

# Abstract Algebra

Paul Melvin  
Bryn Mawr College  
Fall 2011

lecture notes loosely based on Dummit and Foote's text

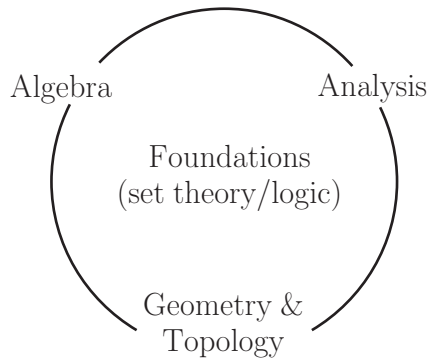
Abstract Algebra (3rd ed)

Prerequisite:

Linear Algebra (203)

# Introduction

## Pure Mathematics



## What is Algebra?

- Number systems  $\mathbb{N} = \{1, 2, 3, \dots\}$  “natural numbers”

$$\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\} \quad \text{“integers”}$$

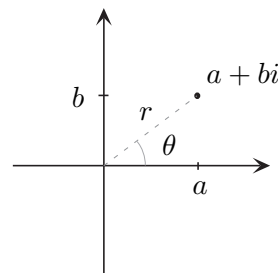
$$\mathbb{Q} = \{\text{fractions}\} \quad \text{“rational numbers”}$$

$$\mathbb{R} = \{\text{decimals}\} = \text{pts on the line} \quad \text{“real numbers”}$$

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\} = \text{pts in the plane} \quad \text{“complex nos”}$$

|| polar form

$$re^{i\theta}, \text{ where } a = r \cos \theta, b = r \sin \theta$$



Note  $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$  (all proper inclusions, e.g.  $\sqrt{2} \notin \mathbb{Q}$ ; exercise)  
There are many other important number systems inside  $\mathbb{C}$ .

- Structure “binary operations”  $+$  and  $\cdot$

associative, commutative, and distributive properties  
 “identity elements” 0 and 1 for  $+$  and  $\cdot$  resp.

solve equations, e.g. ①  $ax^2 + bx + c = 0$  has two (complex) solutions

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

②  $x^2 + y^2 = z^2$  has infinitely many solutions, even in  $\mathbb{N}$   
 (the “Pythagorean triples”: (3,4,5), (5,12,13), ...).

③  $x^n + y^n = z^n$  has no solutions  $x, y, z \in \mathbb{N}$  for any fixed  $n \geq 3$   
 (Fermat’s Last Theorem, proved in 1995 by Andrew Wiles; we’ll give  
 a proof for  $n = 3$  at end of semester).

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

A group is a set  $G$  with an associative binary operation  $*$  which has  
 an identity element  $e$  ( $x * e = x = e * x$  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  $(\mathbb{N}, +)$  is not a group: no identity.  $(\mathbb{Z}, +)$  is.  $(\mathbb{Z}, \cdot)$  is not:  
 no inverses.  $(\mathbb{Q}, \cdot)$  isn’t, but  $(\mathbb{Q} - \{0\}, \cdot)$  is.

Focus of first semester: groups and rings

Some history Theory of equations ( $\rightsquigarrow$  modern algebra)

- Quadratic equation (antiquity)

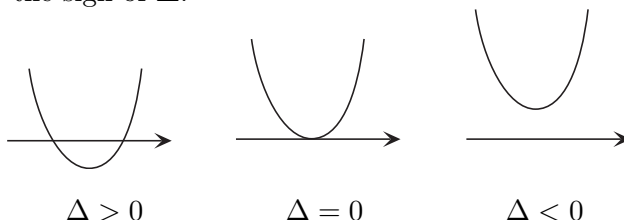
$$ax^2 + bx + c = 0$$

Divide by  $a$  and complete the square, i.e. substitute  $y = x + b/2a$  to get

$$y^2 + p = 0$$

where  $p = c/a - (b/2a)^2$ . The roots are  $y = \pm\sqrt{-p}$  which gives the usual  
 formula by substitution.

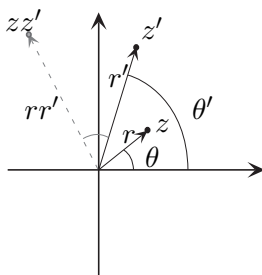
Remark  $\Delta = b^2 - 4ac = -4a^2p$  is called the discriminant of the polynomial  $ax^2 + bx + c$ . If  $a, b, c \in \mathbb{R}$ , then the equation has 2, 1 or 0 real roots according to the sign of  $\Delta$ :



Aside (complex mult and roots) If  $z = re^{i\theta}$  and  $z' = r'e^{i\theta'}$ , then

$$zz' = rr'e^{i(\theta+\theta')},$$

i.e. lengths multiply and angles add (prove this using trigonometry).\*



It follows that each nonzero complex number has two square roots, three cube roots, etc. In particular, the  $n$ th roots of  $z = re^{i\theta}$  are

$$u, u\omega, \dots, u\omega^{n-1}$$

where  $u = r^{1/n}e^{i\theta/n}$  and  $\omega = e^{2\pi i/n}$ . These points are equally distributed on a circle of radius  $r^{1/n}$  about the origin (since multiplication by  $\omega$  rotates  $\mathbb{C}$  about 0 by  $2\pi/n$  radians).

- Cubic equation (16th century: del Ferro, Tartaglia  $\rightsquigarrow$  Cardan, Viète)

$$ax^3 + bx^2 + cx + d = 0$$

Divide by  $a$  and complete the cube, i.e. substitute  $y = x + b/3a$  to eliminate the quadratic term. This gives

$$y^3 + py + q = 0$$

---

\*Thus for any  $z, z'$  in the unit circle  $S^1$ , we have  $zz', z^{-1} \in S^1$  so  $(S^1, \cdot)$  is a group!

which has three roots  $y_1, y_2, y_3$ . They can be found using Viète's magical substitution

$$y = v(z) = z - \frac{p}{3z}.$$

Indeed, this leads to a *quadratic* equation in  $w = z^3$ ,

$$w^2 + qw - (p/3)^3 = 0$$

whose roots are  $w = -q/2 \pm \sqrt{\Delta}$ , where  $\Delta = (q/2)^2 + (p/3)^3$ . Thus

$$z = \left(-q/2 \pm \sqrt{\Delta}\right)^{1/3}$$

(choose any one of the six possible cube roots) which yields Cardan's formula

$$y_1 = v(z) \quad y_2 = v(\omega z) \quad y_3 = v(\omega^2 z)$$

where  $\omega = e^{2\pi i/3} = -(1/2) + (\sqrt{3}/2)i$ . The roots of the original equation are now obtained by subtracting  $b/3a$ .

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

Solution Substituting  $y = x + 2$  gives  $y^3 - 3y$ . Viète's substitution is  $y = z + z^{-1}$ , giving the quadratic  $w^2 + 1 = 0$  in  $w = z^3$ , with roots  $w = \pm i$ . Thus  $z$  is any cube root of  $\pm i$ , say  $z = i$ . Cardan's formula then gives  $y_1 = i + i^{-1} = 0$ ,  $y_2 = \omega i + (\omega i)^{-1} = -\sqrt{3}$ ,  $y_3 = \omega^2 i + (\omega^2 i)^{-1} = \sqrt{3}$  (draw a picture), and so  $x_1 = -2$ ,  $x_2 = -\sqrt{3} - 2$ ,  $x_3 = \sqrt{3} - 2$  are the roots.

Exercise (not to hand in) Verify that  $y_1, y_2, y_3$  are indeed roots of the eqn. Hint:  $r$  is a root  $\iff (y - r)$  is a factor of  $y^3 + py + q$ , so it suffices to show  $y^3 + py + q = (y - y_1)(y - y_2)(y - y_3)$ . But expanding out the last expression gives  $y^3 - (y_1 + y_2 + y_3)y^2 + (y_1y_2 + y_1y_3 + y_2y_3)y - y_1y_2y_3$ . So you must show ①  $y_1 + y_2 + y_3 = 0$ , ②  $y_1y_2 + y_1y_3 + y_2y_3 = p$  and ③  $y_1y_2y_3 = q$ . Use the fact that  $\omega^3 = 1$  and  $1 + \omega + \omega^2 = 0$ .

Question What is the significance of the sign of  $\Delta$ ?

- Quartic equation 16th century: Ferrari
- Quintic equation (and higher degree) 19th century: Abel proved that there does not exist a formula for the roots! Galois developed general theory (second semester)  $\rightsquigarrow$  birth of modern algebra.

Some arithmetic (study of the natural numbers)

Definition Say  $d$  divides (or is a divisor of)  $a$ , written  $d|a$ , if  $\exists c$  with  $a = cd$ . Denote the greatest common divisor of  $a$  and  $b$  by  $\gcd(a, b)$ .

GCD Lemma  $\forall a, b \in \mathbb{N}, \exists x, y \in \mathbb{Z}$  such that  $\gcd(a, b) = ax + by$ .

(e.g.  $\gcd(10, 14) = 2 = 10 \cdot 3 + 14 \cdot (-2)$ )

Proof Consider  $S = \{ax + by \mid x, y \in \mathbb{Z}\}$ . (Remark  $S$  is closed under subtraction, and multiplication by any integer; we say  $S$  is an ideal in  $\mathbb{Z}$ .)  
Set

$$d = \min(S \cap \mathbb{N})$$

the smallest positive elt of  $S$ . Claim  $d = \gcd(a, b)$ . Must show

$$\textcircled{1} \ d|a, d|b \quad \textcircled{2} \ e|a, e|b \implies e \leq d$$

$\textcircled{1}$  Clearly  $a = qd + r$  for some  $q, r \in \mathbb{Z}$  w/  $0 \leq r < d$ , so  $r = a - qd \in S$  (by the remark). By the minimality of  $d$ ,  $r = 0$ , and so  $d|a$ . Similarly  $d|b$ .

