, indices, normality and quotients. In other words,

(a) *$S < T \iff f(S) < f(T)$, in which case $|T : S| = |f(T) : f(S)|$*
(b) *$S \lhd T \iff f(S) \lhd f(T)$, in which case $T/S \cong f(T)/f(S)$*

Proof The inverse of f is the "preimage" map $f^{-1} : \mathcal{H} \to \mathcal{G}$ sending each subgroup $A \in \mathcal{H}$ to its full preimage $f^{-1}(A) \in G$.

First we show $f^{-1}(f(S)) = S$: The inclusion $\supset$ holds in general:

$$s \in S \implies f(s) \in f(S) \text{ (by definition) } \implies s \in f^{-1}(f(S)).$$

The other inclusion $\subset$ holds since $S \supset K$:

$$x \in f^{-1}(f(S)) \Longrightarrow f(x) \in f(S) \Longrightarrow f(x) = f(s) \text{ (for some } s \in S)$$

which implies $f(xs^{-1}) = 1$, and so $xs^{-1} \in K$, whence $x \in Ks \subset S$ since $K \subset S$.

Similarly $f(f^{-1}(A)) = A$: $\subset$ holds in general, and $\supset$ since $A \subset I$. Thus f is a bijection.

The rest is straightforward, and is left as an exercise for the reader; the UPQG is used to construct the isomorphism of quotient groups. □

Examples ① The First Isomorphism Theorem applied to det: $GL_n(\mathbb{R}) \to \mathbb{R}^\bullet$ gives $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\bullet$.

② The Diamond Isomorphism Theorem applied to any pair of distinct proper normal subgroups M and N of a group G gives isomorphisms

$$MN/M \cong N/(M \cap N) \quad \text{and} \quad MN/N \cong M/(M \cap N).$$

Note that if M and N are both "maximal" (i.e. not contained in any larger proper normal subgroups) then $MN = G$. Indeed, $M, N \lhd G$ implies $MN \lhd G$ by the usual argument ($mn \in MN$ and $x \in G$ implies $x(mn)x^{-1} = (xmx^{-1})(xnx^{-1}) \in MN$), and so $MN = G$ by the maximality of M and N. This is relevant to the following:

Application: Classification of Finite Groups

Definition A composition series for a finite group G is a sequence of subgroups

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_{n-1} \rhd G_n = 1$$

each a maximal proper normal subgroup of the preceeding.

The quotients G_i/G_{i+1} are simple, by the correspondence theorem, and G can be viewed as being built up from these composition factors, which are unique up to order by the "Jordan Hölder Theorem" (proved using the isomorphism theorems, in particular via Example ② above and induction on the order of the group).

Unfortunately $\exists$ distinct groups with identical composition factors, so the classification of finite groups is in fact a two-step program: the Hölder Program (late 19th century):

① Classify all simple finite groups
② Find all ways to "put simple groups together" to form other groups

The first step was recently achieved (∼1980): 18 infinite families

a) C_p (p prime)
b) A_n ($n \geq 5$)
c) $PSL_n(F)$ (F a finite field, $n \geq 2$) ... etc.

and 26 "sporadic" (exceptional) simple groups. The smallest sporadic group, of order 7920, was discovered by Mattieu in 1861. The largest, of order

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,268,000,000,000$$

was constructed by Fischer-Griess in 1981; it is known as the "monster" group.

Sylow Theory

Throughout this section

$$\boxed{G \text{ will denote a finite group of order } n.}$$

Recall Lagrange's Theorem: $\exists\, H < G$ with $|H| = k \Longrightarrow k|n$. The converse fails:

$$k|n \;\;\not\Longrightarrow \exists H < G,\;\, |H| = k.$$

For example

$$A_4 \;(\cong T_{12}) \text{ has no subgroup of order } 6$$

as proved above. (Another proof using quotient groups: Suppose $H < A_4$, $|H| = 6$. Then $H \lhd A_4$, so $A_4/H \cong C_2 \Longrightarrow H$ contains all eight 3-cycles τ in A_4, since $\tau H = (\tau H)^3 = \tau^3 H = H \Longrightarrow \tau \in H$. This contradicts $|H| = 6$.)

Partial converses hold:

2.26 **Cauchy's Theorem** *If p is prime and p divides n, then $\exists\, H < G$ with $|H| = p$ (or equivalently, G has an element of order p).*

More generally

2.27 **Sylow Theorem I** (Existence) *If p is prime and $p^k|n$, then $\exists\, H < G$ with $|H| = p^k$.*

Definition Let p be a prime. Any group P of order p^k is called a p-group, and if $P < G$ then P is called a p-subgroup of G. If in addition p^k is the *largest* power of p that divides $|G|$, that is

$$\boxed{n = p^k r \;\text{ and }\; p \nmid r}$$

then P is called a Sylow p-subgroup of G. (They always exist by Sylow I)

Example If $n = 500 = 2^2 5^3$, then G has subgroups of orders $2,\ 4,\ 5,\ 25$ and 125. The ones of order 4 are the Sylow-2 subgroups, and those of order 125 are the Sylow-5 subgroups.

