MA 45000 – H01 CRN 23368 Honors Algebra.

https://www.math.purdue.edu/~twooley/2022algebra/2022algebra.html

Resource for all assignments, other arrangements for course, news.

Office Hours:

M	2-3pm	Zoom, or in person in 4.22 Math.
W	1-2pm	
F	3-4pm	

Exams:

MT1: In Class Monday 3rd October, 2022

MT2: In Class Wednesday 2nd November, 2022

FE: Finals Week, TBA.

Textbook:

- Abstract Algebra, I.N. Herstein, 3rd edition, Wiley, 1996.
  ~ First 5 chapters + some additional material.

Secondary:

- Abstract Algebra, D.S. Dummit & R.M. Foote, 3rd edition, Wiley 2004
  (Concise, dense, serious) >900 pages.
- Contemporary Abstract Algebra, J.A. Gallian, 10th edition, CRC Press, 2020.
  (No detail left out, [redacted], harder to isolate important details).

J.B. Fraleigh

Homeworks: Weekly, due noon Wednesday in Gradescope / Brightspace
(to be confirmed with grader)

Assessment: Maximum of

35% HW + 20% MT1 + 10% MT2 + 35% FE

35% HW + 10% MT1 + 20% MT2 + 35% FE

Top 10 (of ≥12) homeworks counted, each equally.

See notes on course for minimum requirements to guarantee A, B, C, ...

DRC

COVID-19: Masks, attendance etc

Emergency: Fire – evacuate to area between Bearing Hall (BRNG) and UNIV, or lobby of BRNG (bad weather)

Tornado: (shelter in place) interior of UNIV or basement of BRNG

Active Threat: UNIV 101.

First homework due Wednesday 31 August at noon.

---

§1. Review of set theory, mappings and the integers.

§1.1 Sets.

Assume that you have encountered the basics of set theory in earlier courses.

Some words on notation:

$A = \{a_1, a_2, \dots, a_n\}$ the set containing elements $a_1, a_2, \dots, a_n$.

$\emptyset$ set containing no elements (empty set, null set).

$A \subset B$ means for all $a \in A$ one has $a \in B$. (subset of)

$A \subseteq B$ means $A \subset B$

$A \subsetneq B$ means $A \subseteq B$ but $A \neq B$.

$A \subset B$ & $B \subset A$ implies $A = B$ (prove!)

If $A, B \subset S$ then

$A \cap B := \{a \in S : a \in A \text{ and } a \in B\}$

$A \cup B := \{a \in S : a \in A \text{ or } a \in B\}$

(possibly $a \in A \cap B$).

$A \setminus B := \{a \in S : a \in A \text{ and } a \notin B\} = A - B$.

$A \setminus A = \emptyset$.

$A^c := \{a \in S : a \notin A\} = A'$.

Note: $A \cup (B \cap C) = (A \cup B) \cap (A \cap C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cup C)$ (prove!)

Cartesian Products: Given sets A, B, define

$$A \times B = \{ (a,b) : a \in A \text{ and } b \in B \}$$

((a,b): ordered pair.)

example: If $A = \{1,2\}$ and $B = \{x,y,z\}$ then

$$A \times B = \{ (1,x), (2,x), (1,y), (2,y), (1,z), (2,z) \}.$$

$$A_1 \times A_2 \times \cdots \times A_n = \{ (a_1, a_2, \ldots, a_n) : a_i \in A_i \ (1 \le i \le n) \}.$$

Cardinality: Number of elements in a set (if finite) — more on this later. If $A = \{a_1, \ldots, a_n\}$ then

$$\text{card}(A) = \#\{a_1, \ldots, a_n\} = n = |A|.$$

Power set Given $A \subset S$, write

$$2^A := \{ B \subset S : B \subset A \}.$$

(set of all subsets of A.)

exercise: Prove $\text{card}(2^A) = 2^{\text{card}(A)}$ when $\text{card}(A)$ is finite.

---

§1.3. Mappings. Given two sets S and T, consider a **mapping** (or function)

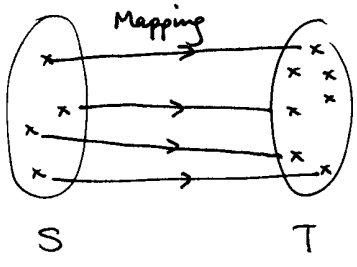
$$f : S \longrightarrow T, \quad s \longmapsto f(s)$$

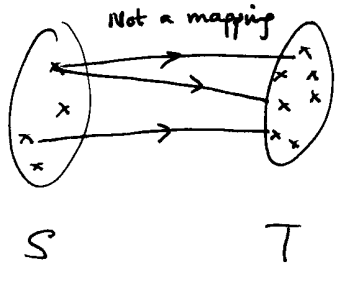
(S: domain; $f(s)$: image of s under f.)

a rule which to each element $s \in S$ assigns one (and only one) element of T. Thus f is defined as the set

$$F := \{ (s, f(s)) : s \in S \text{ and } f(s) \in T \} \subset S \times T,$$

with the property that whenever $(s_1, t_1) \in F$ and $(s_2, t_2) \in F$, then if $s_1 = s_2$ then $t_1 = t_2$.





Properties: Given mappings $f : S \to T$

$g : S \to T$

Say $f = g$ when $f(s) = g(s)$ for all $s \in S$.

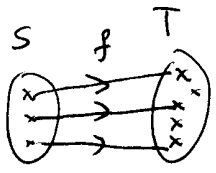
Surjective (or onto): $f : S \to T$ is surjective if, for all $t \in T$ there exists $s \in S$ such that $f(s) = t$.

Injective (or one-to-one) $f : S \to T$ is injective if, whenever $s_1, s_2 \in S$ and $f(s_1) = f(s_2)$, then $s_1 = s_2$.

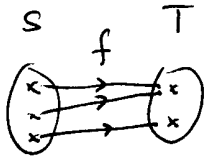
(equivalently, $s_1 \neq s_2 \Rightarrow f(s_1) \neq f(s_2)$).

Bijective $f : S \to T$ is bijective if it is both injective and surjective.

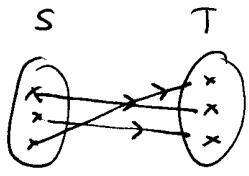
(1-1 correspondence).



injective



surjective



bijective.

N.B. Caution when number of elements is infinite! For example, there is a bijection from

$$\mathbb{N} = \{1, 2, \ldots\}$$

to

$$\mathbb{Q} = \left\{ \pm \frac{m}{n} : m \in \mathbb{N} \cup \{0\} \text{ and } n \in \mathbb{N} \right\}.$$

Definition: Let $f : S \to T$ be a mapping and $A \subset T$.

Then $f^{-1}(A) := \{ s \in S : f(s) \in A \}$ is called the inverse image of A under f.

If $t \in T$, then $f^{-1}(t) := f^{-1}(\{t\})$ is preimage of t.

It is not necessarily the case that f^{-1} defines "the" inverse function.

Only a mapping if $f^{-1}(t)$ is non-empty and contains precisely one element for each $t \in T$.

Exercise: Prove that if $f: S \to T$ is bijective, then f^{-1} defines a mapping from T onto S, and further f^{-1} is bijective.

Compositions. Suppose $g: S \to T$ and $f: T \to U$ are mappings. Then the composition of f and g is defined by

$$f \circ g : S \to U$$

where $f \circ g(s) = f(g(s))$ for all $s \in S$.

- Check this is a mapping: $g(s) \in T$ for all $s \in S$, and so $f(g(s))$ is defined (uniquely). ["well-defined"].

Can also define $f \circ g \circ h$ (etc) when

$h: S \to T$, $g: T \to U$, $h: U \to V$

are mappings.

Exercises: (1) Suppose $f: S \to T$ is a bijective mapping, so $f^{-1}: T \to S$ is a bijective mapping.

Prove that $f \circ f^{-1} = id_T$ and $f^{-1} \circ f = id_S$,

where $id_S : S \to S$ and $id_T : T \to T$

$s \mapsto s$ $\quad$ $t \mapsto t$.

Properties of Compositions:

Lemma 1.3.1: If $h: S \to T$, $g: T \to U$ & $f: U \to V$ are mappings, then $f \circ (g \circ h) = (f \circ g) \circ h$ (associative law).

Proof: Need to show $f\circ(g\circ h)$ & $(f\circ g)\circ h$ define the same mappings, so need that for all $s\in S$ have

$$(f\circ(g\circ h))(s) = ((f\circ g)\circ h)(s).$$

But $(f\circ(g\circ h))(s) = f((g\circ h)(s)) = f(g(h(s)))$

$= ((f\circ g)\circ h)(s) = (f\circ g)(h(s))$ for all $s\in S$.