$\textcircled{2}$   $e|a, e|b \implies e|(ax + by)$  for all  $x, y$ , and in particular  $e|d$ . Thus  $e \leq d$ .  $\square$

This proof used structural prop of  $\mathbb{Z}$  ( $+, \cdot, <$ :  $\mathbb{Z}$  is an “ordered ring”), the “Well Ordering Principle” (WOP) and the “Division Algorithm” (DA):

WOP *Every non-empty subset of the natural numbers has a least element* (or in symbols,  $S \subset \mathbb{N}, S \neq \emptyset \implies \exists m \in S$  such that  $m \leq s$  for all  $s \in S$ )

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 can prove DA from WOP: Let  $S = \{a - xd \mid x \in \mathbb{Z}, a \geq xd\} \subset \mathbb{N} \cup \{0\}$ . By WOP,  $\exists r = \min S = a - qd$ , i.e.  $a = qd + r$ , for some  $q$ . Then  $r < d$ . For if  $r \geq d$ , then  $0 \leq r - d = a - (q + 1)d < r$ , contradicting the minimality of  $r$ .  $\square$

Where does GCD lead? To Euclid’s Lemma and the

Fundamental Theorem of Arithmetic (FTA) *Every natural no.  $n > 1$  can be written as a product of primes. This product is unique up to the order of the factors.*

(A natural number is prime if it has exactly two divisors)

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

Proof Suppose  $p \nmid a$ . Then  $\gcd(a, p) = 1$  (since  $p$  is prime) and so by the GCD Lemma,  $1 = ax + py$  for some  $x, y$ . Thus  $b = 1 \cdot b = (ax + py)b = (ab)x + pyb$ , which is clearly divisible by  $p$ .  $\square$

Summarizing the logic so far: WOP  $\implies$  Euclid's Lemma (via DA and GCD). For FTA, also need "induction", which we use informally in the following proof (see below for more formal treatment).

Proof of FTA (existence) If  $n$  is prime, there's nothing to prove. If not, 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  $p_1 | p_1 \cdots p_r$ , so  $p_1 | q_1 q_2 \cdots q_s$ . By Euclid's Lemma 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.  $\square$

## Induction

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

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

then  $S = \mathbb{N}$ .

Theorem  $WOP \iff Induction$

$\implies$  is HW #2. This shows that in fact  $WOP \implies FTA$

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

Proof Let  $S = \{k \in \mathbb{N} \mid 1 + \cdots + k = k(k + 1)/2\}$ . Then  $1 \in S$ , since  $1 = 1(2)/2$ . Assume  $n \in S$ , and so

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

We must show  $n + 1 \in S$ . 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  $n + 1 \in S$ , and so by induction,  $S = \mathbb{N}$ .  $\square$

# I Foundations

## §0. Sets

Assume familiarity with basics of set theory:

set  $S = \{\dots | \dots\}$

elements  $x \in S$

subsets  $A \subset S$

proper subset  $A \subsetneq S$

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:  $\forall, \exists, !, \implies, \iff$  (if and only if, or iff),  $\implies \Leftarrow$  (contradiction).

## §1. Functions

Definition A function  $f : S \rightarrow T$  (also written  $S \xrightarrow{f} T$ ) consists of a pair of sets  $S, T$  (the domain and codomain of the function) and a “rule”  $s \mapsto f(s)$  assigning to each element  $s \in S$  an element  $f(s) \in T$ . (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  $(S, T, R \subset S \times T)$ ...)

Remark The domain and codomain are essential parts of the function. For example the functions  $\mathbb{R} \rightarrow \mathbb{R}$  and  $\mathbb{R} \rightarrow \mathbb{R}^+$  (the real nos  $\geq 0$ ), both given by the rule  $x \mapsto x^2$ , are distinct.

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

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

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

- ④ projections  $S \leftarrow S \times T \rightarrow T$ ,  $s \leftarrow (s, t) \mapsto t$ .
- ⑤ constant functions  $S \rightarrow T$ ,  $s \mapsto t_0$ , where  $t_0$  is a fixed elt of  $T$ .
- ⑥ composition of functions Given functions  $g : R \rightarrow S$  and  $f : S \rightarrow T$ , define  $f \circ g : R \rightarrow T$  by  $(f \circ g)(r) = f(g(r))$ . Thus  $f \circ g$  (also written  $fg$ ) is defined by the “commutative diagram”

$$\begin{array}{ccc} R & \xrightarrow{f \circ g} & T \\ & g \searrow & \nearrow f \\ & & S \end{array}$$

Definition Given  $f : S \rightarrow T$  and subsets  $S_0 \subset S$  and  $T_0 \subset T$ , define the image of  $S_0$  under  $f$  to be

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

and the preimage of  $T_0$  under  $f$  to be

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

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

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

②  $f^{-1}(P \cap Q) = f^{-1}(P) \cap f^{-1}(Q)$

Proof ① (Note: often prove  $=$  of sets in two steps,  $\subset$  and  $\supset$ , though sometimes done simultaneously)  $x \in f^{-1}(P \cup Q) \iff f(x) \in P \cup Q \iff f(x) \in P \text{ or } f(x) \in Q \iff x \in f^{-1}(P) \text{ or } x \in f^{-1}(Q) \iff x \in f^{-1}(P) \cup f^{-1}(Q)$  ② Same as ① with  $\cup$  and “or” replaced with  $\cap$  and “and”.  $\square$

Definition A function  $f : S \rightarrow T$  is one-to-one (or monic or injective) if it maps at most one element of  $S$  to any given 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  $T$ , i.e.  $\text{im}(f) = T$ . In other words,  $\forall t \in T, \exists s \in S$  with  $f(s) = t$ , or equivalently  $|f^{-1}(t)| \geq 1$  for all  $t \in T$ .

Exercise Classify  $x \mapsto x^2$  as a map  $\mathbb{R} \rightarrow \mathbb{R}, \mathbb{R}^+ \rightarrow \mathbb{R}, \mathbb{R} \rightarrow \mathbb{R}^+, \mathbb{R}^+ \rightarrow \mathbb{R}^+$

Proposition 1.2  $f : S \rightarrow T$  is

Ⓐ monic  $\iff \exists \ell : T \rightarrow S$  with  $\ell \circ f = \text{id}_S$  ( $\ell$  is a “left inverse” of  $f$ )

Ⓑ epic  $\iff \exists r : T \rightarrow S$  with  $f \circ r = \text{id}_T$  ( $r$  is a “right inverse” of  $f$ )

Proof (Sketch) (Ⓐ  $\implies$ ) For  $t \in \text{im}(f)$ , define  $\ell(t)$  to be the (unique)  $s \in f^{-1}(t)$ , and define  $\ell(t)$  arbitrarily for  $t \notin \text{im}(f)$ . (Ⓑ  $\implies$ ) Define  $r(t) =$  any  $s \in f^{-1}(t)$ .  $\square$

Definition If  $f$  is both one-to-one (also written 1-1) and onto, then it is called a bijection, and has an inverse function  $f^{-1} : T \rightarrow S$  defined by  $f^{-1}(t) =$  the unique elt  $s \in S$  for which  $f(s) = t$ .

Note  $f^{-1}$  is characterized by  $f \circ f^{-1} = \text{id}_T$ ;  $f^{-1} \circ f = \text{id}_S$ .

## §2. Equivalence Relations

Definition A partition of a set  $S$  is a collection of nonempty disjoint subsets of  $S$  whose union is  $S$ .

Examples (including Banach-Tarski Paradox)

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

- ① reflexive :  $x \sim x$  (for all  $x \in S$ )
- ② symmetric :  $x \sim y \implies y \sim x$
- ③ transitive :  $x \sim y$  and  $y \sim z \implies x \sim z$

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

Proposition 2.1 *The collection of equivalence classes of an equivalence relation on  $S$  form a partition of  $S$ . Conversely, any partition  $S = \coprod_{\alpha} S_{\alpha}$  gives rise to a unique equivalence relation  $\sim$  whose equivalence classes are the  $S_{\alpha}$ 's, namely  $x \sim y \iff \exists \alpha$  with  $x, y \in S_{\alpha}$ . Proof: exercise*

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

$$S / \sim := \{R \subset S \mid R = \bar{x} \text{ for some } x \in S\}$$

and the map  $S \rightarrow S / \sim$ ,  $x \mapsto \bar{x}$  is the natural projection of  $S$  onto  $S / \sim$ .

Examples ① (the integers mod  $n$ )  $S = \mathbb{Z}$ . For each  $n \in \mathbb{N}$ , define the “congruence mod  $n$ ” relation  $\equiv_n$  by  $a \equiv_n b$  (also written  $a \equiv b \pmod{n}$ )  $\iff n \mid (a - b)$  (i.e.  $a$  and  $b$  have the same remainder when divided by  $n$ ). (Check properties ①, ②, ③, e.g. ③ ... )

The equiv class

$$\bar{a} = \{a + kn \mid k \in \mathbb{Z}\} = \{\dots, a - n, a, a + n, a + 2n, \dots\}$$

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

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

### §3. Binary Operations

Definition A binary operation on a set  $S$  is a function

$$S \times S \xrightarrow{*} S.$$

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  $+, \cdot$  on  $S = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  (associative and commutative);  
 $-$  on  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  is neither

②  $\cdot$  of  $n \times n$  matrices (associative but not commutative)

③  $+, \cdot$  on  $\mathbb{Z}_n$  (“modular arithmetic”):

$$\bar{a} + \bar{b} := \overline{a + b}$$

(the LHS is defined by the RHS). Must show this is “well-defined”: Suppose  $a \equiv a', b \equiv b'$ , i.e.  $n \mid (a - a'), n \mid (b - b')$ . Then  $n \mid [(a - a') + (b - b')] \implies n \mid [(a + b) - (a' + b')]$ . Thus  $\bar{a} + \bar{b} = \overline{a + b} = \overline{a' + b'} = \bar{a}' + \bar{b}'$ . Similarly define

$$\bar{a} \cdot \bar{b} := \overline{a \cdot b}$$

and show well defined. These operations are associative and commutative. Also  $\cdot$  is distributive over  $+$ :

$$\bar{a}(\bar{b} + \bar{c}) = \overline{a(b + c)} = \overline{ab + ac} = \bar{a}\bar{b} + \bar{a}\bar{c}.$$

Definition A morphism of sets w/ binary operations  $f : (S, *) \rightarrow (S', *')$  is a function  $f : S \rightarrow S'$  satisfying

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

for all  $a, b \in S$ . Say  $f$  is a monomorphism if  $f$  is 1-1, and an epimorphism if  $f$  is onto. An isomorphism is a morphism which has an inverse which is also a morphism.<sup>†</sup>

Examples ① The “exponential map”  $(\mathbb{R}, +) \xrightarrow{\text{exp}} (\mathbb{R}, \cdot)$ ,  $x \mapsto e^x$ , is a morphism, since  $e^{x+y} = e^x e^y$ .