2.28 **Sylow Theorem II** (Conjugacy) *Any two Sylow p-subgroups P, Q of G are conjugate, i.e. $\exists\, x \in G$ such that $Q = xPx^{-1}$.*

2.29 **Sylow Theorem III** (Counting) *The total number $n_p = n_p(G)$ of Sylow p-subgroups of G satisfies $\textcircled{a}$ $n_p|r$ and $\textcircled{b}$ $n_p \equiv 1 \pmod p$.*

Example If G has order $12 = 2^2 3$, then $n_3|4$ and $n_3 \equiv 1 \pmod 3$, so $n_3 = 1$ or 4. Either case may arise: $n_3(C_{12}) = 1$ and $n_3(A_4) = 4$ (the four Sylow 3-subgroups of A_4 are $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$ and $\langle(234)\rangle$). Similarly $n_2 = 1$ or 3, e.g. $n_2(C_{12}) = n_2(A_4) = 1$ while $n_2(D_{12}) = 3$ (can you find all three Sylow-2 subgroups of D_{12}?).

Application (non-simplicity results)

Observe that if a finite group G has only one Sylow p-subgroup P, for some prime divisor p of $|G|$, then $P \lhd G$ (since any xPx^{-1} is also a Sylow p-subgroup of G). Thus

$$n_p(G) = 1 \Longrightarrow G \text{ is not simple}$$

if G is not a p-group. (It can also be shown that the only p-group that is simple is C_p, see below). It's often not hard to show some $n_p = 1$:

2.30 Theorem

① *$|G| = pq$ for distinct primes p and q $\implies$ G is not simple. For example, no groups of order $6, 10, 14, 15, 21, 22, 26, 33, \ldots$ are simple.*

② *$|G| = 30 = 2 \cdot 3 \cdot 5$ $\implies$ G is not simple.*

Proof ① We may assume $p > q$, and then $n_p | q$ and $n_p \equiv 1 \pmod{p}$, by Sylow III, which forces $n_p = 1$.[†]

② The possibilities (using Sylow III) are $n_2 = 1, 3, 5, 15$, $n_3 = 1, 10$ and $n_5 = 1, 6$. Thus if G is simple, then $n_2 \geq 3$, $n_3 = 10$ and $n_5 = 6$

Now observe that if P and Q are distinct Sylow subgroups of G, then $P \cap Q = 1$. This is true in general if P and Q are associated with distinct primes, since $P \cap Q$ is a subgroup of both P and Q, and so $|P \cap Q|$ divides both $|P|$ and $|Q|$ $\implies$ $|P \cap Q| = 1$ (since $|P|$ and $|Q|$ are relatively prime). If P and Q are associated with the same prime p and are of prime order (this is the case for $n = 30$ since 30 is square free), then $P \cap Q$ must be trivial since it is a proper subgroup of P and $|P| = p$. (Note that two Sylow p-subgroups that are not of prime order may overlap nontrivially!)

Finally, count the nonidentity elements in G, using the fact that the Sylow subgroups don't overlap: $|G| > 6 \cdot 4 + 2 \cdot 10 + 1 \cdot 3 = 47 \Rightarrow\Leftarrow$. Thus G is not simple. □

More is known: No group of order pqr is simple, where p, q and r are distinct primes (HW; counting argument as in ②). Similarly groups of order $p^2 q$ and p^α (for any $\alpha > 1$) are never simple. Much deeper results:

2.31 Burnside Theorem *$|G| = p^\alpha q^\beta \implies G$ is not simple.*

2.32 Feit-Thompson Theorem *$|G|$ odd (but not prime) $\implies G$ is not simple*

Proofs of Sylow Theorems (using group actions)

Let $G \times X \to X$, $(g, x) \mapsto g \cdot x$ be an action of a group G on a set X. For any $x \in X$, define the orbit of x to be

$$Gx = \{g \cdot x \mid g \in G\} \subset X$$

and the stabilizer (or isotropy subgroup) of x to be

$$G_x = \{G \in G \mid g \cdot x = x\} < G.$$

(note the subscript). Call x a fixed point of the action if $g \cdot x = x$ for all $g \in G$, or equivalently $Gx = \{x\}$, or $G_x = G$. Let $X^G = \{\text{all fixed points}\}$.

The most important theorem in the subject is:

2.33 Orbit Stabilizer Theorem (OST) *If G and X are finite, then the size of any orbit Gx is equal to the index of the corresponding stabilizer G_x. In symbols $|Gx| = |G : G_x|$, or equivalently $|G| = |Gx||G_x|$.*

[†] In fact, Sylow theory gives more information. For example, if $q \nmid (p-1)$, then G is in fact cyclic! Indeed Sylow III then gives $n_q = 1$ as well, so G has a unique Sylow p-subgroup $P \cong C_p$ and a unique Sylow q-subroup $Q \cong C_q$. Thus $P, Q \lhd G$ and $P \cap Q = 1$, and Lagrange's Theorem shows that $PQ = G$, and so $G \cong P \times Q \cong C_{pq}$, by the product recognition theorem. This shows that all groups of order $15, 33, \ldots$ are cyclic.