This completes the proof. //

Lemma 1.3.2 a If $g: S\to T$ and $f: T\to U$ are both injective, then $f\circ g$ is injective.

Proof: Ex. $f\circ g(s_1) = f\circ g(s_2) \Leftrightarrow f(g(s_1)) = f(g(s_2)) \overset{\text{inj } f}{\Leftrightarrow} g(s_1) = g(s_2) \overset{\text{inj } g}{\Leftrightarrow} s_1 = s_2$. //

Lemma 1.3.2b If $g: S\to T$ and $f: T\to U$ are both surjective, then $f\circ g$ is surjective.

Proof. Suppose $u\in U$. Then by surj. of f there exists $t\in T$ with

$$f(t) = u.$$

Since $t\in T$, by surj. of g there exists $s\in S$ with $g(s) = t$. Then $f(g(s)) = f(t) = u$. So for all $u\in U$ there exists $s\in S$ s.t. $f(g(s)) = u$, so $f\circ g$ is surj. //

Lemma 1.3.3. If $g: S\to T$ and $f: T\to U$ are both bijections, then $f\circ g$ is bijective.

Proof: Combine Lemmata 1.3.2 a, b. //

Lemma 1.3.4. Suppose that $f: S\to T$ is a bijection.

Then $f^{-1}: T\to S$ is a bijection, and

$$f\circ f^{-1} = id_T, \quad f^{-1}\circ f = id_S. \quad \text{(identity mappings)}$$

Proof: Given $t\in T$, one has $f^{-1}(t)\in S$, say $f^{-1}(t) = s$. Then

$f(s) = t$, and $f \circ f^{-1}(t) = f(f^{-1}(t)) = f(s) = t$.

So $f \circ f^{-1} = id_T$. Similarly for $f^{-1} \circ f$. //

Exercise (Lemma 1.3.5) If $f : S \to T$ then

$$i_T \circ f = f \quad \text{and} \quad f \circ i_S = f.$$

Note: If $f : A \to \{1, 2, \ldots, n\}$ is bijective, then $|A| = n$.

§1.4. Self-mappings.

Defn When $S \neq \phi$,

Define $A(S) = \{ f : f : S \to S \text{ is a bijective mapping} \}$.

Special case: When card (S) is finite, say $|S| = n$, then

$A(S)$ is the set of permutations of S,

(the symmetric group of degree n).

Suffices to consider $S = \{1, 2, \ldots, n\}$, and then write

S_n for the set of permutations of $\{1, 2, \ldots, n\}$.

If $f \in S_n$, we can define the action of f symbolically by writing

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}.$$

There is also the cycle decomposition notation — more on this later.

For example

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} \text{ becomes } (1\ 2\ 4)(3\ 5)(6)$$

Lemma 1.4.1. ("A(S) forms a group" — and we have not yet defined a "group"!)

The set of bijective self-maps $A(S)$ satisfies the following properties:

(a) whenever $f, g \in A(S)$, then $f \circ g \in A(S)$ ("closure")

(b) when $f, g, h \in A(S)$, then $f \circ (g \circ h) = (f \circ g) \circ h$ ("associativity")

(c) there is an element $i \in A(S)$ such that, for all $f \in A(S)$, one has $i \circ f = f \circ i = f$ ("identity element")

(d) For all $f \in A(S)$, there exists $g \in A(S)$ such that $f \circ g = g \circ f = i$ ("inverse element")

[Customary to write $g = f^{-1}$.]

Proof. Given what we have already discussed, these are easy exercises — note; we are using the bijective property of elements of $A(S)$ extensively. //

Lemma 1.4.2. When $|S| = n$ we have $|A(S)| = n!$.

Proof. We can label S as $S = \{x_1, \dots, x_n\}$. Then if $f \in A(S)$, we have that f is bijective. In particular, we have $f(x_i) \neq f(x_j)$ for $i \neq j$, and for all $1 \leq i \leq n$ there exists $1 \leq j \leq n$ with $f(x_j) = x_i$.

Then
$$f(x_1) \in \{x_1, \dots, x_n\}, \qquad n \text{ choices}$$
$$f(x_2) \in \{x_1, \dots, x_n\} \setminus \{f(x_1)\} \qquad n-1 \text{ choices}$$
$$f(x_3) \in \{x_1, \dots, x_n\} \setminus \{f(x_1), f(x_2)\} \qquad n-2 \text{ choices}$$
$$\vdots \qquad\qquad \vdots$$
$$f(x_n) \in \{x_1, \dots, x_n\} \setminus \{f(x_1), \dots, f(x_{n-1})\} \qquad 1 \text{ choice}$$

$|\{f(x_1), \dots, f(x_n)\}| = n$, so f is surjective.

Then there are $n(n-1)\cdots 2\cdot 1 = n!$ possible choices for f, all distinct. //

§1.5. Arithmetic of the integers. We labour this topic a little because it motivates the arithmetic of polynomial rings later in the course.

$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$, $\mathbb{N} = \{1, 2, \dots\}$

integers — Natural numbers

Definition (Divisibility). (i) Suppose $a, b \in \mathbb{Z}$. We say b divides a (written $b|a$) when there exists $c \in \mathbb{Z}$ s.t. $a = bc$.

We then say a is divisible by b, or b is a divisor of a.

(ii) When a is not divisible by b, we write $b \nmid a$.

(iii) When $b|a$ and $1 \le b < |a|$, we say b is a proper divisor of a.

(iv) Write $a^k \| b$ when $a^k | b$ but $a^{k+1} \nmid b$.

("$b|a$" makes sense only when $b \neq 0$).

Lemma 1.5.2. (i) $a|a$ for all $a \in \mathbb{Z}\setminus\{0\}$

(ii) $a|0$ for all $a \in \mathbb{Z}\setminus\{0\}$

(iii) $a|b$ and $b|c$ implies $a|c$

(iv) $a|b$ and $a|c$ implies, for all $x, y \in \mathbb{Z}$, one has $a \mid (bx+cy)$

(v) $a|b$ and $b|a$ implies $a = \pm b$

(vi) $a|b$ and $a > 0$ and $b > 0$ implies $a \le b$

(vii) when $m \neq 0$, one has $a|b$ if and only if $ma|mb$.

Proof: Exercises.

(Herstein calls this Euclid's Algorithm — incorrectly).

Theorem 1.5.1 (Division Algorithm). For any $a, b \in \mathbb{Z}$ with $a > 0$, there exist unique integers q and r with $b = qa + r$ and $0 \leq r < a$. If, further, one has $a \nmid b$, then $0 < r < a$.

Proof. Let aq be the largest multiple of a not exceeding b.

Put $r = b - aq$, so $r \geq 0$. By hypothesis, one has $a(q+1) > b$, so $r = b - aq < a$. Thus the specified integers r and q exist. □

For uniqueness, suppose another pair q', r' exist satisfying analogous properties. If $r \neq r'$, we may suppose (by symmetry) that $r < r'$. Then

$$aq' + r' = b = aq + r,$$

whence

$$a(q - q') = r' - r.$$

Thus $a \mid (r' - r)$ and $0 < r' - r < a$ ⁂ (vi) of Theorem 1.5.2.

Thus $r = r'$, whence $aq' = q'a$, so that $q = q'$ (since $a \neq 0$).

Thus $(q, r) = (q', r')$ giving uniqueness. □

The final assertion follows on noting that if $r = 0$ then $b = qa$, so $a \mid b$. #

Definition. (i) Suppose $a \in \mathbb{Z} \setminus \{0\}$ and $b, c \in \mathbb{Z}$. Say a is a common divisor of b and c when $a \mid b$ and $a \mid c$;

(ii) The greatest common divisor of b and c, when $(b, c) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, is the largest common divisor, written (b, c).

(iii) When $g_1, \dots, g_n$ are integers, not all zero, write $(g_1, \dots, g_n)$ for the largest integer d satisfying $d \mid g_i$ $(1 \le i \le n)$.

Example $(0, 2) = 2$, $(-1, 3) = 1$, $(1729, 182) = 91$.

Note: (b, c) is unique, since it is the largest positive common divisor.

Theorem 1.5.3. If $g = (b, c)$, then there exist integers x and y with $g = bx + cy$.

Proof. Define $d = \min\{bu + cv : u, v \in \mathbb{Z} \text{ and } bu + cv > 0\}$. Also, let x, y be the values of u, v corresponding to this minimum, so $d = bx + cy$.