②  $M_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}$  is a multiplicative morphism, since  $\det(AB) = \det(A) \det(B)$ .

---

<sup>†</sup>In fact, any morphism  $f$  which has an inverse  $f^{-1}$  (or equivalently any bijective morphism) is 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  $x = f(a)$  and  $y = f(b)$  for some  $a, b \in S$ . Now plug in . . .

## II Groups

### §1. Basic Concepts: groups, homomorphisms, and group actions

Definition A group is a set  $G$  with a binary operation  $G \times G \xrightarrow{*} G$ ,  $(a, b) \mapsto a * b$ , satisfying

(G1) associativity:  $(a * b) * c = a * (b * c)$  for all  $a, b, c \in G$

(G2) identity:  $\exists e \in G$  s.t.  $e * a = a = a * e$  for all  $a \in G$

(G3) inverses:  $\forall a \in G, \exists b \in G$  s.t.  $a * b = e = b * a$ .

If  $*$  is commutative, say  $G$  is abelian.  $|G|$  is the order of  $G$ . If  $|G| < \infty$ , say  $G$  is finite; otherwise  $G$  is infinite. The order of an element  $a \in G$  is

$$|a| := \min\{n \in \mathbb{N} \mid \underbrace{a * \cdots * a}_{n \text{ factors}} = e\}$$

unless this set is empty, in which case  $|a| = \infty$  by convention (e.g. every nonzero integer has infinite order, and  $|0| = 1$ ).

Remarks ① Identities and inverses are unique

Proof: Suppose  $e_1, e_2$  are both identities. Then

$$\begin{aligned} e_1 &= e_1 * e_2 && \text{G2 (} e_2 \text{ is an identity)} \\ &= e_2 && \text{G2 (} e_1 \text{ is an identity)} \end{aligned}$$

Now suppose  $b_1, b_2$  are both inverses of  $a$ . Then

$$\begin{aligned} b_1 &= b_1 * e && \text{G2} \\ &= b_1 * (a * b_2) && \text{G3} \\ &= (b_1 * a) * b_2 && \text{G1} \\ &= e * b_2 && \text{G3} \\ &= b_2 && \text{G2} \end{aligned}$$

② Usually write

· 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) when  $n > 0$ , and for  $(a^{|n|})^{-1}$  when  $n < 0$ .

If  $G$  is abelian, sometimes write  $+$  for  $*$ ;  $a + b$ ,  $0$ ,  $-a$ , and  $na$  for  $a * b$ ,  $e$ , the (additive) inverse of  $a$ , and  $a * \cdots * a$  ( $n$  times).

- ③ Other structures
- Ⓐ semigroup G1 only (set with an assoc bin op)
  - Ⓑ monoid G1 and G2 only (set with an assoc bin op with identity)
  - Ⓒ ring abelian group  $(R, +)$  with an add'l assoc binary op  $R \times R \rightarrow R$  which is distributive over  $+$ , i.e.  $a(b+c) = ab+ac$  and  $(a+b)c = ac+bc$  (e.g.  $(\mathbb{Z}, +, \cdot)$ ). Say  $R$  is commutative if  $\cdot$  is, with identity if  $\exists 1$ .
  - Ⓓ field commutative ring  $(F, +, \cdot)$  with  $1 \neq 0$  such that each nonzero elt has a mult inverse (e.g.  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ , and  $\mathbb{Z}_n$  for prime  $n$ ; HW).

Cancellation Property If  $a, b, c \in G$  ( $a$  group) satisfying  $ab = ac$ , then  $b = c$ .

Proof (supply reasons)  $ab = ac \implies a^{-1}(ab) = a^{-1}(ac) \implies (aa^{-1})b = (aa^{-1})c \implies 1b = 1c \implies b = c$ .  $\square$

#### Familiar examples of groups

- ①  $(\mathbb{Z}, +)$  infinite abelian group. In fact  $(\mathbb{Z}, +, \cdot)$  is a commutative ring with 1, but not a field ( $\nexists$  inverses in gen'l)
- ②  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  under  $+$ , and  $\mathbb{Q} - 0, \mathbb{R} - 0, \mathbb{C} - 0$  under  $\cdot$
- ③  $(\mathbb{Z}_n, +)$  finite abelian group

$$|\mathbb{Z}_n| = n \quad \mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

In fact  $(\mathbb{Z}_n, +, \cdot)$  is a comm ring with 1. (Example:  $\mathbb{Z}_2$ , mult table)

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  $\nexists$  any 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  $\bar{a}\bar{x} = \bar{c}$ . Since  $d = 1$ , the GCD lemma  $\implies ap + bq = 1$  for suitable integers  $p, q$ . Thus  $ap \equiv 1 \pmod{b}$ , i.e.  $\bar{a}$  has an inverse, namely  $\bar{p}$ , in  $\mathbb{Z}_b$ . Thus the unique solution to the equation in  $\mathbb{Z}_b$  is  $\bar{x} = \bar{p}\bar{c} \implies$  one solution in  $\mathbb{Z}$  is  $x_0 = pc, y_0 = (c - ax_0)/b = (c - apc)/b$ .

To get all the solutions, note that we can change  $x_0$  by adding any multiple  $nb$  of  $b$ . This will change  $y_0$  by subtracting  $na$ . Thus the full set of solutions is  $\{(pc + nb, (c - apc)/b - na) \mid n \in \mathbb{Z}\}$ .

Example Solve  $6x+10y = 14$ . Equivalent equation  $3x+5y = 7$ . Working mod 5

$$3x \equiv 7 \implies x \equiv 3^{-1} \cdot 7 \equiv 2 \cdot 7 \equiv 14 \equiv 4$$

so solutions are  $\{(x, y) = (4 + 5n, -1 - 3n) \mid n \in \mathbb{Z}\}$ .

### More examples of groups

- ① The circle group  $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$  infinite abelian group (in fact a Lie group: a group which is also a manifold ... locally Euclidean)
- ② The cyclic group of order  $n$ ,  $C_n = \{z \in \mathbb{C} \mid z^n = 1\}$ . Note that  $C_n \subset S^1$ . Also  $(C_n, \cdot)$  is “isomorphic” to  $(\mathbb{Z}_n, +)$  via  $e^{2\pi ik/n} \mapsto \bar{k}$ .
- ③ The Klein 4-group  $V_4 = \{1, a, b, c\}$  with  $a^2 = b^2 = c^2 = 1$ , and the product of any two of  $a, b, c$  equals the third. This is not isomorphic to  $C_4$  (why?). Every group of order 4 is iso to either  $C_4$  or  $V_4$  (study mult tables).
- ④ (products)  $G, H$  groups  $\implies G \times H$  is a group under the operation  $(g, h) \cdot (g', h') := (gg', hh')$ . (For example,  $S^1 \times S^1$  is the torus (picture), and  $C_2 \times C_2 = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\} \cong V_4$ .)

Note ① The product of abelian gps is abelian ②  $|G \times H| = |G||H|$ .

- ⑤ (units) Let  $(R, \cdot)$  be a monoid (e.g. ignore  $+$  in any ring  $R$ ), and set

$$R^\bullet = \{a \in R \mid \exists a' \in R \text{ with } aa' = a'a = 1\}$$

i.e. the “invertible elts” of  $R$ . The elements in  $R^\bullet$  are called units in  $R$ .

Claim  $(R^\bullet, \cdot)$  is a group (Proof Must first show that  $\cdot$  induces an operation on  $R^\bullet$ , i.e.  $R^\bullet$  is closed under multiplication: if  $a, b \in R^\bullet$ , i.e.  $\exists a', b' \in R$  with  $aa' = a'a = 1 = bb' = b'b$ , then  $a', b' \in R^\bullet \implies (ab)(b'a') = 1 = (b'a')(ab) \implies ab \in R^\bullet$ . Associativity is inherited.  $1 \in R$ , since  $1 \cdot 1 = 1$ , and any  $a \in R^\bullet$  has an inverse in  $R^\bullet$ , namely the  $a'$  from above.)

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

- ②  $\mathbb{Z}_n^\bullet = \{\bar{a} \in \mathbb{Z}_n \mid \exists \bar{b} \text{ with } \bar{a}\bar{b} = \bar{1}\} \stackrel{\text{claim}}{=} \{\bar{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$

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

Thus

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

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

·	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

We know two other gps of order 4:  $C_4$  and  $C_2 \times C_2$ . These are not isomorphic to each other: in  $C_2 \times C_2$ , all squares = 1 (as in  $\mathbb{Z}_8^\bullet$ ), but not so in  $C_4$ . Are  $\mathbb{Z}_8^\bullet$  and  $C_2 \times C_2$  isomorphic? Yes:

$$\begin{aligned} \bar{1} &\longleftrightarrow (1, 1) \\ \bar{3} &\longleftrightarrow (1, -1) \\ \bar{5} &\longleftrightarrow (-1, 1) \\ \bar{7} &\longleftrightarrow (-1, -1) \end{aligned}$$

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

Ⓐ  $\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$ . For example:

$$\varphi(76) = \varphi(2^2 \cdot 19) = 76(1 - \frac{1}{2})(1 - \frac{1}{19}) = 2^2 \cdot 19 \cdot \frac{1}{2} \cdot \frac{18}{19} = 36$$

Ⓑ  $\mathbb{Z}_n^\bullet \cong \mathbb{Z}_{p_1^{e_1}}^\bullet \times \cdots \times \mathbb{Z}_{p_k^{e_k}}^\bullet$  (where  $\cong$  means “isomorphic to”). Furthermore, if  $n$  is a power of a prime  $p$ , then  $\mathbb{Z}_n^\bullet \cong C_{\varphi(n)}$  for odd  $p$  and  $C_2 \times C_{\varphi(n)/2}$  for  $p = 2$ . For example,  $\mathbb{Z}_{76}^\bullet \cong C_2 \times C_{18}$ .