Proof The function $G/G_x \to Gx$, $gG_x \mapsto g \cdot x$ is a well defined bijection: $gG_x = hG_x \iff g^{-1}h \in G_x \iff g^{-1} \cdot h \cdot x = x \iff h \cdot x = g \cdot x$. □

Examples (1) Let G act on itself by conjugation, $g \cdot x = gxg^{-1}$. Then $Gx = C(x)$ (the conjugacy class of x), $G_x = Z(x)$ (the centralizer of x) and $G^G = Z(G)$ (the center of G). The OST says

$$|C(x)| = |G : Z(x)|.$$

(2) Let G act on the set X of all its subgroups by conjugation, $g \cdot S = gSg^{-1}$. Then $GS = C(S) = \{\text{conjugates of } S\}$, $G_S = N(S)$ (the normalizer of S) and $X^G = \{\text{normal subgroups of } G\}$. The OST says

$$|C(S)| = |G : N(S)|.$$

Now observe that the orbits of an action of G on X partition X (since $Gx \cap Gy \neq \varnothing \implies g \cdot x = h \cdot y$ for some $g, h \in G \implies k \cdot y = (kh^{-1}g) \cdot x \implies Gy \subset Gx$, and similarly $Gx \subset Gy$, so $Gx = Gy$). Thus

$$|X| = \sum |Gx_i|$$

where the sum is over a set of representatives x_i, one chosen from each orbit. Since $|Gx| = |G : G_x|$ by the OST, the right hand side can be rewritten as $\sum |G : G_{x_i}| = |X^G| + \sum |G : G_{x_i}|$ where the last sum is only over those x_i that are not fixed points. This gives the class equation (for finite X and G)

$$|X| = |X^G| + \sum |G : G_{x_i}|$$

summed over representatives x_i of the non-trivial orbits. In the special case when G acts on itself by conjugation, as in Example (1) above, this reads

$$|G| = |Z(G)| + \sum |G : Z(x_i)|$$

summed over representatives of the non-trivial conjugacy classes.

One very useful consequence of the general class equation, which is the key to our proof of Sylow's Theorems, is

2.34 Lemma *If a p-group P acts on a finite set X, then $|X| \equiv |X^P| \pmod p$.*

Proof The class equation says $|X| = |X^P| + \sum |P : H_i|$, where the H_i are proper subgps of P, and each $|P : H_i| \equiv 0 \pmod p$ since P is a p-group, so $|X| \equiv |X^P| \pmod p$. □

2.35 Corollary *The center Z of any nontrivial p-group P is nontrivial.*[†]

Proof Let P act on itself by conjugation. Then the fixed point set is Z, which by the lemma has order divisible by p, so cannot be trivial. □

Now we are ready to prove Sylow's Theorems.

Proof of Sylow I The result is obvious if G is the trivial group, so we suppose G nontrivial and induct on its order $|G| = p^k r$ (with $p \nmid r$) assuming the result for groups of smaller order. Set Z = center of G.

[†] It follows that if $|P| = p^2$, then P is abelian: Assume not. Then Z is cyclic of order p by the Corollary and Lagrange's Theorem, so P/Z is also cyclic of order p, say generated say by some xZ. But then any element in P is of the form $x^k u$ for some $k \in \mathbb{Z}$, $u \in Z$ and so P is in fact abelian (since $\forall u, v \in Z$, $x^k u x^\ell v = x^{k+\ell} uv = x^\ell v x^k u$) contrary to our assumption.

Case 1: p divides $|Z|$. Then it follows easily from the structure theorem for finite abelian groups that Z has a subgroup P of order $p \Longrightarrow |G/Z| = p^{k-1}r \Longrightarrow$ (by induction) G/P has subgroups of order $1, p \ldots, p^{\alpha-1} \Longrightarrow$ (by the correspondence theorem) G has subgroups of order $1, p, \ldots, p^k$.

Case 2: p does not divide $|Z|$. Then by the class equation, p does not divide the index of the centralizer $Z(x)$ of some $x \notin Z \Longrightarrow p^k$ divides $|Z(x)| \Longrightarrow$ (by induction) $Z(x)$ has subgroups of order $1, p, \ldots, p^k \Longrightarrow G$ does as well. □

Proof of Sylow II For any two Sylow p-subgroups P and Q of G, let P act by left multiplication on G/Q. Since $|G/Q| = r \not\equiv 0 \pmod{p}$, it follows from the lemma that $\exists$ a fixed point xQ, i.e. for all $g \in P$, have

$$gxQ = xQ \Longrightarrow gx \in xQ \Longrightarrow g \in xQx^{-1}.$$

Thus $P \subset xQx^{-1}$, and so they are equal since they have the same order. □

Note : This proof shows that any p-subgroup of G is a subset of some Sylow p-subgroup.

Proof of Sylow III Let $X = \{\text{Sylow } p\text{-subgroups of } G\}$, so

$$n_p = |X|.$$

Choose $P \in X$ (by Sylow I) so $X = C(P)$, the set of all subgroups conjugate to P (by Sylow II). Thus $|X| = |G : N(P)|$ (see example ② on page 40), which is a divisor of $r = |G : P| = |G : N(P)||N(P) : P|$, i.e. $n_p|r$.