First prove $d \mid b$. If not, and $d \nmid b$, then by the Division Algorithm there exist $r, q \in \mathbb{Z}$ with $b = qd + r$ and $0 < r < d$. Then

$$r = b - dq = b - q(bx + cy) = b(1 - qx) + c(-qy),$$

whence $r \ge \min\{bu + cv : u, v \in \mathbb{Z} \ \& \ bu + cv > 0\} = d$.

But $r < d$, so # contradiction proves $d \mid b$.

Similarly $d \mid c$, so d is a common divisor of b & c, say $d \le (b, c)$. But $g = (b, c)$, so there exist integers B and C with $b = gB$ and $c = gC$, and $d = g(Bx + Cy)$, whence $g \mid d$. Then $g > 0$, $d > 0$ and $g \mid d$, so $g \le d$. Then $d \ge (b, c)$ yet also $d \le (b, c)$. Hence $d = (b, c)$ and $(b, c) = bx + cy$. //

We say a and b are coprime (or relatively prime) if $(a,b)=1$.

Theorem 1.5.5. If $(a,b)=1$ and $a|bc$ then $a|c$.

Proof. There exist $x,y \in \mathbb{Z}$ with $1 = ax+by$, and $l \in \mathbb{Z}$ with $bc = al$. Then

$$\begin{aligned} c &= acx + bcy \\ &= a(cx+ly), \end{aligned}$$

so $a|c$. //

Definition. A natural number p (i) $p>1$ and (ii) whenever $d|p$, then $|d|=1$ or p, is called a prime number. All other integers exceeding 1 are called composite.

Theorem 1.5.7 Every integer n exceeding 1 is the product of prime numbers.

Proof. The theorem holds for $n=2$, since 2 is automatically prime. Suppose the theorem holds for $1<n\le N$. The least divisor of $N+1$ with $d>1$ is plainly prime, say p. But $(N+1)/p \le N$, so $\frac{N+1}{p}$ is either 1, or by hypothesis is a product of primes. Then $N+1$ is a product of primes whenever N is. Then (by induction) all $n>1$ are the product of primes. //

Theorem 1.5.8. (Fundamental Theorem of Arithmetic) Positive integers $n>1$ have unique factorisations into primes.

Proof. Suppose, by way of contradiction, that $n>1$ is the smallest natural number failing to have a unique factorisation into primes. Then if $n = q_1 \cdots q_t$ is one factorisation of n as the product of primes, and p is a prime factor of n in another factorisation, we have $p | q_1 \cdots q_t$. If $p \nmid q_i$ for

every i, then $(p, q_i) = 1$ for all i, and hence $p \nmid q_1 \cdots q_t$ (from Theorem 1.5.5: if $(p, q_1) = 1$ and $p \mid q_1(q_2 \cdots q_t)$, then $p \mid q_2 \cdots q_t$). # Thus $p \mid q_i$ for some i, so $q_i = p$ for some i. But then the integer n is either equal to p, and has a unique factorisation, or else the integer n_0, with $1 < n_0 = n/p < n$ fails to possess a unique factorisation into primes. This contradicts the minimality of n, so no and hence also n has a unique factorisation into primes. //

We can of course rearrange the factorisation of n so that

$$n = p_1^{a_1} \cdots p_t^{a_t},$$

where $p_1 < p_2 < \ldots < p_t$ are primes, $a_i \in \mathbb{N}$, and this representation is unique.

Theorem 1.5.9 (Euclid): There are infinitely prime numbers.

Proof. Suppose that $p_1, \ldots, p_k$ are distinct prime numbers. Then $n = p_1 \cdots p_k + 1$ satisfies $(n, p_i) = 1$ for each i, so n is an integer that is divisible by a prime p_{k+1} distinct from $p_1, \ldots, p_k$. Since 2 is prime, this argument shows that there are at least k primes for any $k \in \mathbb{N}$, and hence infinitely many primes. //

Let $p_1 = 2,\ p_2 = 3, \cdots,\ p_k$ = k-th largest prime in sequence. Then the smallest prime divisor of

$$(p_1 \cdots p_k)^{(p_1 \cdots p_k)^{(p_1 \cdots p_k)}} - 1$$ is p_{k+1}.

§1.6. Mathematical Induction — this is for you to review.

Chapter 2. Groups.

§2.1. Definitions and Examples.

We saw in our discussion of mappings that the set of bijective self-maps satisfy four important properties. We now make this notion abstract by considering a set G equipped with a binary operation $*$.

What is a binary operation? Formally speaking, a binary operation is a mapping $\psi : G \times G \to G$ that uniquely assigns one element of G to each ordered pair of elements of G.

It is convenient to write $a * b$ in place of $\psi(a, b)$.

Definition. A non-empty set G, equipped with a binary operation $*$, is called a **group** when the following hold:

(G0) for all $a, b \in G$, one has $a * b \in G$ (Closure) [part of definition of binary operation]

(G1) for all $a, b, c \in G$, one has $a * (b * c) = (a * b) * c$ (Associative Law)

(G2) there exists $e \in G$ such that, for all $a \in G$, one has $a * e = e * a = a$ (Identity exists)

(G3) for all $a \in G$, there exists $b \in G$ such that $a * b = b * a = e$ (Inverses exist)

[Usually write this element b as a^{-1}].

Examples (see also the book by Herstein).

(1) The group $(A(S), \circ)$ of {bijective self-mappings} of a non-empty set S, together with the binary operation of composition.

(G0) ✓ closure, (G1) ✓ assoc., (G2) id_S is identity ✓, (G3) inverse mappings exist as a consequence of bijectivity.

---

(2) The group $(\mathbb{Z}, +)$ of integers with the binary operation of addition.

(G0) ✓ closure (G1) ✓ assoc. (G2) 0 is identity ✓; $n+0=0+n=n$, all $n \in \mathbb{Z}$ (G3) $-n$ is inverse of n for all $n \in \mathbb{Z}$. ✓

Similarly, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ forms groups.

---

(3) The group $(\mathbb{Z}_n, +)$ of integers (mod n) with the binary operation of addition.

Here, as usual, we take $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, and when $a, b \in \mathbb{Z}_n$, we define $+ \pmod n$ by

$$a + b = \begin{cases} a+b & \text{when } 0 \le a+b < n \text{ as an ordinary integer} \\ a+b-n & \text{when } n \le a+b < 2n \text{ as an ordinary integer.} \end{cases}$$

(G0) ✓ closure (G1) ✓ assoc. (G2) 0 is identity ✓ (G3) $n-a$ is inverse of a for $1 \le a < n$, and 0 is inverse of 0.

---

(4) The group $(\mathbb{R}^\times, \times)$ of non-zero real numbers with the binary operation of multiplication.

(G0) ✓ closure $a, b \in \mathbb{R}^\times \Rightarrow a \times b \in \mathbb{R}$ and $a \times b \neq 0$.

(G1) associativity ✓

(G2) 1 forms identity ✓ (G3) when $a \in \mathbb{R}^\times$, $\frac{1}{a} \in \mathbb{R}^\times$ is inverse.

(5) The group $(SL_2(\mathbb{R}), *)$ of 2×2 matrices in real numbers having determinant 1, with the binary operation of matrix multiplication.

(G0) $M_1, M_2 \in SL_2(\mathbb{R}) \Rightarrow \det(M_1 * M_2) = \det(M_1 M_2)$
$= \det(M_1)\det(M_2) = 1$,

$\therefore M_1 * M_2 \in SL_2(\mathbb{R})$ ✓

(G1) Assoc. ✓ $\quad (M_1 M_2) M_3 = M_1 (M_2 M_3)$

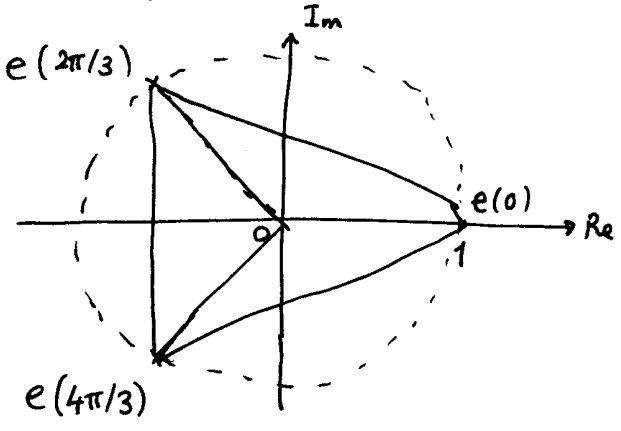
(G2) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{R})$ is identity

(G3) If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$, then $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in SL_2(\mathbb{R})$ acts as inverse, since $ad - bc = 1$.