Examples of groups (continued)

⑥ Dihedral groups

$$D_{2n} := \{\text{symmetries of a regular } n\text{-gon } P \subset \mathbb{C}\}$$

( $P$  has vertices at  $e^{2\pi ik/n}$ ) A symmetry of  $P$  is a rigid motion (i.e. distance preserving function  $f : \mathbb{C} \rightarrow \mathbb{C}$ ) which carries  $P$  onto itself (i.e.  $f(P) = P$ );

each such is either a rotation about 0, or a reflection across a line thru 0. Clearly  $D_{2n}$  consists of  $n$  rotations and  $n$  reflections, so  $|D_{2n}| = 2n$ . The operation on  $D_{2n}$  is composition.

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

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

Note the “relations”  $r^n = s^2 = 1$  and  $rs = sr^{-1}$  (since  $\zeta_n \bar{z} = \overline{\zeta_n^{-1} z}$ ). Since any word in the letters  $r, s, r^{-1}, s^{-1}$  can be reduced using these relations to the unique form  $s^a r^b$  (for some  $a = 0, 1$  and  $b = 0, \dots, n-1$ ) we say  $D_{2n}$  is generated by  $r, s$  with relations  $r^n = s^2 = 1, rs = sr^{-1}$ , written

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

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).

⑦ Symmetric Groups Set  $\underline{n} = \{1, \dots, n\}$ . Then

$$S_n := \{\text{bijections } \underline{n} \rightarrow \underline{n}\}$$

is a group under composition. Its elements are called permutations (of  $n$  symbols or letters), and  $(S_n, \circ)$  is called the symmetric group of degree  $n$ . Note that  $S_n$  is a finite, nonabelian (for  $n \geq 3$ ) group of order  $n!$ ,

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

(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  $A \rightarrow A$  is a group under composition, the symmetric group on  $A$ .

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

② 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

Obvious fact Every  $\sigma \in S_n$  can be written uniquely (up to order of cycles and cyclic permutation in each cycle) as a product of disjoint (i.e. non overlapping) cycles, called its cycle decomposition. (Often suppress 1-cycles in notation)

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  $1, \dots, n$  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  $\pi$ ),  $\pi(2) = 2$  (giving the cycle  $(2)$ ),  $\pi(4) = 5$  and  $\pi(5) = 4$  (giving the cycle  $(4\ 5)$ ). Thus

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

Note The order (as an elt of  $S_n$ ) of any  $k$ -cycle is  $k$ , and in gen'l 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

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

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

### Two final examples

⑧ Quaternion groups The set of quaternions is

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

where  $i^2 = j^2 = k^2 = -1$ ,  $ij = k = -ji$ ,  $jk = i = -kj$ ,  $ki = j = -ik$ . Note that  $\mathbb{H}$  is a group under addition, but not under multiplication. However, it is a ring, in fact *almost* a field; the only axiom that fails is commutativity of multiplication. Such a structure is called a division ring.

Exercise The 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

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

The finite quaternion group

$$Q_8 := \{\pm 1, \pm i, \pm j, \pm k\}$$

is a nonabelian (multiplicative) subgroup of  $\mathbb{H}^\bullet$  of order 8; it lies in the infinite subgroup

$$S^3 := \{a + bi + cj + dk \in \mathbb{H} \mid a^2 + b^2 + c^2 + d^2 = 1\}$$

called the 3-sphere which arises in topology.

⑨ Matrix groups  $R =$  commutative ring with 1

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

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

There are many important subgps of  $GL_n(R)$ :  $SL_n(R) = \{A \mid \det(A) = 1\}$ . For  $R = \mathbb{R}$  have  $O(n)$  (orthogonal matrices) and  $SO(n)$ . For  $R = \mathbb{C}$  have  $U(n)$  (unitary matrices) and  $SU(n)$ . Tricky exercise: Show  $SU(2) \cong S^3$ .

## Homomorphisms

Definition Let  $G, H$  be groups. A function  $f : G \rightarrow H$  is a group homomorphism (or morphism) if  $f(xy) = f(x)f(y)$  for all  $x, y \in G$ . The image and kernel of  $f$  are

$$\text{im}(f) := \{f(x) \mid x \in G\} = f(G)$$

$$\text{ker}(f) := \{x \in G \mid f(x) = 1\} = f^{-1}(1)$$

For ex the trivial morphism, defined by  $f(x) = 1$  for all  $x \in G$ , has kernel  $G$  and image  $= \{1\}$ . Define mono, epi, and iso-morphisms in usual way (mono

= 1-1, epi = onto, and iso = both). We say  $G$  and  $H$  are isomorphic if  $\exists$  and isomorphism  $G \rightarrow H$ . A morphism from a group to itself (i.e.  $G = H$ ) is called an endomorphism. An automorphism is a bijective endomorphism.

Examples ①  $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^\bullet, \cdot)$  is a monomorphism.

②  $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^\bullet$  is an epimorphism (where it is understood that the operation is multiplication in both groups).

③ For any abelian group  $G$ , the map  $\phi_- : G \rightarrow G, x \mapsto x^{-1}$  is a homomorphism since  $\phi_-(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi_-(x)\phi_-(y)$ . In fact  $\phi_-$  is an automorphism which is its own inverse!

If  $G$  is nonabelian, then  $\phi_-$  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.

Remarks ④ Any composition of morphisms is a morphism (verify)

① Let  $f : G \rightarrow H$  be a homomorphism of groups. Then

- Ⓐ  $f$  is onto  $\iff \text{im}(f) = H$  (true for all functions) and  $f$  is 1-1  $\iff \ker(f) = \{1\}$  (HW).
- Ⓑ  $f(1) = 1$  (proof:  $f(1) = f(1 \cdot 1) = f(1)f(1)$ ; now multiply by  $f(1)^{-1}$ ) and  $f(x^{-1}) = (f(x))^{-1}$  (HW)
- Ⓒ  $|f(x)|$  divides  $|x|$  Proof Set  $n = |x|$  and  $k = |f(x)|$ . Then  $x^n = 1 \implies f(x)^n = f(x^n) = f(1) = 1$ . Now appeal to:

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

Proof If  $k$  is finite, then for any  $i$  and  $j$  we can write  $i - j = qk + r$  with  $0 \leq r < k$ . Thus  $a^i \equiv a^j \pmod{k} \iff a^{i-j} = 1 \iff a^r = 1$ , since  $a^{qk+r} = (a^k)^q a^r = a^r$ . But  $a^r = 1 \iff r = 0$ , since  $r < k = |a|$ , and  $r = 0 \iff i \equiv j \pmod{k}$ . The last statement is clear since  $a^i = a^j \iff a^{i-j} = 1$ .  $\square$

② If  $f : G \rightarrow H$  is an isomorphism of groups, then

- Ⓐ  $|G| = |H|$
- Ⓑ  $G$  is abelian  $\iff H$  is abelian
- Ⓒ  $|f(x)| = |x| \forall x \in G$  (HW)

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

Ⓐ  $C_m \not\cong C_n$  for  $m \neq n$  since they have different orders.

Ⓑ  $C_6 \not\cong S_3$  since  $C_6$  is abelian and  $S_3$  is not.

Ⓒ  $\mathbb{Z}_{24}^\bullet \not\cong C_8$  since  $C_8$  has elts of order 8, but  $\mathbb{Z}_{24}^\bullet$  doesn't. Can also count the number of elements of a given order to distinguish groups, e.g.:  $D_{24} \not\cong S_4$  since  $D_{24}$  has 13 elts of order 2 while  $S_4$  has 9 (why?).

Open Problem Classify all groups (up to isomorphism)

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

② There exist 2 of order 4 ( $C_4, V_4$ ), 2 of order 6 ( $C_6, S_3$ ), 5 of order 8 ( $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8, Q_8$ ), 2 of order 9 ( $C_9, C_3 \times C_3$ ), 2 of order 10 ( $C_{10}, D_{10}$ ), 5 of order 12, 14 of order 16 ... (see page 168 in text)

Group Actions (a central theme in the course)

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

$$(A1) \quad g \cdot (h \cdot a) = (gh) \cdot a \qquad (A2) \quad 1 \cdot a = a$$

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

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

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

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

Examples ① trivial action  $g \cdot a = a$  for all  $a \in A$  (i.e.  $\sigma$  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 or right multiplication:  $g \cdot a = ga$  or  $ag^{-1}$  (verify that these are both actions) or by conjugation

$$g \cdot a = gag^{-1}$$

(HW) Note  $gag^{-1}$  is called the conjugate of  $a$  by  $g$ .

## §2. Subgroups

Definition A subset  $H$  of a group  $G$  is a subgroup of  $G$ , written  $H < G$ , if it is a group under the operation induced from  $G$ , i.e.

$$(S1) \ x, y \in H \implies xy \in H \quad (S2) \ 1 \in H \quad (S3) \ x \in H \implies x^{-1} \in H$$

(Note: associativity is automatic)

Examples ① Every group has the trivial subgroups  $\{1\}$  and  $G$ . Any other subgroup will be called proper.