To see $n_p \equiv 1 \pmod{p}$, consider the action of P on X by conjugation. Since $n_p|r$, we have $n_p \not\equiv 0 \pmod{p} \Longrightarrow \exists$ a fixed point $Q \in X$, i.e. $P \subset N(Q)$. But this forces $P = Q$, since $Q \lhd N(Q)$ (by definition) and so Q is the only Sylow p-subgroup of $N(Q)$. Thus P is the *unique* fixed point of this action, so $n_p \equiv 1 \pmod{p}$ by the lemma. □

Exercise ① Find all orders $n < 100$ for which Sylow III applies directly (without extra counting arguments as above) to produce a normal Sylow subgroup. (Answer: all except $n = 12, 24, 30, 36, 48, 56, 60, 72, 80, 90, 96$)

② Show that S_4 (of order 24) has no normal Sylow subgroups, but that every group of order less than 24 has at least one such subgroup.

Remark It is an immediate consequence of Burnside's Theorem that no groups of order $2^k \cdot 3$ (e.g. of order 12, 24, 48 or 96) are simple. This can also be proved in an elementary way as follows. Let G be a noncyclic group of order $n = p^k r$, with $p \nmid r$ as usual. Then

$$n_p = 1 \implies G \text{ is not simple}$$

This can be strengthened to

$$n \nmid n_p! \implies G \text{ is not simple.}$$

The proof is slick, but easy: Let G act by conjugation on the set of all Sylow-p subgroups of G, with associated permutation homomorphism $\rho : G \to S_{n_p}$. Thus if G is simple, then $\ker(\rho)$ is trivial, so ρ is one-to-one, so n divides $n_p!$ by Lagrange's Theorem, as claimed.

Furthermore $n_p|r$ by Sylow counting, so (continuing to assume G is simple) we see that n divides $n_p!$ (as shown above) which divides $r!$. Thus p^k divides $(r-1)!$, which clearly puts a lower bound on r. For example, if $n = 2^k \cdot 3$, then for G to be simple we would need 2^k to divide $2!$, i.e. $k = 1$, but by hand we see that no group of order 6 is simple.

Alternative Proof of Sylow I and III (November 2019)

Let $s_d(G)$ denote the number of subgroups of order d in a finite group G of order n. Thus $s_d(G)$ is zero if d does not divide n, by Lagrange's Theorem, but may also be zero when d does divide n (e.g. $s_6(A_4) = 0$). Sylow's Theorem III shows that if if d is the *maximal* power of a prime p that divides n, then $s_d(G) \equiv 1 \pmod{p}$ (and thus $s_d(G) \geq 1$, proving Sylow I as well). The following theorem of Frobenius generalizes this result:

Frobenius' Theorem (1895) *If d divides n and is a power of a prime p, then $s_d(G) \equiv_p 1$.*

Proof: We show more generally that for arbitrary divisors d of n

$$(\star) \qquad s_d(G) \;=\; \binom{n-1}{d-1} - s$$

where s is a sum of nontrivial (i.e. $\neq 1$) divisors of d. The theorem follows: If d is a p-power then $s \equiv_p 0$, so the mod p reduction of $s_d(G)$ depends only on the order of G, not on its structure. Thus $s_d(G) \equiv_p s_d(\text{cyclic group of order } n) = 1$.

Now here's the proof of $(\star)$:

Let X be the set of all subsets of G of size d, so $|X| = \binom{n}{d}$, and $s_d(G)$ is the number of elements of X that are actually subgroups.

Let G act on X by left multiplication. There are two types of orbits: "good" ones that contain a subgroup, and "bad" ones that don't. In fact any good orbit $\mathcal{O}$ contains *exactly one* subgroup S, since by definition $\mathcal{O} = G/S$, the set of left cosets of S in G. Thus $s_d(G)$ *is the number of good orbits, and each good orbit contains n/d elements.*

Now let $\mathcal{O}$ be a bad orbit. By an obvious translation, $\mathcal{O}$ has an element S that contains the identity element of G. Let H denote the stabilizer of S. Then H is a proper subset of $HS = S$ (proper since S is not a subgroup) of order dividing the order of S (since $S = HS$ is a union of right cosets of H). That is, $|H| = d/d_{\mathcal{O}}$ for some nontrivial divisor $d_{\mathcal{O}}$ of d. Thus by the orbit stabilizer theorem, $|\mathcal{O}| = n/|H| = nd_{\mathcal{O}}/d$.

Now since X is the union of all the orbits,

$$|X| \;=\; \binom{n}{d} \;=\; \frac{n}{d}\left(s_d(G) + \sum d_{\mathcal{O}}\right)$$

where the last sum is over bad orbits, and the result follows since $\frac{d}{n}\binom{n}{d} \;=\; \binom{n-1}{d-1}$. □

3. Rings

Basic Concepts

Definition A ring is a set R with two binary operations $+$ and $\cdot$ satisfying

ⓐ $(R, +)$ is an abelian group (with identity 0),
ⓑ $(R, \cdot)$ is a semigroup, and
ⓒ $\cdot$ is distributive over $+$ (on both sides)

Make sure you know what this entails (e.g. distributivity says that $r(s+t) = rs + rt$ and $(s+t)r = sr + tr$, $\forall r, s, t \in R$). Say R is a ring with 1 if it contains a multiplicative identity element, and R is commutative if multiplication is commutative.

A subset $S \subset R$ is a subring of R, denoted $S < R$, if $0 \in S$ and $s, t \in S \implies -s,\ s+t$ and $st \in S$. Can show (as in group theory) that $S < R \iff S$ is nonempty and closed under subtraction and multiplication.