---

(6) The group $(D_{2n}, *)$ of symmetries of a regular n-sided polygon under composition.

One way to describe the set D_{2n} is as the set of vertices of a regular n-sided polygon in the complex plane:



$e(z) := e^{2\pi i z}$

$e^{2\pi i a/n} = \cos\left(\frac{2\pi a}{n}\right) + i \sin\left(\frac{2\pi a}{n}\right)$

$(0 \le a < n)$.

Two symmetries (mappings) to consider:

$\sigma: e^{2\pi i a/n} \longmapsto e^{2\pi i (a+1)/n}$

(multiply by $e^{2\pi i/n}$)

$\tau: e^{2\pi i a/n} \longmapsto e^{-2\pi i a/n}$

(conjugation).

Then consider all mappings obtained by composing sequences of mapping.

(G0) Closure ✓ (check)

(G1) Assoc. ✓

(G2) Identity: $id = \sigma^n$ = multiply by 1

(G3) Inverse: $\sigma^{-1}: e^{2\pi i a/n} \longmapsto e^{2\pi i (a-1)/n}$
(multiply by $e^{-2\pi i/n}$)

$\tau^{-1}: e^{2\pi i a/n} \to e^{-2\pi i a/n}$.

It turns out that this does form a group having $2n$ elements given by

$$1, \sigma, \sigma^2, \dots, \sigma^{n-1}, \quad \tau, \tau\sigma, \tau\sigma^2, \dots, \tau\sigma^{n-1},$$

where $\sigma\tau = \tau\sigma^{-1}$

[Note $\sigma\tau\left(e^{2\pi i a/n}\right) = \sigma\left(e^{-2\pi i a/n}\right) = e^{2\pi i(1-a)/n}$

$\tau\sigma^{-1}\left(e^{2\pi i a/n}\right) = \tau\left(e^{2\pi i(a-1)/n}\right) = e^{-2\pi(a-1)/n}$ for all a]

Definition A group $(G, *)$ is said to be a finite group when $\text{card}(G) < \infty$, in which case we say that the order of G is (equal to) $|G| = \text{card}(G)$.

---

(1) $|A(S)| = n!$ when $|S| = n$

(2) $|\mathbb{Z}| = +\infty$ (not finite order)

(3) $|\mathbb{Z}_n| = n$

(4) $|\mathbb{R}^\times| = +\infty$

(5) $|SL_2(\mathbb{R})| = +\infty$.

Harder — one can consider $SL_2(\mathbb{Z}_p)$ for prime numbers p, where $\mathbb{Z}_p$ denotes the set of integers modulo p. It transpires that $|SL_2(\mathbb{Z}_p)| = (p-1)p(p+1)$.

(6) $|D_{2n}| = 2n$.

An important simplifying property holds for certain groups.

Definition. A group $(G, *)$ is said to be abelian when, for all $a, b \in G$, one has $a * b = b * a$.

---

(1) In general, $A(S)$ is not abelian. (We'll come back to this)

(2) $\mathbb{Z}$ abelian, (3) $\mathbb{Z}_n$ abelian, (4) $\mathbb{R}^\times$ abelian,

(5) $SL_2(\mathbb{R})$ is not abelian. To see this, note that

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

(6) In general the group D_{2n} is not abelian. To see this, note that when $n \geq 3$ one has

$$\sigma\tau = \tau\sigma^{-1} \neq \tau\sigma \qquad (\text{since } \sigma \neq \sigma^{-1}).$$

Examples of non-groups:

(1) The set $\mathbb{Z}$ of integers with the binary operation of multiplication.

(G0) ✓ domain (G1) ✓ Assoc. (G2) 1 is identity ✓ (G3) inverses: 0, 2 has no inverse in $\mathbb{Z}$.

- Also, the set $\mathbb{Z}^*$ of integers that are non-zero, with $\times$.

---

(2) The set $\mathbb{Z}_6$ of integers modulo 6 with binary operation of multiplication modulo 6.

(G0) ✓ domain (G1) · ✓ Assoc. (G2) 1 is ~~identity~~ ✓ (G3) 2, 3 do not have inverses modulo 6.

---

§2.2. The most basic properties.

The first remark, which we have already applied, is that it may be convenient to replace the binary operation $*$ by

$+$ (additive notation)

$\times$ (multiplicative notation $a \times b$, or even ab).

Lemma 2.2.1: Suppose that G is a group. Then:

(a) the identity element $e \in G$ is unique;

(b) for every $a \in G$, the inverse element $a^{-1} \in G$ is unique;

(c) for all $a \in G$ one has $(a^{-1})^{-1} = a$;

(d) for all $a, b \in G$ one has $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: (a) Suppose e_1 and e_2 are two identity elements in G. Then $e_1 e_2 = e_2$ and $e_1 e_2 = e_1$ (using identity properties), so $e_1 = e_2$ and the identity is unique. □

(b) Suppose b_1 and b_2 are both inverses for a. Then if e is the identity, we have

$$b_1 = b_1 e = b_1 (a b_2) = (b_1 a) b_2 = e b_2 = b_2,$$

so the inverse for a is unique, for each a. □

(c) If a^{-1} is the inverse for a, then $a^{-1}a = e = a a^{-1}$, whence a acts as the inverse for a^{-1}, that is, $a = (a^{-1})^{-1}$. □

(d) Let $c = (ab)^{-1}$. Then $(ab)c = e$. Thus

$$a^{-1}((ab)c) = a^{-1}e = a^{-1}$$

$$\Rightarrow \quad (a^{-1}a)(bc) = a^{-1}$$

$$\| \qquad\qquad \|$$

$$e(bc) = bc$$

$$\Rightarrow \quad b^{-1}(bc) = b^{-1}a^{-1}$$

$$\| \qquad\qquad \|$$

$$(b^{-1}b)c = ec = c.$$

So $(ab)^{-1} = b^{-1}a^{-1}$, for all $a, b \in G$. //

Lemma 2.2.2 (cancellation rule) Suppose that G is a group and $a, b, c \in G$. Then:

(a) whenever $ab = ac$, one has $b = c$.

(b) whenever $ba = ca$, then $b = c$.

Proof. (a) Since $ab = ac$, we have

$$a^{-1}(ab) = a^{-1}(ac)$$

$$\| \qquad\qquad \|$$

$$b = eb = (a^{-1}a)b \qquad (a^{-1}a)c = ec = c,$$

so $b = c$. □

(b) Likewise, since $ba = ca$, we have

$$(ba)a^{-1} = (ca)a^{-1}$$

and the proof proceeds similarly. □ //

Note that in a group G, if b is a left-inverse for $a \in G$, then b is also a right-inverse for $a \in G$, and hence the inverse.

For if $ba = e$, then $(ba)b = eb = b$, i.e. $b(ab) = b$,

whence $b^{-1}(b(ab)) = b^{-1}b = e$, so $ab = e$.
$(b^{-1}b)(ab) = e(ab) = ab$

---

§2.3. Subgroups. The property of being a group is a special property with useful features. If G is a group of large order, it might be useful to identify a subset of G, much smaller in order, which also has these useful features.

Definition Suppose that H is a non-empty subset of a group G equipped with a binary operation. If H forms a group with respect to the same binary operation, then we call H a subgroup of G, and write $H \leq G$.

Remark: If G is a group having identity element e, then $\{e\} \leq G$ and $G \leq G$. These are called trivial subgroups, all other subgroups (if any) being called proper subgroups.

Lemma 2.3.1 (Subgroup criterion) Suppose that G is a group, and $\emptyset \neq H \subseteq G$. Then $H \leq G$ if and only if, for all $a, b \in H$ one has $ab^{-1} \in H$.

Proof. ($\Rightarrow$) If $H \leq G$ then for all $b \in H$ one has $b^{-1} \in H$, and so by the closure axiom, for all $a, b \in H$ one has $ab^{-1} \in H$. $\square$

($\Leftarrow$) Let $a \in H$ with $\emptyset \neq H \subseteq G$. We are permitted to assume that, for all $b \in H$, one has $ab^{-1} \in H$. Thus, in particular $\underbrace{aa^{-1}}_{e} \in H$, so $e \in H$. Also, in particular, since $e \in H$ we have $\underbrace{ea^{-1}}_{a^{-1}} \in H$, so $a^{-1} \in H$.