② For  $k = 0, 1, 2, \dots$ , the set  $k\mathbb{Z} = \{nk \mid n \in \mathbb{Z}\}$  of all multiples of  $k$  is a subgroup of  $\mathbb{Z}$ ; 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,  $2\mathbb{Z} = \text{evens}$ , etc.

③  $\{1, r, \dots, r^{n-1}\}$  and  $\{1, s\}$  are subgps of  $D_{2n}$ .

④  $\{1, -1\}$  and  $\{1, i, -1, -i\}$  are subgroups of  $Q_8$ .

⑤  $C_n < S^1 < \mathbb{C}^\bullet$ .

Subgroup Criterion A subset  $H$  of a group  $G$  is a subgroup if and only if ①  $H$  is nonempty, and ②  $x, y \in H \implies xy^{-1} \in H$ .

Proof ( $\implies$ )  $1 \in H$  by (S2) so  $H \neq \emptyset$ . If  $x, y \in H$ , then  $y^{-1} \in H$  by (S3) so  $xy^{-1} \in H$  by (S1). Thus ② holds.

( $\impliedby$ )  $\exists x_0 \in H$  by ①, so  $1 = x_0x_0^{-1} \in H$  by ②  $\implies$  (S2). Now  $x \in H \implies x^{-1} = 1 \cdot x^{-1} \in H$  by ②  $\implies$  (S3). Finally  $x, y \in H \implies y^{-1} \in H$  by (S3)  $\implies xy = x(y^{-1})^{-1} \in H$  by ②, so (S1) holds.  $\square$

Remark If  $H$  is finite, ② can be replaced by (S1), since  $x \in H \implies x^n = 1$  for some  $n$  (since  $G$  is finite)  $\implies 1 = x^n \in H$  and  $x^{-1} = x^{n-1} \in H$ .

### More examples of subgroups

⑥ Let  $G$  be a group. Then any subgp of a subgp of  $G$  is a subgp of  $G$ , and any intersection of subgps of  $G$  is a subgp of  $G$  (why?).

⑦ For any homomorphism  $G \xrightarrow{f} H$  of groups,

$$\ker(f) < G \quad \text{and} \quad \text{im}(f) < H$$

(check this by the def'n of subgp or using the subgp criterion)

⑧ The center  $Z(G) := \{x \in G \mid xg = gx \text{ for all } g \in G\}$  of a group  $G$  is a subgp of  $G$ . Proof: For  $x, y \in Z(G)$  and  $g \in G$ , we have  $xyg = xgy = gxy \implies xy \in Z(G)$  (proving S1) and  $xg^{-1} = g^{-1}x \implies$  (taking inverses)  $x^{-1}g = gx^{-1} \implies x^{-1} \in Z(G)$  (proving S3). For (S2), note that  $1 \in Z(G)$  since  $1g = g = g1$  for all  $g$ . (Exercise Give an alternative proof using the subgp criterion and the observation that  $xg = gx \iff x = gxg^{-1}$ )

More generally, for any subset  $A \subset G$ , define the centralizer of  $A$  in  $G$  to be

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

(so  $Z(G) = C_G(G)$ ), and the normalizer of  $A$  in  $G$  to be

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

where  $xA = \{xa \mid a \in A\}$  and  $Ax = \{ax \mid a \in A\}$ . All are subgroups of  $G$  (general proof given in ⑨ below).

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

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

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

$xA$  and  $Ax$  are special cases of this, as is  $xAx^{-1} = \{xax^{-1} \mid a \in A\}$ . Note that the conditions  $xa = ax$  and  $xA = Ax$  defining  $C_G(a)$  and  $N_G(A)$  can be rewritten as  $xax^{-1} = a$  and  $xAx^{-1} = A$ .

⑨ If a group  $G$  acts on a set  $A$  and  $a \in A$ , then the stabilizer of  $a$  is

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

This is a subgroup of  $G$  for each  $a$ . (Proof:  $1 \in G_a$  by (A2), so  $G_a \neq \emptyset$ . 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 ① The stabilizer of  $1 \in \mathbb{C}$  under the usual action of the dihedral group  $D_{2n}$  is  $\{1, s\}$ .

② 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 be viewed in terms of actions: For  $A \subset G$ , the normalizer  $N_G(A)$  acts on  $A$  by conjugation, and  $C_G(A)$  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.

### Normal subgroups

Definition A subgroup  $H < G$  is called a normal subgroup (written  $H \triangleleft G$ ) if

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

(or equivalently  $N_G(H) = G$ ). Thus a subgroup of  $G$  is normal iff it is “closed under conjugation” by any elt in  $G$ . For example  $\{1, -1, i, -i\} \triangleleft Q_8$ , as shown above. In general

- ①  $Z(G) \triangleleft G$  (why?)
- ②  $\ker(f) \triangleleft G$  for any morphism  $f : G \rightarrow H$  (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  $x = h^{-1}h' \in H \implies \Leftarrow$ ). So  $xH = G - H$ . Similarly  $Hx = G - H$ . Thus  $xH = Hx \implies xHx^{-1} = H \implies H \triangleleft G$ .  $\square$

Warning:  $K \triangleleft H \triangleleft G \not\Rightarrow K \triangleleft G$ .  $\exists$  examples with  $|G| = 8$  (HW).

### Cyclic groups and subgroups

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

$$\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\} \quad (\text{w/ repetitions deleted})$$

This is a subgroup of  $G$  (verify) called the cyclic subgroup generated by  $x$ . If

$$G = \langle x \rangle \quad \text{for some } x \in G$$

we say  $G$  is a cyclic group, and any such  $x$  is called a generator of  $G$  (there may be many). Note: if  $|G| = n$ , then  $G$  cyclic  $\iff G$  has an elt of order  $n$ .

Examples ①  $\mathbb{Z}$  under  $+$  (or its mult analogue  $C_\infty = \{t^k \mid k \in \mathbb{Z}\}$ , where  $t$  is an indeterminate) is cyclic with generator 1 (or  $t$ ). Alternatively,  $-1$  (resp.  $t^{-1}$ ) is a generator.

②  $C_n$  is cyclic with generator  $t = e^{2\pi i/n}$  (or  $t^k$  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  $\langle r^k s \rangle = \{1, r^k s\} \neq D_{2n}$

Remark The order  $n$  of any element  $x$  in a group is equal to the order of the cyclic subgroup it generates:  $|x| = |\langle x \rangle|$ . (Clear 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  $1, x, \dots, x^{n-1}$ .)

Classification Theorem for Cyclic Groups Every cyclic group  $C = \langle x \rangle$  is isomorphic to  $C_n$  for some  $n = 1, 2, \dots, \infty$ . 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  $C \rightarrow C_n$  mapping  $x^k$  to  $t^k$  (for each  $k \in \mathbb{Z}$ ) is a well defined isomorphism (why?).  $\square$

Classification Theorem for Subgroups of Cyclic Groups Let  $C = \langle x \rangle$  be a cyclic group. Then

① Every subgroup  $H$  of  $C$  is cyclic. In particular any nontrivial  $H = \langle x^m \rangle$ , where  $m$  is the smallest positive integer for which  $x^m \in H$ .

② If  $C$  is finite of order  $n$ , then it has a subgroup of order  $k \iff k$  divides  $n$ . In fact there is only one such subgroup for each divisor  $k$ .

Proof ① HW

② ( $\implies$ ) If  $H < C$  with  $|H| = k$ , then  $H = \langle x^m \rangle$ , for  $m$  as in ①. Set  $d = \gcd(m, n)$ . Then  $x^d = x^{am+bn}$  (for suitable  $a, b$ )  $= (x^m)^a \in H \implies m = d$ , which divides  $n \implies k = n/m$  divides  $n$  (and in fact  $H = \langle x^{n/k} \rangle$ , so  $H$  is the only subgroup of order  $k$ ). ( $\impliedby$ )  $k|n \implies H = \langle x^{n/k} \rangle$  has order  $k$ .  $\square$

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

Remarks 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  $= \langle r, s \mid r^8 = 1 = s^2, rs = sr^5 \rangle$ .

Question Does ⑥ generalize to other finite groups  $G$ ?

Answer  $\implies$  does (Lagrange's theorem, below), but  $\impliedby$  does not. For example the group  $T_{12}$  of symmetries of the tetrahedron has order 12 but has no subgroup of order 6. To see this, note that  $T_{12}$  consists of eight  $2\pi/3$ -rotations (about lines through the vertices), three  $\pi$ -rotations (about lines joining midpoints of opposite sides), and the identity element. Now suppose that  $H < T_{12}$  with  $|H| = 6$ . Then it must contain at least one  $2\pi/3$ -rotation  $r$ . But then it must contain all of them (since they are all conjugate to  $r$  or  $r^{-1}$ , and  $H \triangleleft G$  as shown above) and this is clearly impossible.

Lagrange's theorem The order of any subgroup of a finite group  $G$  divides  $|G|$

Definition If  $H$  is a subgroup of a group  $G$ , 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  $G$ . Similarly define the right cosets  $Hx \subset G$ . The left (resp. right) cosets of  $H$  partition  $G$  into equal sized subsets:

Coset Lemma ①  $|xH| = |H|$  ②  $xH \cap yH \neq \emptyset \implies xH = yH$ , and  
③  $\cup_{x \in G} xH = G$  (and similarly for right cosets)

Proof ① The map  $H \rightarrow xH$ ,  $h \mapsto xh$  is a bijection, by cancellation  
② hyp  $\implies xi = yj$  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  $xH = yH$ .  
③  $x \in xH$ . □

The number of left (or right) cosets of  $H$  in  $G$  is called the index of  $H$  in  $G$ , denoted  $|G : H|$ . The coset lemma shows that  $|G| = |G : H||H|$ , which proves Lagrange's Theorem.