Examples ① The trivial ring $R = \{0\}$ is commutative with $1 = 0$.

② $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C} < \mathbb{H}$ are all rings with 1, and all but the last are commutative.

③ $\mathbb{Z}_n$ is a commutative ring with 1, for any $n \in \mathbb{N}$.

④ The set $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ of Gaussian integers is a subring of $\mathbb{C}$. Similarly

$$\mathbb{Z}[u] := \{a + bu \mid a, b \in \mathbb{Z}\} \ < \ \mathbb{C} \quad \text{where} \quad u = e^{2\pi i/3} \in \mathbb{C}.$$

This ring will play a special role in the proof below of Fermat's last theorem for $n = 3$. (Picture these rings as square/triangular lattice points in the complex plane)

⑤ (new rings from old) For any rings R and S have

a) the product $R \times S$ with component-wise operations
b) matrix rings $M_n(R)$ of $n \times n$ matrices with entries in R with the usual addition and multiplication of matrices
c) polynomial rings $R[x] = \{\sum_{i=0}^n r_i x^i \mid r_i \in R\}$ with the usual addition and multiplication of polynomials, and in more variables $R[x, y]$, $R[x, y, z]$, etc.
d) power series rings $R[[x]] = \{\sum_{i=0}^\infty r_i x^i \mid r_i \in R\}$, $R[[x, y]]$, etc.
e) group rings $RG = \{\sum_{=0}^n r_i g_i \mid r_i \in R, g_i \in G\}$ of G (any group) over R, with the operations $\sum_{i=0}^n r_i g_i + \sum_{i=0}^n s_i g_i = \sum_{i=0}^n (r_i + s_i) g_i$ and $(\sum_{i=0}^n r_i g_i)(\sum_{j=0}^n s_j g_j) = \sum_{i,j=0}^n (r_i s_j) g_i g_j$
f) function rings The set $[X, R]$ of all functions from a set X to R under the operations $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$.

Remark Many familiar properties of $\mathbb{Z}$ generalize to allrings, for example ⓐ $0r = 0$, ⓑ $(-r)s = r(-s) = -(rs)$, ⓒ $-1 \cdot r = -r$ (in rings with 1); see the text for proofs. But not all, e.g. commutativity. Also, it is not true in general(even in commutative rings) that

$$rs = 0 \implies r \text{ or } s = 0$$

e.g. $2 \cdot 2 = 0$ in $\mathbb{Z}_4$. Commutative rings with $1 \neq 0$ wherethis holds are called integral domains (more on this below).

Definition A function $f : R \to S$, where R and S are rings, is called a ring homomorphism if

$$f(r+s) = f(r) + f(s) \text{ and } f(rs) = f(r)f(s)$$

for all $r, s \in R$. If R and S are rings with identity, often also require that $f(1) = 1$. The kernel of f, denoted $\ker(f)$ is defined to be the set of all elements in R that f maps to 0 (not to 1), and the image $\mathrm{Im}(f)$ is defined in the usual way. Both are subrings (of R and S respectively). Have the usual criterion f is 1-1 $\iff \ker(f) = \{0\}$.

Examples ① $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(k) = \overline{k}$ is an epimorphism with kernel $n\mathbb{Z}$.

② $g : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $g(k) = (\overline{k}, \overline{k})$ (e.g. if $m = 5, n = 9$ then $f(13) = (3, 4)$) is a homomorphism with kernel $\ell\mathbb{Z}$, where ℓ is the lcm of m and n.

Ideals and Quotient Rings

Definition A subring A of a ring R is an ideal in R, denoted $A \lhd R$, if Ra and aR are subsets of A for every $a \in A$, i.e. A is closed under multiplication on the left or right by arbitrary elements of R. (Here $Ra = \{ra \,|\, r \in R\}$, etc.)

ideals are the ring theory analogue of normal subgroups in group theory

Examples ⓪ For any ring R, both $\{0\}$ and R are ideals.

① $n\mathbb{Z} \lhd \mathbb{Z}$ for any n (these are the only ideals in $\mathbb{Z}$).

② Let R be a commutative ring with 1 and $a \in R$. Then $aR = Ra$ (also denoted $\langle a \rangle$) is an ideal in R containing a (verify this) called the principal ideal generated by a. An ideal $J \lhd R$ is called a principal ideal if $J = \langle a \rangle$ for some $a \in R$.

③ Let $f : R \to S$ be a ring morphism. Then $\ker(f) \lhd R$ (verify this).

Definition Given an ideal J in a ring R, define the quotient ring R/J to be the set of cosets $\{r + J \mid r \in R\}$ with operations $+$ and $\cdot$ defined in the obvious way

$$(r+J) + (s+J) = (r+s) + J \quad \text{and} \quad (r+J)(s+J) = (rs) + J.$$

These operations are well-defined (e.g. for multiplication: if $r + J = r' + J$, i.e. $r - r' \in J$, then $rs - r's = (r - r')s \in J$, so $rs + J = r's + J$; similarly independent of the choice of rep for $s + J$). They make R/J into a ring; the additive identity is $0 + J = J$ and the negative of $r + J$ is $(-r) + J$.