This confirms axioms (G2) and (G3) for H. The associative axiom (G1) is inherited from G. As for closure, we see that whenever $a, b \in H$, then $a, b^{-1} \in H$, whence $a(b^{-1})^{-1} \in H$, so that ab H satisfies (G0). Thus H is a subgroup of G. □ //

Lemma 2.3.2. Suppose G is a group and $\emptyset \neq H \subseteq G$. Suppose also that H is of finite cardinality and is closed under the group product of G. Then $H \leq G$.

Proof: Suppose $a \in H$. Then each of the elements a, $a \cdot a = a^2$, $a^3, \ldots$ lie in H. But H is finite, so there exist $n, m \in \mathbb{N}$ with $m < n$ such that $a^n = a^m$, whence $a^{n-m} = e$. Thus $a^{-1} = a^{n-m-1} \in H$, and by the closure property of H, whenever $a, b \in H$ one has $ab^{-1} \in H$. Then the conclusion follows from Lemma 2.3.1. //

Examples – special and general

(1) Let $n \in \mathbb{N}$ (think of $n \geq 2$), and consider $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$ as a subset of $\mathbb{Z}$ under ordinary addition. We claim that $n\mathbb{Z} \leq \mathbb{Z}$. Here, whenever $a, b \in n\mathbb{Z}$, we have $n \mid a$ and $n \mid b$, whence $n \mid (a-b)$, so $a - b \in n\mathbb{Z}$. The desired conclusion therefore follows from Lemma 2.3.1.

---

(2) Let $(\mathbb{C}^\times, \cdot)$ be the group of non-zero complex numbers under multiplication.

- Then if $T = \{z \in \mathbb{C} : |z| = 1\}$, then T forms a subgroup of $\mathbb{C}^\times$.
- Also, $\mu_n = \{e^{2\pi i a/n} : 0 \leq a < n, a \in \mathbb{N}\}$ forms a subgroup of T, and also of $\mathbb{C}^\times$.

(3) Let $(G, \cdot)$ be a group, and let $a \in G$ be any element of G. Then $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$ forms a subgroup of G.

Proof: For all $a^i, a^j \in \langle a \rangle$, one has $a^i (a^j)^{-1} = a^{i-j} \in \langle a \rangle$, so conclusion follows from Lemma 2.3.1. //

Definition A group G generated by a single element a, so that

$$G = \langle a \rangle = \{ a^n : n \in \mathbb{Z} \}$$

is called cyclic.

We shall see later that cyclic groups are morally the same as either $(\mathbb{Z}, +)$, or $(\mathbb{Z}_n, +)$ for some $n \in \mathbb{N}$.

---

(4) We have $\langle 2 \rangle \leq \mathbb{Z}_6$ and $\langle 3 \rangle \leq \mathbb{Z}_6$ with respect to $+$.

$\langle 2 \rangle = \{0, 2, 4\}$ $\quad$ $\langle 3 \rangle = \{0, 3\}$

---

(5) Centralizer When $a \in G$, define

$$C(a) = \{ g \in G : ga = ag \} \quad \text{(Centralizer of } a\text{)}.$$

Theorem: For each $a \in G$, one has $C(a) \leq G$.

Proof: Observe first that whenever $h \in C(a)$, then

$$ha = ah \rightarrow hah^{-1} = a \Rightarrow h^{-1}h = ah^{-1},$$

so $h^{-1} \in C(a)$. Thus, whenever $g, h \in C(a)$ one has

$$(ag)h^{-1} = (ga)h^{-1} = (gh^{-1})a,$$

so $gh^{-1} \in C(a)$. Thus $C(a) \leq G$ as a consequence of the subgroup criterion. //

(6) Center $Z(G) := \{ z \in G : zx = xz \text{ for all } x \in G \}$.

↑ zentrum — commutes with every element

Proof. Observe that

$$Z(G) = \bigcap_{a \in G} C(a).$$

But if K and H are two subgroups of G, then $K \cap H$ is also

a subgroup of G. For K has the property that whenever $g, h \in K$, then $gh^{-1} \in K$, and likewise with H in place of K. Thus, if $g, h \in K \cap H$, then $gh^{-1} \in K \cap H$, whence $K \cap H \leq G$. But $C(a) \leq G$ for each $a \in G$, so $\bigcap_{a \in G} C(a) \leq G$. //

Similar argument works for finite or infinite intersection.

(7) Conjugate subgroups. Suppose $H \leq G$. Then for each $g \in G$, the subset

$$g^{-1} H g = \{ g^{-1} h g : h \in H \}$$

is a subgroup of G (a conjugate subgroup).

Proof: Whenever $h_1, h_2 \in H$, one has $h_1 h_2 \in H$. But then

$$(g^{-1} h_1 g)(g^{-1} h_2 g)^{-1} = (g^{-1} h_1 g)(g^{-1} h_2^{-1} g) = g^{-1} h_1 h_2^{-1} g \in g^{-1} H g.$$

Thus, whenever $a, b \in g^{-1} H g$, one has $ab^{-1} \in g^{-1} H g$, so $g^{-1} H g \leq G$. //

(8) Normalizer When $A \subseteq G$, define

$$N(A) = \{ g \in G : gA = Ag \} = \{ g \in G : g^{-1} A g = A \}$$

to be the normalizer of A. One has $N(A) \leq G$ (exercise). For if $g, h \in N(A)$, then $g, h^{-1} \in N(A)$, whence

$$(gh^{-1})^{-1} A (gh^{-1}) = h(g^{-1} A g) h^{-1} = hAh^{-1} = (h^{-1})^{-1} A h^{-1} = A.$$

Thus $gh^{-1} \in N(A)$, so $N(A) \leq G$. //

§2.4 Lagrange's Theorem. Orders of subgroups H of groups G.

When G is a finite group and $H \leq G$, we consider the subsets gH of G, where $g \in G$. It transpires that these subsets partition G into subsets (disjoint) containing equal numbers of elements. The consequence will be that $|H| \mid |G|$.

In order to justify this conclusion, it is useful to introduce the concept of an equivalence relation.

Definition. A relation R on a set S is a statement concerning a pair of elements $a, b \in S$ of the shape aRb, which may be true or false. We write aRb to indicate the truth of the statement.

For example, on the set $\mathbb{Z}$ the relations $=$, $<$, $\geq$ are all relations.

Definition. An equivalence relation $\sim$ on a set S is a relation satisfying:

(a) $a \sim a$ for all $a \in S$ (reflexivity)

(b) $a \sim b$ implies $b \sim a$ (symmetry)

(c) $a \sim b$ and $b \sim c$ implies $a \sim c$ (transitivity).

Examples: (1) Any set S and ordinary equality "$=$".

(2) The set $\mathbb{Z}$ and "congruence modulo n".

$a \equiv a \pmod n$ (reflexive) since $n \mid (a-a)$ for all $a \in \mathbb{Z}$.

$a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$ (symmetry)

since $n \mid (a-b) \Rightarrow n \mid (b-a)$

$a \equiv b \pmod n$ & $b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$

(transitive)

since $n \mid (a-b)$ & $n \mid (b-c) \Rightarrow n \mid (a-b+b-c)$.

(3) Let G be a group and suppose $H \leq G$.

When $a, b \in G$, define $a \sim b$ when $ab^{-1} \in H$ ("congruence modulo H").

We claim that $\sim$ defines an equivalence relation on G.

Let us check:

(reflexive): We have $a \sim a$ if and only if $aa^{-1} \in H$, which is guaranteed since $e \in H$. ✓

(symmetry): We have $a \sim b$ if and only if $ab^{-1} \in H$

$\Leftrightarrow (ab^{-1})^{-1} \in H$

$\Leftrightarrow ba^{-1}$

$\Leftrightarrow b \sim a$. ✓

(transitivity): We have $a \sim b$ and $b \sim c$ if and only if $ab^{-1} \in H$ & $bc^{-1} \in H$

$\Leftrightarrow (ab^{-1})(bc^{-1}) \in H$

$\Leftrightarrow ac^{-1}$

$a \sim c$. ✓

So this relation $\sim$ does indeed form an equivalence relation on G.

Definition: The equivalence class $[a]$ of elements in a set S equipped with an equivalence relation $\sim$ is given by

$$[a] = \{ b \in S : b \sim a \}.$$

Theorem 2.4.1. Suppose that $\sim$ is an equivalence relation on a set S. Then $\sim$ partitions S into equivalence classes. Thus

$$S = \bigcup_{a} [a],$$

where the union is over representatives of each distinct equivalence class of S.

[Note: if $[a]$ and $[b]$ are two equivalence classes of S, then either $[a] = [b]$ or $[a] \cap [b] = \emptyset$].