Remarks ① 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 (coset recognition: HW)  $x, y \in G$  lie in the same coset of  $H \iff x^{-1}y \in H \iff y = xh$  for some  $h \in H$  (and similarly for right cosets)

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

## Applications of Lagrange's Theorem

- ① The order of any element  $x$  in a finite group  $G$  divides  $|G|$ .
- ② Any group of prime order  $p$  is cyclic (and so there's only one).
- ③ (Euler's Theorem) If  $a, n \in \mathbb{N}$  are relatively prime, then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where  $\phi(n) = |\mathbb{Z}_n^\bullet|$ . Special case (Fermat's Little Theorem): If  $p$  is prime and  $p \nmid a$ , then  $a^{p-1} \equiv 1 \pmod{p}$  (since  $\phi(p) = p - 1$ ). For example  $3^4 = 81 \equiv 1 \pmod{5}$ ,  $3^6 = 729 \equiv 1 \pmod{7}$ , etc.

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

- ② Any  $x \neq 1$  in  $G$  has order dividing  $p$  (by ①) and thus equal to  $p$ , since  $p$  is prime; so  $G = \langle x \rangle$ .
- ③  $(a, n) = 1 \implies \bar{a} \in \mathbb{Z}_n^\bullet$  (by the GCD Lemma)  $\implies a^{\phi(n)} = \bar{1}$  (by ①, since  $\mathbb{Z}_n^\bullet$  has order  $\phi(n)$ ), i.e.  $a^{\phi(n)} \equiv 1 \pmod{n}$ .  $\square$

### §3. 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,

Fundamental Theorem of Finite Abelian Groups (Primary Form) *Every finite abelian gp is isomorphic to a product of cyclic groups of prime power order. Moreover, the number of factors and their orders are uniquely determined by the group.*

This leads to an algorithm for finding all abelian groups of 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  $k_1 \geq \dots \geq k_s$  of natural numbers such that  $k = k_1 + \dots + k_s$ ), namely

$$C_{p^{k_1}} \times \dots \times C_{p^{k_s}}.$$

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

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

corresp 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 is one abelian group for each list of partitions of  $k_1, k_2, \dots$ .

Exercise 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 is another standard form for finite abelian groups: Using the fact (from homework) 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  $n_1, n_2, \dots$  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

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

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

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  $f : H \times K \rightarrow G$  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  $H \triangleleft G$ , or as  $(hkh^{-1})k^{-1} \in K$  since  $K \triangleleft G$ ). 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 elts 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.  $\square$

Now let  $G$  be a finite abelian group. We wish to show that  $G$  is a product of cyclic groups of prime power orders. We split off one prime at a time: Suppose  $|G| = p^k q$ , where  $p$  is prime and  $p \nmid q$ . Set

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

Then  $P$  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  $n$ ) to prove that  $P$  is a product of cyclic groups. This is the content of the following theorem:

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  $x^p \in K$ .

Pf 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  $K' \supsetneq K$ , which contradicts the maximality of  $K$ .  $\square$

#### §4. Cayley's Theorem and the Symmetric Group

Cayley's Theorem *Every group  $G$  is isomorphic to a subgroup of the symmetric group  $S_G$ .*

Proof Let  $G$  act on itself by left multiplication. Then the associated permutation homomorphism  $\lambda : G \rightarrow S_G$  ( $\lambda(g) =$  left mult by  $g$ ) is 1-1 (by the cancellation property in  $G$ ) and so  $G \cong \text{im}(\lambda) < S_G$ .  $\square$

In particular, every finite group of order  $n$  is isomorphic to a subgroup of  $S_n$ . One especially important subgroup of  $S_n$  is the alternating group  $A_n$  consisting of all even permutations (defined below).

Note that every permutation  $\sigma \in S_n$  can be written as a product of transpositions, since any cycle can:

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

(e.g.  $(i j k l) = (i j)(j k)(k l)$ ). This decomposition is not unique, e.g.  $1 = (1 2)(1 2) = (1 2)(3 4)(1 2)(3 4)$ , but the parity (even or odd) of the number of transpositions is always the same:

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

In particular odd-length cycles are even and even-length cycles are odd (by the formula displayed above). Also even·even = odd·odd = even, and even·odd = odd·even = odd.

Remarkable Fact No permutation is both even and odd.

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

$$c : S_n \rightarrow \mathbb{N}$$

assigning to  $\sigma \in S_n$  the number of cycles in the disjoint cycle decomp of  $\sigma$  (counting the 1-cycles). For example  $c(k\text{-cycle}) = n - k + 1$ . Readily verify

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

for any transposition  $\tau = (i j)$ . Indeed if  $i$  and  $j$  lie in the same cycle in  $\sigma$  then that cycle splits into two in  $\sigma\tau$ , and if they lie in distinct cycles in  $\sigma$  then those cycles are joined into one in  $\sigma\tau$ . The remaining cycles of  $\sigma$  and  $\sigma\tau$  coincide. It follows that if  $\sigma$  is a product of  $m$  transpositions then  $c(\sigma) \equiv c(1) + m \equiv n + m$ , and so the parity of  $m$  is determined by  $\sigma$ .

Thus there is a well-defined homomorphism

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

sending even permutations to  $+1$  and odd ones to  $-1$ . The kernel is the set  $A_n$  of all even permutations, known as the alternating group of degree  $n$ . It is a normal subgroup of index 2, i.e.  $|A_n| = n!/2$  (do you see why?).

Remarks ① The parity of a permutation  $\sigma$  is equal to the parity of

Ⓐ (algebraic) the number of even-length cycles in any cycle decomposition of  $\sigma$ ; the number of odd-length cycles is irrelevant. Thus even permutations are those with even number of even-length cycles:  $(\cdot \cdot \cdot)$ ,  $(\cdot \cdot)(\cdot \cdot)$ ,  $(\cdot \cdot \cdot \cdot)$ ,  $(\cdot \cdot \cdot)(\cdot \cdot \cdot)$ ,  $(\cdot \cdot \cdot \cdot)(\cdot \cdot)$ ,  $(\cdot \cdot)(\cdot \cdot)(\cdot \cdot)$ , ... This helps enumerate the elements in  $A_n$ :  $A_3 = \{1, (1\ 2\ 3), (3\ 2\ 1)\}$ ;  $A_4 = \{1, (1\ 2\ 3), \dots, (1\ 2)(3\ 4), \dots\}$ , etc.

Ⓑ (geometric) the number of intersection points in any “picture” of  $\sigma$

② Conjugation in  $S_n$ : To compute  $\sigma\tau\sigma^{-1}$ , write  $\tau$  as a product  $(i\ j\ \dots)$  of cycles; then

$$\sigma(i\ j\ \dots)\sigma^{-1} = (\sigma(i)\ \sigma(j)\ \dots)$$

i.e. *replace each number in  $\tau$  by its image under  $\sigma$* . This is easy to see if  $\tau$  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 if two elements in  $S_n$  are conjugate, then they have the same cycle structure. The converse is also

true; indeed it is an easy to determine all  $\sigma$  for which  $\sigma\tau\sigma^{-1} = \tau'$  for any  $\tau$  and  $\tau'$  which have the same cycle structure.

Conjugation in  $A_n$  is more complicated; one must check whether any of the possible conjugating permutations is even. For example  $\tau = (2\ 3\ 4)$  and  $\tau' = (4\ 3\ 2)$  are conjugate in  $S_4$  (why?) but not in  $A_4$  (since  $\sigma\tau\sigma^{-1} = \tau' \implies \sigma$  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.

③  $A_1$  and  $A_2$  are trivial groups;  $A_3 \cong C_3$ ;  $A_4 \cong T_{12}$ ,  $A_5 \cong I_{60}$ .

④  $A_n$  is generated by 3-cycles. Indeed each element of  $A_n$  can be written as a product of an even number of transpositions, and  $(i\ j)(j\ k) = (i\ j\ k)$ ,  $(i\ j)(k\ \ell) = (i\ j\ k)(j\ k\ \ell)$ .

⑤ Recall that  $A_n \triangleleft S_n$ . In fact if  $n \geq 5$ , then  $A_n$  is the only proper normal subgroup of  $S_n$ .

Proof: Let  $1 \neq K \triangleleft S_n$ . Then any  $\sigma \neq 1$  in  $K$  has a disjoint cycle decomposition of the form  $(i\ j\ \dots)$ , and so does not commute with the transposition  $\tau = (j\ k)$ , for any chosen  $k \neq i, j$ . 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  $[\sigma, \tau] \in K$  (since  $[\sigma, \tau] = \sigma(\tau\sigma^{-1}\tau^{-1})$  and  $K$  is normal) and  $[\sigma, \tau]$  is a product  $(\sigma\tau\sigma^{-1})(\tau^{-1})$  of two distinct transpositions (by ②). If these transpositions overlap, then  $[\sigma, \tau]$  is a 3-cycle  $\implies K$  contains all 3-cycles (since it is normal)  $\implies K \subset A_n$  (by ④)  $\implies K = A_n$  or  $S_n$ . If they don’t overlap, then  $K$  contains all products of pairs of disjoint transpositions (since it is normal), and in particular  $(1\ 2)(3\ 4)$  and  $(3\ 4)(2\ 5)$ , whose product is the 3-cycle  $(1\ 2)(2\ 5) = (1\ 2\ 5) \implies K$  contains all 3-cycles and so  $K = A_n$  or  $S_n$ .

Note We have repeatedly used the observation that a normal subgroup that contains an element  $h$  must contain all conjugates of  $h$ . In fact  $H$  is normal in  $G$  if and only if it is a union of conjugacy classes in  $G$ . (The conjugacy class of  $x \in G$  is the set of all elts in  $G$  that are conjugate to  $g$ .)

In general, one can understand a lot about the structure of a group from a knowledge of its normal subgroups. A group which has no proper normal subgroups is called a simple group; these are the building blocks of all finite groups. (More on this later)

Examples ① Any group of prime order is simple (indeed such a group has no proper subgroups whatsoever by Lagrange’s Theorem).

② Abel's Theorem  $A_n$  is simple for all  $n \geq 5$ .