There's a universal property, as for groups, and isomorphism theorems, e.g.:

3.1 First Isomorphism Theorem (for rings) *If $f : R \to S$ is a ring homomorphism, then $R/\ker(f) \cong \mathrm{Im}(f)$.*

Examples ① Using $f : \mathbb{Z} \to \mathbb{Z}_n$ of example ① in §1, have $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

② Using $g : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ of example ② in §1, have $\mathrm{Im}(g) \cong \mathbb{Z}/\ell\mathbb{Z}$, where $\ell = \mathrm{lcm}(m, n)$. In particular, if m and n are relatively prime, so $\ell = mn$, then (counting elements) we see that g induces an isomorphism

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \qquad \text{if } (m, n) = 1$$

mapping $\overline{k}$ to $(\overline{k}, \overline{k})$. This $\Longrightarrow$ the "Chinese Remainder Theorem" that states that for any $a, b \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ satisfying the system of congruences

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

and all other solutions are of the form $x + kmn$ for some $k \in \mathbb{Z}$. For example, if $m = 5, n = 9$ and $a = 2, b = 8$, then have the solution set $\{17 + 45k \mid k \in \mathbb{Z}\}$.

Integral Domains and Fields

Throughout this section, assume R is a commutative ring with $1 \neq 0$.

Definition A nonzero element $a \in R$ is ⓐ a zero divisor if $\exists\, b \in R - 0$ such that $ab = 0$ ⓑ a unit if $\exists\, b \in R$ such that $ab = 1$ (Note that b is unique, if it exists, and is denoted a^{-1}.) Two elements $a, b \in R$ are associates, written $a \sim b$, if $a = bu$ for some unit u.

Set $R^\circ = \{\text{zero divisors in } R\}$ and $R^\bullet = \{\text{units in } R\}$. Then

$$R^\circ \cap R^\bullet = \varnothing$$

since $a \in R^\circ \cap R^\bullet \Longrightarrow 0 = ab$ for some $b \neq 0 \Longrightarrow b = a^{-1}ab = a^{-1}0 = 0$ which is a contradiction.

Definition [†] R is called an integral domain (or just a domain) if it has no zero divisors (i.e. $R^\circ = \varnothing$), and a field if all nonzero elements are units (i.e. $R^\bullet = R - \{0\}$).

Clearly every field is a domain (since $R^\circ \cap R^\bullet = \varnothing$) but not conversely (e.g. $\mathbb{Z}$ is a domain but not a field). There is a useful characterization of fields in terms of ideals:

3.2 Lemma [†] *R is a field $\Longleftrightarrow$ R has no proper ideals.*

Proof ($\Longrightarrow$) For any nonzero ideal J, choose $a \neq 0$ in J. Then for any $r \in R$ have $r = ra^{-1}a \in J$, so $J = R$. ($\Longleftarrow$) For any $a \neq 0$ in R, the principal ideal $aR \neq 0$, so by hypothesis $aR = R$. Thus $\exists r \in R$ such that $ar = 1$ so a is a unit. Thus R is a field. □

There are two special kinds of ideals that relate to these notions:

Definition[†] Let J be a proper ideal in R (note that $J = \{0\}$ is allowed). Then J is prime if $ab \in J \Longrightarrow a \in J$ or $b \in J$, and J is maximal if $J \subset K \lhd R \Longrightarrow K = J$ or $K = R$.

Exercise R is a domain $\Longleftrightarrow$ $\{0\}$ is a prime ideal.

3.3 Theorem *Let R be a commutative ring with $1 \neq 0$ and $J \lhd R$. Then ⓐ J is prime $\Longleftrightarrow$ R/J is a domain ⓑ J is maximal $\Longleftrightarrow$ R/J is a field.*

Proof ⓐ HW ⓑ By the correspondence theorem J is maximal $\Longleftrightarrow$ R/J has no proper ideals, and this is equivalent to R/J being a field by the previous lemma. □

Examples ① $n\mathbb{Z} \lhd \mathbb{Z}$ is prime $\Longleftrightarrow$ maximal $\Longleftrightarrow$ n is a prime number.

② In general, maximal ideals are always prime (HW) but not conversely. For example $\langle x \rangle \lhd \mathbb{Z}[x]$ consisting of all polynomials with 0 constant term) is prime but not maximal: $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ (and now apply the theorem).

[†] Recall that we are assuming that R is a commutative ring with $1 \neq 0$.

Coda

3.4 **Fermat's Last Theorem** (1637, proved by A. Wiles in 1995) *For $n \geq 3$, the equation*

$$x^n + y^n = z^n$$

has no non-zero integral solutions x, y, z. (Call this FLT_n for any given n.)

Remarks ① $\mathrm{FLT}_n \Longrightarrow \mathrm{FLT}_{kn}$, since any solution x, y, z for kn would give the solution x^k, y^k, z^k for n. Fermat knew a proof for $n = 4$, and so this reduces the proof to the case of odd primes, i.e. it suffices to prove that

$$x^p + y^p = z^p$$

has no non-zero integral solutions x, y, z for any odd prime p.

② A solution x, y, z is primitive if x, y and z are nonzero and have no common factor. Enough to prove $\nexists$ primitive solutions (since any soln cx, cy, cz gives another x, y, z). Note x, y, z primitive solution $\Longrightarrow$ pairwise relatively prime.