For if $c \in [a] \cap [b]$, then $a \sim c$ and $c \sim b$, whence $a \sim b$. But then $d \in [a]$ if and only if $d \in [b]$, so $[a] = [b]$.

Proof of Theorem 2.4.1: Since $a \in [a]$ for all $a \in S$, have $S = \bigcup_{a \in S} \{a\} \subseteq \bigcup_{a \in S} [a]$.

But $[a] \subseteq S$, so $\bigcup_{a \in S} [a] \subseteq S$, and thus $S = \bigcup_{a \in S} [a]$. But as we have noted, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$, and thus S is the union over representatives of each distinct equivalence class. //

Let us return to the equivalence relation $\sim$ on a group G with subgroup H defined by $a \sim b$ whence $ab^{-1} \in H$.

(Right coset) We have $[a] = \{ b \in G : ba^{-1} = h \text{ for some } h \in H \}$

$= \{ b \in G : b = ha \text{ for some } h \in H \}$

$= Ha$ (the right coset of H given by a).

So $G = \bigcup_{\substack{a \in G \\ \text{representatives}}} Ha$.

Moreover, each of these right cosets contains the same number of elements. To confirm this property, we construct a bijective mapping

$$\psi : H \to Ha$$
$$h \mapsto ha$$

Injective: $\psi(h_1) = \psi(h_2) \Leftrightarrow h_1 a = h_2 a \Leftrightarrow h_1 = h_2$. ✓

Surjective: If $g \in Ha$, then $g = ha$ for some $h \in H$, whence $g = \psi(h)$ ✓

Thus $|Ha| = |H|$ (note that $H = He$) for all $a \in G$.

Theorem 2.4.2. (Lagrange's Theorem). Suppose that G is a finite group and $H \leq G$. Then the order of H divides the order of G.

Proof. We apply the equivalence relation defined via right cosets, so $a \sim b$ if and only if $ab^{-1} \in H$.

Let the number of distinct equivalence classes be k, so that

for some $a_1, \dots, a_k \in G$ one has the partition

$$G = \bigcup_{\ell=1}^{k} [a_\ell] = \bigcup_{\ell=1}^{k} Ha_\ell, \quad \text{with } Ha_\ell \cap Ha_m = \phi \text{ when } \ell \neq m.$$

But $|Ha_\ell| = |H|$ for every ℓ, so

$$|G| = \sum_{\ell=1}^{k} |Ha_\ell| = k|H|.$$

In particular, one has $|H| \mid |G|$. //

Corollary [Theorem 2.4.3]. A group G having prime order is cyclic.

Proof. Suppose $|G| = p$ with p a prime number. If $H \leq G$, then $|H| \mid p$, so $|H| = 1$ or p, whence $H = \{e\}$ or G. So G has no proper subgroups. But if $a \in G$ and $a \neq e$, then $\langle a \rangle \leq G$, so since $\langle a \rangle \neq \{e\}$ one has $\langle a \rangle = G$. Thus G is cyclic. //

Consequence: any group of prime order is abelian

Definition. Let G be a group. The smallest positive integer m such that $a^m = e$, if one exists, is called the order of a, written $o(a)$. If no such integer exists, then a has infinite order.

Theorem 2.4.4 Suppose that G is finite. Then whenever $a \in G$, one has $o(a) \mid |G|$.

Proof. If $a \in G$, then $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$, for some integer n with $a^n = e$, and we can assume that these elements are distinct. Then $\langle a \rangle \leq G$ with $|\langle a \rangle| = n$. But then Lagrange's Theorem shows that $|\langle a \rangle| \mid |G|$, whence $n \mid |G|$.

However, it is apparent that $n = o(a)$. //

Corollary (Theorem 2.4.5) Suppose that G is a finite group of order n. Then $a^n = e$ for all $a \in G$.

Proof. Let $a \in G$ and $m = o(a)$. Then $m \mid |G|$, so that

$$a^{|G|} = a^{ml}, \quad \text{where } l = |G|/m$$
$$= (a^m)^l = e^l = e. \; //$$

Elementary Number Theory again:

We have seen that $(\mathbb{Z}_n, +)$ forms the group of residues modulo n under addition. Thus we consider the equivalence classes of integers

$$[0], [1], \ldots, [n-1]$$

of integers under equivalence $a \equiv b \pmod{n} \hookrightarrow a \sim b$, with $[a] + [b] := [a+b]$. Note: $\mathbb{Z}_n = \langle [1] \rangle$ is cyclic.

We can also consider multiplication modulo n

$$[a] \times [b] = [a \times b].$$

Here, $(\mathbb{Z}_n, \times)$ does not in general form a group, on recalling $[2]$ does not have an inverse modulo 6. (i.e. in $\mathbb{Z}_6$).

Define $U_n = \{ [a] : (a, n) = 1 \}$, where $[a]$ denotes the equivalence class of integers a modulo n.

Claim: U_n forms a group with multiplication modulo n.

Check: • $(a,n) = 1 = (b,n) \Rightarrow (ab,n) = 1$, so if $[a], [b] \in U_n$ then $[ab] \in U_n$. ✓

• $[1] \in U_n$ is identity. ✓

• Associativity inherited from $\mathbb{Z}$. ✓

• if $(a,n) = 1$, then there exists $b \in \mathbb{Z}$ with $(b,n) = 1$ such that $ab \equiv 1 \pmod{n}$. To see this, note that there exist integers b and c such that $ab + nc = 1 \Rightarrow ab \equiv 1 \pmod{n}$. Thus if $[a] \in U_n$, there exists $[b] \in U_n$ such that $[ab] = [1]$. ✓

Definition The Euler φ-function is defined for each integer $n \in \mathbb{N}$ by

$$\varphi(n) = \text{card}\{1 \le a \le n : (a,n) = 1\}.$$

Thus $\varphi(n) = |U_n|$, and so it follows from Theorem 2.4.5 that:

Theorem 2.4.8. (Euler) Whenever $a \in \mathbb{Z}$ and $(a,n) = 1$, one has $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. U_n forms a group with multiplication modulo n, and $[a] \in U_n$, whence $[a]^{|U_n|} = [1]$, or equivalently,

$$[a]^{\varphi(n)} = [1] \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}. \;//$$

Corollary. (Fermat's Little Theorem). When p is a prime number and $p \nmid a$, one has $a^{p-1} \equiv 1 \pmod{p}$.

Moreover, for all integers b one has $b^p \equiv b \pmod{p}$. //

Proof. One has $\varphi(p) = \text{card}\{1 \le a \le p : (a,p)=1\} = p-1$. Thus $(a,p)=1$ implies $a^{p-1} \equiv 1 \pmod p$ and also $a^p \equiv a \pmod p$. When $(b,p)>1$ one has $p \mid b$, whence $b^p \equiv b \pmod p$. Then in either case $b^p \equiv b \pmod p$. //

Exercise: Show that $U_n^{(d)} := \{a^d : a \in U_n\}$ forms a subgroup of U_n, for each $d \in \mathbb{N}$.

Fact: Every finite abelian group is isomorphic to some group of the shape $U_n^{(d)}$, for suitable $n, d \in \mathbb{N}$. (subject of next section!)

---

§2.5. Homomorphisms and normal subgroups.

Definition. Let G and G' be two groups. The mapping

$$\varphi : G \longrightarrow G'$$

is called a homomorphism when for all $a, b \in G$, one has $\varphi(ab) = \varphi(a)\varphi(b)$

Notice: the idea is that the binary operation in G is respected by the homomorphism φ in the image group (and its own binary operation).

Special kinds of homomorphisms:

- injective : called monomorphisms
- surjective : called epimorphisms
- bijective : called isomorphisms
- isomorphism of G onto itself is called an automorphism.

Examples: (1) Trivial homomorphism $\varphi : G \to G'$, $g \mapsto e'$, identity of G'.

Have $e' = \varphi(gh) = \varphi(g)\varphi(h) = e'\cdot e' = e'$.

(2) Consider $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ (with addition).
$a \longmapsto a \pmod n$

Then $\varphi(a+b) = (a+b)_{\bmod n} = (a)_{\bmod n} + (b)_{\bmod n} = \varphi(a) + \varphi(b)$.

(3) Another kind of trivial homomorphism

$\varphi : G \longrightarrow G$ (identity mapping).
$g \longmapsto g$

(4) $\varphi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Q}^*, \times)$
$n \longmapsto 2^n$

$\varphi(a+b) = 2^{-(a+b)} = 2^{-a} \cdot 2^{-b} = \varphi(a)\varphi(b)$.