Proof Suppose  $\exists K \triangleleft A_n$ , but  $K \neq A_n$  or  $1$ . Then  $A_n$  is the normalizer of  $K$  in  $S_n$ , by remark ⑤ above, and so  $K$  has exactly two “conjugates” in  $S_n$ ; i.e. setting  $H = (1\ 2)K(1\ 2)$ , we have  $\tau K \tau^{-1} = K$  or  $H$  according to whether  $\tau$  is even or odd (check this). But then  $H \cap K \triangleleft S_n$  and so  $H \cap K = 1$ , by ⑤ again. It follows that the elements of  $H$  commute with the elements of  $K$  (note  $H \triangleleft A_n$ ). But if  $\sigma \neq 1 \in K$ , then  $\exists$  odd  $\tau$  such that  $\sigma$  and  $\tau \sigma \tau^{-1}$  do not commute (for example, if  $\sigma = (i\ j\ k\ \dots)$  or  $(i\ j)(k\ \ell)\dots$ , take  $\tau = (k\ m)$  for any  $m \neq i, j, k, \ell$  and consider the image of  $j$  or  $\ell$ , respectively), which is a contradiction.  $\square$

## §5. Quotient Groups

Recall that normal subgroups can be characterized in a variety of ways.

Normality Lemma A subgroup  $H$  of  $G$  is normal in  $G$  if and only if any of the following conditions holds:

- Ⓐ  $H$  is a union of conj classes in  $G$     Ⓑ  $xhx^{-1} \in H$  for all  $h \in H, x \in G$
- Ⓒ  $xHx^{-1} \subset H$  for all  $x \in G$     Ⓓ  $xHx^{-1} = H$  for all  $x \in G$
- Ⓔ  $xH = Hx$  for all  $x \in G$     Ⓕ  $xHyH = xyH$  for all  $x, y \in G$

Proof The equivalence of Ⓐ – Ⓔ was noted previously, so it suffices to show Ⓔ  $\implies$  Ⓕ  $\implies$  Ⓒ: Assuming Ⓔ, have  $xHyH = xyHH = xyH$  ( $HH \subset H$  since  $H < G$ , and  $HH \supset H$  since  $1 \in H$ ). Assuming Ⓕ, have  $xHx^{-1}H = H \implies xHx^{-1} \subset H$  since  $1 \in H$ .  $\square$

Using Ⓕ, can make the set  $G/H$  of left cosets of  $H$  in  $G$  into a group, called the quotient group of  $G$  by  $H$ , provided  $H$  is normal in  $G$ :

Theorem If  $H \triangleleft G$ , then  $G/H$  is a group under the operation defined by  $xH \cdot yH = xyH$ . Furthermore the map

$$p: G \rightarrow G/H$$

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 homomorphism, 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 The product of two cosets  $H_1, H_2$  in  $G/H$  can be described in words as follows: Choose one element from each. Then  $H_1H_2$  is the coset containing the product of these elements. The lemma shows that this is “well-defined”, i.e. independent of which elements you choose.

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  $\mathbb{Z}/n\mathbb{Z} = \{k + n\mathbb{Z} \mid k = 0, \dots, n-1\}$ .

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  $(g, g') + (h, h') = (g + h, g' + h')$ . In other words  $G \oplus G'$  is the same group as  $G \times G'$ , but written additively (cf. example ② below).

③ Any quotient group  $G/H$  of an abelian group  $G$  is abelian, since  $xHyH = xyH = yxH = yHxH$ , for any  $x, y \in G$ .

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

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

③ Let  $S := \langle (0, 1) \rangle < G := \mathbb{Z}_2 \oplus \mathbb{Z}_4$ . Note that  $|S| = 4$  (since  $(0, 1)$  has order 4) so  $G/S$  has order  $|G/S| = |G|/|S| = 4/2 = 2$ , 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  $(1\ 2\ 3)$ ,  $H = \langle (1\ 2\ 3) \rangle = \{1, (1\ 2\ 3), (1\ 3\ 2)\} < S_3$ . 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  $Z(D_8) = \{1, r^2\} < D_8$ , 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

Universal Property of Quotient Groups *Let  $K \triangleleft G$  and  $p : G \rightarrow G/K$  be the natural projection. Then for any homomorphism  $f : G \rightarrow H$  whose kernel contains  $K$ , there exists a unique homomorphism  $g : G/K \rightarrow H$  such that  $f = g \circ p$ , i.e. the following diagram commutes*

$$\begin{array}{ccc} G & \xrightarrow{p} & G/\ker(f) \\ f \searrow & & \downarrow g \\ & & H \end{array}$$

*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 homomorphism ( $g(xKyK) = g(xyK) = xy = g(xK)g(yK)$ ) with  $\ker(g) = \{xK \mid f(x) = 1\} = \ker(f)/K$  and  $\text{im}(g) = \{f(x) \mid x \in G\} = \text{im}(f)$ .  $\square$

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 ② above) by constructing an explicit iso. One such arises from the UPQG via the map  $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$ ,  $(a, b) \mapsto (a, b)$  (check this).

It has the following important consequences:

The Isomorphism Theorems

- ① *If  $f : G \rightarrow H$  is a homomorphism, then  $G/\ker(f) \cong \text{im}(f)$ .*
- ② *If  $H < G$  and  $K \triangleleft G$ , then  $H \cap K \triangleleft H$  and  $HK/K \cong H/H \cap K$ .*

$$\begin{array}{ccc} & HK & \\ & / \quad \backslash & \\ H & & K \\ & \backslash \quad / & \\ & H \cap K & \end{array}$$

- ③ *If  $H, K \triangleleft G$  with  $H \subset K$ , then  $K/H \triangleleft G/H$  and  $G/K \cong (G/H)/(K/H)$ .*

Proof Apply the Universal Property to

$$\begin{array}{ccc} \textcircled{1} & G & \longrightarrow G/\ker(f) \\ & f \searrow & \downarrow \\ & & \text{im}(f) \subset H \end{array}$$

\textcircled{2} (note that  $HK$  is a subgroup of  $G$ )

$$\begin{array}{ccc} H & \longrightarrow & H/H \cap K \\ \text{incl} \downarrow & & \downarrow \\ HK & \longrightarrow & HK/K \end{array}$$

$$\begin{array}{ccc} \textcircled{3} & G & \longrightarrow G/H \\ & \searrow & \downarrow \leftarrow \text{now apply } \textcircled{1} \text{ to this} \\ & & G/K \end{array}$$

The Correspondence Theorem Let  $f : G \rightarrow H$  be a homomorphism of groups,  $\mathcal{G}$  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  $I = \text{im}(f)$ . Then the map

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

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

$$(a) \quad S < T \iff f(S) < f(T), \text{ in which case } |T : S| = |f(T) : f(S)|$$

$$(b) \quad S \triangleleft T \iff f(S) \triangleleft f(T), \text{ in which case } T/S \cong f(T)/f(S)$$

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

Indeed  $f^{-1}f(S) = S$ : The inclusion  $\supset$  holds in general ( $s \in S \implies f(s) \in f(S)$ , i.e.  $s \in f^{-1}f(S)$ ) and  $\subset$  holds since  $S \supset K$  (if  $x \in f^{-1}f(S)$ , i.e.  $f(x) \in f(S)$  so  $f(x) = f(s)$  for some  $s \in S$ , then  $f(xs^{-1}) = 1$ , i.e.  $xs^{-1} \in K \implies x \in Ks \subset S$ ). Similarly  $ff^{-1}(A) = A$ :  $\subset$  holds in gen'l, 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.  $\square$

Examples ① applied to  $GL_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^\bullet$  gives  $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\bullet$ .

② applied to  $M, N \triangleleft G$  for which  $M \cap N = 1$  and  $MN = G$  gives isomorphisms

$$G/M \cong N \quad \text{and} \quad G/N \cong M.$$

Note: if  $M$  and  $N$  are simple groups which are “maximal” proper normal subgroups of  $G$  (i.e. there are no larger such subgroups) then the conditions  $M \cap N = 1$  and  $MN = G$  are automatic.

Application : Classification of Finite Groups

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

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

each a maximal proper normal subgroup of the preceding.

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, cf. the special case in ② above, where  $n = 1$ ).

Unfortunately  $\exists$  distinct groups with identical composition factors, so the classification of finite groups is 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 ( $\sim 1980$ ): 18 infinite families

- 1)  $C_p$  ( $p$  prime)
- 2)  $A_n$  ( $n \geq 5$ )
- 3)  $PSL_n(F)$  ( $F$  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, the “monster” group.

## §6. Sylow Theory

Throughout this section

$G$  will denote a finite group of order  $n$ .

Recall Lagrange's Theorem:  $H < G$ ,  $|H| = k \implies k|n$ . The converse fails:  $k|n \not\implies \exists H < G$ ,  $|H| = k$ . For example

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

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

Partial converses hold:

Cauchy's Theorem *If  $p$  is prime and  $p|n$ , then  $\exists H < G$  with  $|H| = p$ .*

More generally

Sylow Theorem I *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  $p^\alpha$  is called a  $p$ -group, and if  $P < G$  then  $P$  is called a  $p$ -subgroup of  $G$ . If in addition  $p^\alpha$  is the *largest* power of  $p$  that divides  $|G|$ , that is

$$n = p^\alpha m \text{ and } p \nmid m$$

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

For 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.

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

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

Example If  $G$  has order  $12 = 2^2 \cdot 3$ , 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  $\langle(234)\rangle$ , which are all conjugate). 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 the 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  $P \triangleleft G$  (since any  $xPx^{-1}$  is also a Sylow  $p$ -subgroup of  $G$ ). Thus

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

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  $n_p = 1$ :

①  $|G| = pq$  for distinct primes  $p$  and  $q \implies G$  is not simple.

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

For example no groups of order 6, 10, 14, 15, 21, 22, 26, 33, ... are simple.

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

Proof: 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:  $|G| > 6 \cdot 4 + 2 \cdot 10 + 1 \cdot 3 = 47 \implies \Leftarrow$ . Thus  $G$  is not simple.  $\square$

---

<sup>†</sup>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  $q$ -subgroup  $Q \cong C_q$ . Thus  $P, Q \triangleleft G$  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, ... are cyclic.