③ Proof for $p = 3$ (which we give below) was known to Euler, for $p = 5$ to Dirichlet & Legendre, for $p = 7$ to Gabriel Lamé. Indeed Lamé and Cauchy (independently) thought they had it all. Their approach was to show $\nexists$ any solutions in the bigger ring

$$\Lambda_p := \mathbb{Z}[\zeta_p] = \{\text{polys in } \zeta_p \text{ with } \mathbb{Z} \text{ coeffs}\}$$

where $\zeta_p = e^{2\pi i/p}$; their mistake, uncovered by Kummer, was to assume that Λ_p has *unique factorization into primes* (as $\mathbb{Z}$ does) which in fact it does *only* for $p \leq 19$. Kummer's work led him to introduce "ideals" which then led to modern ring theory.

Proof (for $n = 3$) Set $\zeta = \zeta_3$ and $\Lambda = \Lambda_3 = \mathbb{Z}[\zeta]$. We will show that for any unit $u \in \Lambda^\bullet$,

$$x^3 + y^3 = uz^3$$

has no primitive solutions in Λ (FLT is the case $u = 1$). Note that

$$\Lambda^\bullet = \{\pm 1, \pm\zeta, \pm\zeta^2\}$$

as seen by inspection (since these are the elements of complex norm 1 in Λ, and all other elements have norm > 1).

It is a fact (which we won't prove here) that any nonzero, nonunit in Λ can be factored uniquely (up to order and replacement by associates) as a product of primes (nonunits whose only divisors are their associates and units). One such prime is $p := \zeta - 1$. Why is p prime? Well, $|p| = \sqrt{3}$ which is the smallest norm achieved by a nonunit in Λ, so if $p = ab$ then $|p| = |a||b| \Longrightarrow |a|$ or $|b| = 1$, i.e. a or $b \in \Lambda^\bullet$.

Remarks ① 3 is not prime in Λ, but factors as $3 = p^2 u$, where $u = -\zeta^2$. Thus $p^2 | 3$ (also written $3 \equiv_{p^2} 0$) but $p^3 \nmid 3$ ($3 \not\equiv_{p^3} 0$).

② Each $a \in \Lambda$ can be written uniquely in the form $a = \overline{a} + rp$ for some $r \in \Lambda$ where $\overline{a} = 0$, 1 or -1. This defines an isomorphism

$$\Lambda/p\Lambda \to \mathbb{Z}_3 \ , \quad a + p\Lambda \mapsto \overline{a}$$

To show this, write a as a poly w/ integral coeff in ζ, and thus in p by substituting $p+1$ for ζ. Now reduce the constant term to 0 or ± 1 using ① For example $\overline{u} = \pm 1$ for any $u \in \Lambda^\bullet$; in particular $\overline{\zeta} = \overline{\zeta^2} = 1$.

$\textcircled{3}$ For any $a \in \Lambda$, have $a^3 \equiv_{p^3} \overline{a}$. Proof: $a = \overline{a} + rp$, by $\textcircled{2}$, so $a^3 = \overline{a}^3 + 3\overline{a}^2rp + 3\overline{a}r^2p^2 + r^3p^3 \equiv_{p^3} \overline{a}^3$ (by $\textcircled{1}$) $= \overline{a}$.

Now suppose x_o, y_o, z_o is a primitive solution to

$$x^3 + y^3 = uz^3$$

for some unit u. This is Fermat's equation when $u = 1$, but as we shall see, it is easier to prove simultaneously that *none* of these six equations (for the various units u) have solutions.

Case 1 $p \nmid x_oy_oz_o$. Then by the remarks above, $\overline{x}_o, \overline{y}_o, \overline{z}_o = \pm 1 \implies 0 = x_o^3 + y_o^3 - uz_o^3 \equiv_{p^3} \overline{x}_o + \overline{y}_o \pm \overline{z}_o = \pm 1$ or $\pm 3 \not\equiv_{p^3} 0 \Rightarrow\Leftarrow$.

Case 2 $p \mid x_oy_oz_o$. Then p divides *exactly one* of x_o, y_o, z_o, since they are pairwise relatively prime.

Case 2a Suppose $p \,|\, z_o$. Then $\overline{x}_o = -\overline{y}_o = \pm 1$, so without loss of generality, $x_o = rp + 1$ and $y_o = sp - 1$ for suitable $r, s \in \Lambda$.

Let k be the largest natural number for which $p^k \,|\, z_o$, called the p-order of the solution. A simple calculation (reducing mod p^4) shows that in fact $k \geq 2$.[†] We assume that the solution was chosen so that k is minimal.

Now (and this is the magic!) define

$$a = \frac{x_o + y_o}{p} \qquad b = \frac{\zeta x_o + \zeta^2 y_o}{p} \qquad c = \frac{\zeta^2 x_o + \zeta y_o}{p}.$$

The numerators are all divisible by p (e.g. for b, $\overline{\zeta x_o + \zeta^2 y_o} = \overline{x}_o + \overline{y}_o = 0$) and so $a, b, c \in \Lambda$. A straightforward argument, using the fact that $\zeta^3 = 1$ and $1 + \zeta + \zeta^2 = 0$, shows

$\textcircled{1}$ $a + b + c = 0$ $\qquad$ $\textcircled{2}$ $abc = (x_o^3 + y_o^3)/p^3 = u(z_o/p)^3$

$\textcircled{3}$ a, b, c are *pairwise relatively prime*, i.e. have no common prime factors (to see this, note that x_o, y_o are linearly related to any pair of a, b, c, and so a common factor for such a pair would yield one for x_o, y_o).