(5) $\varphi : (\mathbb{Q}^\times, \cdot) \longrightarrow (\mathbb{Q}^\times, \cdot)$
$x \longmapsto x^2$

$\varphi(xy) = (xy)^2 = x^2 \cdot y^2 = \varphi(x)\varphi(y)$

Definition. We say that two groups G and G' are isomorphic if there exists an isomorphism of G onto G'. In such circumstances, we write $G \cong G'$.

Theorem 2.5.1 (Cayley's Theorem) Every group G is isomorphic to a subgroup of $A(S)$, for some set S.

Corollary. When G is a finite group, then G is isomorphic to a subgroup of S_n, where $n = |G|$.

Proof. Let G be a group, and take $S = G$. We define the set $A(G)$ of bijective self-mappings of G onto G.

- Observe that whenever $a \in G$, then the map

$T_a : G \longrightarrow G$
$g \longmapsto ag$

belongs to $A(G)$. To confirm this, note that T_a has inverse

mapping $T_a^{-1} = T_{a^{-1}}$, so is bijective.

Observe next that the set $H = \{T_a : a \in G\}$ is a subgroup of $A(G)$. For whenever $T_a, T_b \in H$, one has

$$T_a \circ T_b^{-1} = T_a \circ T_{b^{-1}} = T_{ab^{-1}} \in H.$$

[Note here that when $a, b \in G$, then for all $g \in G$ one has $T_a \circ T_b(g) = T_a(bg) = abg = T_{ab}(g)$., so $T_a \circ T_b = T_{ab}$].

Finally, we show that $G \cong H$. To see this, consider the map

$$\varphi : G \longrightarrow H$$
$$a \longmapsto T_a .$$

This defines a homomorphism, since for all $a, b \in G$ one has

$$\varphi(ab) = T_{ab} = T_a \circ T_b = \varphi(a) \circ \varphi(b).$$

Injective: $\varphi(a) = \varphi(b) \Leftrightarrow T_a = T_b \Leftrightarrow$ for all $g \in G$, $T_a g = T_g b$ (i.e. $ag = bg$)

$\Leftrightarrow a = b$. ✓

Surjective: whenever $T_a \in H$, one has $\varphi(a) = T_a$. ✓

Then φ is an isomorphism of G onto H, and $H \leq A(G)$. So G is indeed isomorphic to a subgroup of $A(S)$ for some set S. //

When G is finite, the above argument shows that $G \cong H$ for some $H \leq A(G)$. If $|G| = n$, then $A(G)$ is the group of permutations on n elements, and we have called this S_n. But we shall discuss this further in due course.

So — up to relabelling of elements of G and relabelling its binary operation — every finite group is morally "the same" as a subgroup of S_n for some $n \in \mathbb{N}$.

Lemma (2.5.2 + 2.5.3) If $\varphi: G \to G'$ is a homomorphism of groups, then $\varphi(G) \leq G'$.

↑ "image of G".

Proof. We first show that $\varphi(e)$ is the identity, say e', of G'. For we have $\varphi(x) = \varphi(xe) = \varphi(x)\varphi(e)$, whence $\varphi(e) = e'$ by cancellation. Hence, also, for all $a \in G$ we have $e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$, whence $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Finally, whenever $a, b \in G$, we have

$$\varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi(G),$$

whence, for all $g, h \in \varphi(G)$, we have $gh^{-1} \in \varphi(G)$. So $\varphi(G) \leq G'$ by the subgroup criterion. //

A special case of this conclusion has particular significance.

Definition. If $\varphi: G \to G'$ is a homomorphism of groups, then the kernel of φ is defined by $\ker(\varphi) = \{a \in G : \varphi(a) = e'\}$.

Measures how close φ is to being an (injective) monomorphism: if φ is a monomorphism, then $\ker(\varphi) = \{e'\}$.

Exercise: Show that whenever $g' \in G'$ and $\varphi: G \to G'$ is a homomorphism, then whenever $\varphi(h) = g'$ one has

$$\varphi^{-1}(g') = (\ker\varphi)h.$$

$$\| \quad \{g \in G : \varphi(g) = g'\}$$

Hint: If $g_1, g_2 \in G$ both satisfy $\varphi(g_1) = g' = \varphi(g_2)$, then what can you say about $\varphi(g_1 g_2^{-1})$?

Properties of $\ker(\varphi)$:

Theorem 2.5.5. If $\varphi: G \to G'$ is a homomorphism of groups, then:

(a) $\ker(\varphi) \leq G$;

(b) For all $g \in G$, one has $g^{-1}(\ker(\varphi))g \subseteq \ker(\varphi)$.

Proof: (a) Suppose that $a, b \in \ker(\varphi)$. Then

$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e' \cdot (e')^{-1} = e'$, so $ab^{-1} \in \ker(\varphi)$. Then $\ker(\varphi) \leq G$, by the subgroup criterion. □

(b) Whenever $k \in \ker(\varphi)$, then for all $g \in G$ one has

$\varphi(g^{-1}kg) = \varphi(g)^{-1}\varphi(k)\varphi(g) = \varphi(g)^{-1}e'\varphi(g) = \varphi(g)^{-1}\varphi(g) = e'$,

whence $g^{-1}kg \in \ker(\varphi)$. Thus $g^{-1}(\ker\varphi)g \subseteq \ker\varphi$. □ //

Note: $\varphi: G \to G'$ is a monomorphism if and only if $\ker(\varphi)$ is trivial. By this we mean that $\ker(\varphi) = \{e^*\}$. Plainly, if $\ker(\varphi) \neq \{e^*\}$, then there exists $g \in \ker(\varphi) \setminus \{e^*\}$, and so φ cannot be a monomorphism. To see this note that $\varphi(g) = \varphi(e^*) = e'$ and $g \neq e$. So $\ker(\varphi)$ must be trivial if φ is a monomorphism. On the other hand, if $\ker(\varphi)$ is trivial, then whenever $\varphi(g_1) = \varphi(g_2)$, one has $g_1 = g_2$. If not, then if $\varphi(g_1) = \varphi(g_2)$ whilst $g_1 \neq g_2$, we have $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_1)^{-1} = e'$, so $g_1 g_2^{-1} = e$ whilst $g_1 \neq g_2$ ※.

Definition. Suppose that $N \leq G$. Then N is a normal subgroup of G when $g^{-1}Ng \subseteq N$ for all $g \in G$. We then write $N \lhd G$.

Thus $\ker(\varphi) \lhd G$ whenever $\varphi: G \to G'$ is a homomorphism of groups.

Note: If $g^{-1}Ng \subseteq N$, then $g^{-1}Ng = N$, for we have $N = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$. So if these relations hold for

all $g \in G$, then $g^{-1}Ng \subseteq N \subseteq gNg^{-1} \Rightarrow N = gNg^{-1}$.

Also, $gN = Ng$, so left and right cosets coincide for all $g \in G$.

Theorem 2.5.6. One has $N \lhd G$ if and only if $gN = Ng$ for all $g \in G$.

Examples. (a) Suppose G is an abelian group and $H \leq G$.

Then for all $g \in G$ and $h \in H$ one has $g^{-1}hg = g^{-1}gh = h$,

so $g^{-1}Hg = H$ for all $g \in G$. Thus $H \lhd G$. □

(b) Recall $Z(G) = \{z \in G : zx = xz \text{ for all } x \in G\}$.

Thus, for all $g \in Z(G)$, one has $g^{-1}Z(G)g = Z(G)$, so

$Z(G) \lhd G$. □

(c) Consider the group $G = D_{2n} = \langle \sigma, \tau : \sigma^n = \tau^2 = e, \sigma\tau = \tau\sigma^{-1} \rangle$

and $H = \langle \sigma \rangle = \{e, \sigma, \ldots, \sigma^{n-1}\}$.

Then each element of G has the shape σ^ℓ $(0 \leq \ell < n)$

or $\tau\sigma^\ell$ $(0 \leq \ell < n)$.

We have $\sigma^{-m}\sigma^\ell\sigma^m = \sigma^\ell \in H$

and $(\tau\sigma^m)^{-1}\sigma^\ell(\tau\sigma^m) = \sigma^{-m}\tau^{-1}(\sigma^\ell\tau)\sigma^m$

$= \sigma^{-m}\tau^{-1}(\tau\sigma^{-\ell})\sigma^m$

$= \sigma^{-m}\sigma^{-\ell}\sigma^m = \sigma^{-\ell} \in H$.