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  $p^2q$  and  $p^\alpha$  (for any  $\alpha > 1$ ) are never simple. Much deeper results:

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

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

Proofs of Sylow Theorems (using group actions)

Let  $G \times X \rightarrow X$ ,  $(g, x) \mapsto g \cdot x$  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:

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  $|G| = |Gx||G_x|$ .*

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

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  $Gx \cap Gy \neq \emptyset \implies g \cdot x = h \cdot y$  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

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  $|X| \equiv |X^P| \pmod{p}$ .  $\square$

Corollary *The center  $Z$  of any nontrivial  $p$ -group  $P$  is nontrivial.<sup>†</sup>*

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.  $\square$

Now we are ready to prove Sylow's Theorems.

---

<sup>†</sup>It follows that if  $|P| = p^2$ , then  $P$  is abelian. Indeed  $|G/P| = 1$  or  $p$  by the Corollary, and so  $P/Z$  is cyclic, 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 abelian:  $\forall u, v \in Z, x^k u x^\ell v = x^{k+\ell} u v = x^\ell v x^k u$ .

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

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  $p \implies |G/Z| = p^{\alpha-1}m \implies$  (by induction)  $G/P$  has subgroups of order  $1, p, \dots, p^{\alpha-1} \implies$  (by the correspondence theorem)  $G$  has subgroups of order  $1, p, \dots, p^\alpha$ .

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  $x \notin Z \implies p^\alpha \mid |Z(x)| \implies$  (by induction)  $Z(x)$  has subgroups of order  $1, p, \dots, p^\alpha \implies G$  does as well.  $\square$

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  $|G/Q| = m \not\equiv 0 \pmod{p}$ , it follows from the lemma that  $\exists$  a fixed point  $xQ$ , i.e. for all  $g \in P$ , have

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

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

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  $m = |G : P| = |G : N(P)||N(P) : P|$ , i.e.  $n_p \mid m$ .

To see  $n_p \equiv 1 \pmod{p}$ , consider the action of  $P$  on  $X$  by conjugation. Since  $n_p \mid m$ , we have  $n_p \not\equiv 0 \pmod{p} \implies \exists$  a fixed point  $Q \in X$ , i.e.  $P \subset N(Q)$ . But this forces  $P = Q$ , since  $Q \triangleleft N(Q)$  (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.  $\square$

Exercises 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.

### III Rings

#### §1. 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  $\exists 1 \in R$  such that  $1r = r1 = r$  ( $\forall r \in R$ ), and  $R$  is commutative if  $rs = sr$  ( $\forall r, s \in R$ ).

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 comm.

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

$$\mathbb{Z}[\zeta] := \{a + b\zeta \mid a, b \in \mathbb{Z}\} < \mathbb{C}$$

where  $\zeta = e^{2\pi i/3} \in \mathbb{C}$ ; this ring will play a special role in the proof below of Fermat's last theorem for  $n = 3$ . (Draw "pictures" of these rings as square/triangular lattice points in the 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  $RG = \{\sum_{i=0}^n r_i g_i \mid r_i \in R, g_i \in G\}$  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 all rings, 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  $1 \neq 0$  where this holds are called integral domains (more on this below).

Definition A function  $f : R \rightarrow S$ , 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  $f$  is defined by  $\ker(f) = f^{-1}(0)$  (not  $f^{-1}(1)$ !) and the image  $\text{im}(f)$  is defined in the usual way. Both are subrings (of  $R$  and  $S$  respectively). Have the usual criterion  $f$  is 1-1  $\iff \ker(f) = \{0\}$ .

- Example ①  $f : \mathbb{Z} \rightarrow \mathbb{Z}_n, f(k) = \bar{k}$  is an epimorphism with kernel  $n\mathbb{Z}$ .  
 ②  $g : \mathbb{Z} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n, g(k) = (\bar{k}, \bar{k})$  (e.g. if  $m = 5, n = 9$  then  $f(13) = (3, 4)$ ) is a homomorphism with kernel  $\ell\mathbb{Z}$ , where  $\ell$  is the lcm of  $m$  and  $n$ .

## §2. Ideals and Quotient Rings

Definition A subring  $A$  of a ring  $R$  is an ideal in  $R$ , denoted  $A \triangleleft R$ , if  $a \in A, r \in R \implies ra$  and  $ar \in A$ , i.e.  $A$  is closed under multiplication on the left or right by arbitrary elements of  $R$ .

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

Examples ① Every ring  $R$  has the trivial ideals  $\{0\}$  and  $R$ ; all other ideals are called proper.

①  $n\mathbb{Z} \triangleleft \mathbb{Z}$  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

$$aR = \{ar \mid r \in R\} \quad (\text{also denoted } \langle a \rangle)$$

is an ideal in  $R$  containing  $a$  (verify this) called the principal ideal generated by  $a$ . An ideal  $J \triangleleft R$  is called a principal ideal if  $J = \langle a \rangle$  for some  $a \in R$ .

③ Let  $f : R \rightarrow S$  be a ring morphism. Then  $\ker(f) \triangleleft R$  (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  $\cdot$ : 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 indep 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 gps, and isomorphism theorems, e.g.:

First Isomorphism Theorem If  $f : R \rightarrow S$  is a ring homomorphism, then  $R/\ker(f) \cong \text{im}(f)$ .

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

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

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

mapping  $\bar{k}$  to  $(\bar{k}, \bar{k})$ . This  $\implies$  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 soln set  $\{17 + 45k \mid k \in \mathbb{Z}\}$ .

### §3. 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) a zero divisor if  $\exists b \in R - 0$  such that  $ab = 0$  (b) 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

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

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

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

Clearly every field is a domain (since  $R^\circ \cap R^\bullet = \emptyset$ ) 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:

Lemma<sup>†</sup>  $R$  is a field  $\iff R$  has no proper ideals.

Proof ( $\implies$ ) 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  $J = R$ . ( $\impliedby$ ) 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.  $\square$

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

Definition<sup>†</sup> Let  $J \triangleleft R$ ,  $J \neq R$ . Then  $J$  is prime if  $ab \in J \implies a \in J$  or  $b \in J$ , and  $J$  is maximal if  $J \subset K \triangleleft R \implies K = J$  or  $K = R$ .

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

Theorem Let  $R$  be a commutative ring with  $1 \neq 0$  and  $J \triangleleft R$ . Then (a)  $J$  is prime  $\iff R/J$  is a domain (b)  $J$  is maximal  $\iff R/J$  is a field.

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

<sup>†</sup>Recall that we are assuming that  $R$  is a commutative ring with  $1 \neq 0$ .

Examples ①  $n\mathbb{Z} \triangleleft \mathbb{Z}$  is prime  $\iff$  maximal  $\iff n$  is a prime number.

② In general, maximal ideals are always prime (HW) but not conversely. For example  $\langle x \rangle \triangleleft \mathbb{Z}[x]$  (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).

### Coda

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<sub>n</sub> for any given  $n$ .)

Remarks ① FLT<sub>n</sub>  $\implies$  FLT<sub>kn</sub>, 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  $\implies$  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  $\zeta_p = e^{2\pi i/n}$ ; their mistake, uncovered by Kummer, was to assume that  $\Lambda_p$  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  $\Lambda$  (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  $\Lambda$ , and all other elements have norm  $> 1$ ).

It is a fact (which we won't prove here) that any nonzero, nonunit in  $\Lambda$  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  $\Lambda$ , so if  $p = ab$  then  $|p| = |a||b| \implies |a|$  or  $|b| = 1$ , i.e.  $a$  or  $b \in \Lambda^\bullet$ .

Remarks ① 3 is not prime in  $\Lambda$ , 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

$$a = \bar{a} + rp$$

for some  $r \in \Lambda$  where  $\bar{a} = 0, 1$  or  $-1$ . This defines an isomorphism

$$\Lambda/p\Lambda \rightarrow \mathbb{Z}_3, \quad a + p\Lambda \mapsto \bar{a}$$

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

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

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

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

Case 2a Suppose  $p \mid z_o$ . Then  $\bar{x}_o = -\bar{y}_o = \pm 1$ , 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  $p^k \mid z_o$ , called the  $p$ -order of the solution. A simple calculation (reducing mod  $p^4$ ) shows that in fact  $k \geq 2$ .<sup>†</sup> We assume that the solution was chosen so that  $k$  is minimal.

Now (and this is the magic!) define

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

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

①  $a + b + c = 0$

②  $abc = (x_o^3 + y_o^3)/p^3 = u(z_o/p)^3$

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  $x_o, y_o$ ).

② and ③ show that each of  $a, b, c$  is a unit times a cube, and that these cubes are relatively prime. It follows from 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  $p \nmid x_1, p \nmid y_1, p \mid z_1, p^k \nmid z_1$ , and

$$x_1^3 + v y_1^3 + w z_1^3 = 0$$

for suitable units  $v, w$ . It is easy to check that  $v = \pm 1$  (since the left hand side is congruent mod  $p^3$  to  $\bar{x}_1 + v \bar{y}_1 = \pm 1 \pm v \implies v \equiv_{p^3} \pm 1 \implies v = \pm 1$ ) and 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  $p \mid x_o$  (or  $y_o$ ). Then  $u\bar{z} \equiv_{p^3} \bar{x} + \bar{y} \implies u \equiv_{p^3} \pm 1 \implies u = \pm 1 \implies (-y_o)^3 + (\pm z_o)^3 = x_o^3$ , which is handled in case 2a.

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

---

<sup>†</sup>  $x_o^3 + y_o^3 = (rp + 1)^3 + (sp - 1)^3 \equiv_{p^4} r^3 + s^3 - \zeta^2(r + s)p^3 \equiv_{p^4} (\bar{r} + \bar{s} - (\bar{r} + \bar{s}))p^3 = 0 \implies z \equiv_{p^2} 0$ .