$\textcircled{2}$ and $\textcircled{3}$ show that each of a, b, c is a unit times a cube, and that these cubes are relatively prime. It follows from $\textcircled{1}$ that $\exists\, x_1, y_1, z_1$ with x_1^3, y_1^3, z_1^3 associates of a, b, c, in some order, such that $p \nmid x_1$, $p \nmid y_1$, $p \,|\, z_1$, $p^k \nmid z_1$, and

$$x_1^3 + vy_1^3 + wz_1^3 = 0$$

for suitable units v, w. It is easy to check that $v = \pm 1$ (since the left side is congruent mod p^3 to $\overline{x}_1 + v\overline{y}_1 = \pm 1 \pm v \implies v \equiv p^3 \pm 1 \implies v = \pm 1$) so this gives a new solution $x_1, \pm y_1, z_1$ of smaller p-order to one of the original equations, contradicting the minimality of k.

Case 2b Suppose $p \,|\, x_o$ (or y_o). Then $u\overline{z} \equiv_{p^3} \overline{x} + \overline{y} \implies u \equiv_{p^3} \pm 1 \implies u = \pm 1 \implies (-y_o)^3 + (\pm z_o)^3 = x_o^3$, which is handled in case 2a.

Thus Fermat's Last Theorem for $n = 3$ is proved. □

[†] $x_0^3 + y_0^3 = (rp + 1)^3 + (sp - 1)^3 \equiv_{p^4} r^3 + s^3 - \zeta^2(r + s))p^3 \equiv_{p^4} (\overline{r} + \overline{s} - (\overline{r} + \overline{s}))p^3 = 0 \implies z \equiv_{p^2} 0$.

Addendum: Alternative Proof of Abel's Theorem (November 2019 [†])

Given any nontrivial normal subgroup H of A_n for $n \geq 5$, we must show $H = A_n$. It suffices to show that H contains at least one 3-cycle, say σ, for then it contains all of them (any other is conjugate to σ by an element in S_n, which can be chosen in A_n by multiplying if needed by a transposition that commutes with σ, which exists since $n \geq 5$), and A_n is generated by 3-cycles (each element in A_n is a product of an even number of transpositions, which pairwise can be rewritten in terms of 3-cycles: $(i\ j)(j\ k) = (i\ j\ k)$, $(i\ j)(k\ \ell) = (i\ j\ k)(j\ k\ \ell)$").

To show H contains a 3-cycle, first note that the 3-cycles have the largest fixed point sets among all nonidentity elements in A_n. So the idea is to start with any nontrivial element h in H, and to give a way to modify it (if it's not a 3-cycle) to obtain one with more fixed points: Choose any 3-cycle σ in A_n that does not commute with h. (For example if $h(1) = 2$, then choose σ to fix 1 but move 2; this uses $n \geq 4$.) Then the commutator

$$x \ := \ [\sigma, h] \ = \ (\sigma h \sigma^{-1})h^{-1} \ = \ \sigma(h\sigma^{-1}h^{-1})$$

is a nontrivial element in H (by the second equality) that is also a product $x = \sigma\tau$ of two 3-cycles, where $\tau = h\sigma^{-1}h^{-1}$ (by the third), so it has at least $n - 6$ fixed points.

If σ and τ are disjoint, say $\sigma = (1\,2\,3)$ and $\tau = (4\,5\,6)$, then $x = (1\,2\,3)(4\,5\,6)$ commutes with an odd permutation $\alpha = (1\,4)(2\,5)(3\,6)$, so H contains *all* products of two disjoint 3-cycles (indeed any two such are conjugate by *some* permutation, which can be multiplied by α if necessary to make it even), in particular $y = \sigma\tau^2$. Thus $xy = \sigma^2$ is a 3-cycle in H.

If σ and τ overlap singly, say $\sigma = (1\,2\,3)$ and $\tau = (3\,4\,5)$, then $x = (1\,2\,3\,4\,5)$ is a 5-cycle, which can be multiplied by an A_n-conjugate of itself to give a 3-cycle in H: $x(\mu x \mu^{-1}) = (1\,4\,2)$ where $\mu = (1\,3\,5)$.

If σ and τ overlap doubly, say $\sigma = (1\,2\,3)$ and $\tau = (4\,3\,2)$ or $(2\,3\,4)$, then x is either a 3-cycle $(1\,2\,4)$ or a product of two disjoint 2-cycles $(1\,2)(3\,4)$, and in the latter case (using $n \geq 5$) x can be multiplied by an A_n-conjugate of itself to give a 3-cycle in H: $x(\mu x \mu^{-1}) = ((1\,2)(3\,4))((1\,2)(4\,5)) = (3\ 4\ 5)$ where $\mu = (3\ 4\ 5)$.

If σ and τ overlap triply, then $\sigma = \tau$ (since $x \neq 1$) so $x = \sigma^2$ is itself a 3-cycle.

[†] inspired in part by Ken Brown's Cornell Math 4340 Lecture Notes (2009Brown.Alternating.pdf).