Thus $\sigma^{-m}H\sigma^m \subseteq H$ and $(\tau\sigma^m)^{-1}H(\tau\sigma^m) \subseteq H$, whence

$g^{-1}Hg \subseteq H$ for all $g \in G$. Then $H \lhd D_{2n}$. □

§2.6. Factor Groups = Quotient Groups

We attempt to extend the observation that from the groups $(\mathbb{Z}, +)$ and $(n\mathbb{Z}, +)$, we created the group $(\mathbb{Z}_n, +)$ of equivalence classes of integers modulo n.

Recall that when G is a group and $H \leq G$, then we can define an equivalence relation $\sim$: $a \sim b$ if and only if $ab^{-1} \in H$. One then has $[a] = Ha$. [since $b \sim a \Leftrightarrow ba^{-1} \in H \Leftrightarrow b \in Ha$].

Question: Is it possible that the set of equivalence classes Ha of G (the set of right cosets) also forms a group, with the group operation induced by that of G?

What this means is that the group operation on $\{Ha : a \in G\}$ should be defined in such a way that $Ha\, Hb = H(ab)$, where (ab) is defined in G via the group operation in G.

It transpires that this is possible — when H is a normal subgroup of G.

Theorem 2.6.1. Suppose that $N \lhd G$. Define

$$G/N = \{Na : a \in G\}.$$

Then G/N is a group relative to the operation $Na\, Nb = Nab$.

Proof. There are several properties to check here:

(1) The putative group operation is indeed a (well-defined) binary operation on G/N.

To check that this is true, the product of two cosets should not depend on the representatives of those cosets. Thus, if $Na = Na'$ and $Nb = Nb'$, one should have $Na\, Nb = Na'\, Nb'$.

But if $Na = Na'$, then $a' = n_1 a$ for some $n_1 \in N$, and similarly if $Nb = Nb'$, then $b' = n_2 b$ for some $n_2 \in N$.

Thus $a'b' = n_1 a n_2 b = n_1 (\underbrace{a n_2 a^{-1}}) ab$

$aNa^{-1} = N$, since $N \lhd G$.

Then $an_2a^{-1} = n_3 \in N$, say, whence $a'b' = n_1 n_3 ab \in Nab$.

Thus $(a'b')(ab)^{-1} \in N$, whence $Nab = Na'b'$. □

(2) Closure follows from definition of product. □

(3) When $Na, Nb, Nc \in G/N$, then

$$Na(Nb\ Nc) = Na\ Nbc = Na(bc) = N(ab)c = Nab\ Nc = (Na\ Nb)Nc,$$

by associativity in G. Thus G/N is associative. □

(4) $Ne = N \in G/N$ acts as the identity, since

$$Na\ Ne = Nae = Na = Nea = Ne\ Na. \quad \square$$

(5) $Na^{-1} \in G/N$ acts as the inverse of Na in G/N, since

$$Na\ Na^{-1} = Naa^{-1} = Ne = Na^{-1}a = Na^{-1}\ Na. \quad \square$$

So G/N does indeed have a group structure. //

"Factor group" or "quotient group" of G by N.

Theorem 2.6.2. Suppose that $N \triangleleft G$. Then there exists a surjective homomorphism $\psi : G \longrightarrow G/N$ such that $N = \ker(\psi)$.

Proof. We define the "canonical" mapping

$$\psi : G \longrightarrow G/N$$
$$a \longmapsto Na.$$

We have some properties to check:

- For all $a, b \in G$, we have $\psi(ab) = Nab = Na\ Nb = \psi(a)\psi(b)$, so ψ is a homomorphism.
- Since any $Na \in G/N$ satisfies $Na = \psi(a)$ with $a \in G$, one sees that ψ is surjective.
- We have
  $\ker(\psi) = \{a \in G : \psi(a) = Ne = N\}$
  But $Na = N$ if and only if $a \in N$, so $\ker(\psi) = N$.

Thus we have confirmed all the claims of the theorem. //

This result shows that G/N is some kind of "shadow" of G in which many features of the structure of G might be preserved. But is G/N any simpler?

Definition. If G is a (finite) group and $H \leq G$, the number of right cosets of H in G is called the index of H in G, and written $i_G(H)$ or $[G:H]$. ← More common.

Theorem 2.6.3. When G is a finite group and $N \lhd G$, one has $|G/N| = |G|/|N|$.

Proof. We have that $|G/N|$ is equal to the number of right cosets of N in G, namely $[G:N]$. But the proof of Lagrange's theorem shows that $[G:N] = |G|/|N|$. /

Corollary. Suppose that G is a finite group of order p. Then if p is prime, G has no non-trivial normal subgroups.

A group G having no non-trivial normal subgroups is called simple.

So $(\mathbb{Z}_p, +)$ is simple for p prime.

Theorem 2.6.4 (Cauchy's theorem for abelian groups). Suppose that G is a finite abelian group of order $|G|$ and $p \mid |G|$ with p prime. Then G has an element of order p.

We have seen already that if $H \leq G$, then $|H|$ divides $|G|$. One could ask for a converse statement, to the effect that when $d \mid |G|$ there should be a subgroup of order d. Cauchy's Theorem gives a partial converse, valid when d is a prime number, for if $o(a) = p$,

then $|\langle a\rangle| = p$. So far this is only for abelian groups, but later...!

Proof. We proceed by induction on $n = |G|$. The conclusion is trivial when $n = 1$. We suppose then that $n > 1$, and that the desired conclusion holds whenever $1 \leq |G| < n$. We now consider an abelian group G with $|G| = n$.

If G has no non-trivial subgroup, then it must be cyclic of prime order. For by §2·3, Q14, such a group G is necessarily cyclic, say $G = \langle a\rangle$. One then sees that if n is not prime, say $n = md$ with $1 < d < n$, then $\langle a^d\rangle$ is a proper subgroup of G. #. This contradiction confirms that $|G| = n$ is prime, and then $G = \langle a\rangle$ is cyclic of prime order p and $o(a) = p$. We may therefore suppose henceforth that G has a proper subgroup N with $1 < |N| < |G|$.

Since $|N| < n$, our inductive hypothesis ensures that if p is a prime with $p \mid |N|$, then N (and hence also G) has an element of prime order. We may therefore confine our attention to the situation in which $p \nmid |N|$.

Note next that since G is abelian, one has $N \trianglelefteq G$. Also, since $p \nmid |N|$ and $p \mid |G|$, and $|G| = |N| \cdot |G/N|$, one must have $p \mid |G/N|$. But $|N| > 1$ so $|G/N| = |G|/|N| < |G|$, and hence our inductive hypothesis shows that G/N contains an element of order p, say $Na \in G/N$. Notice here that we used the fact that G/N is abelian: if $a, b \in G$ then $Na\,Nb = Nab = Nba = Nb\,Na$. ✓.

What does it mean for Na to have order p in G/N? Suppose a has order m in G. Then $(Na)^m = Na^m = Ne = N$, so Na must have order dividing m. Thus $p \mid m$, say $m = kp$. But now it follows that a^k has order $\frac{m}{k} = p$ in G. We are therefore

forced to conclude even in this case that G has an element of order p. This completes the proof that when $|G| = n$, then it has an element of order p. The conclusion of the theorem therefore follows by induction. //

§2.7. The homomorphism theorems.

We saw in Theorem 2.6.2 that when $N \triangleleft G$, there exists a surjective homomorphism $\psi : G \to G/N$ with $N = \ker(\psi)$. We begin by extending this conclusion.

Theorem 2.7.1 (First Homomorphism Theorem). Let $\varphi : G \to G'$ be a surjective homomorphism of groups with kernel K. Then $G' \cong G/K$.

The isomorphism here is defined by $\psi : G/K \to G'$
$Ka \mapsto \varphi(a)$.

Proof. Define the map ψ as in the statement for $a \in G$. If this is to provide an isomorphism, as claimed in the theorem, then we have some properties to check:

- (Well-defined) We must show that if $Ka = Kb$ then $\psi(Ka) = \psi(Kb)$. But $\psi(Ka) = \varphi(a)$ and $\psi(Kb) = \varphi(b)$. If $Ka = Kb$, then $K = Kba^{-1}$, whence $ba^{-1} \in K$, so that $\varphi(ba^{-1}) = e'$. Hence $\varphi(b)\varphi(a)^{-1} = e'$, so $\varphi(b) = \varphi(a)$. Consequently, $\psi(Ka) = \psi(Kb)$. □
- (ψ a homomorphism): Whenever $a, b \in G$, one has
$$\psi(Ka)\psi(Kb) = \varphi(a)\varphi(b) = \varphi(ab) = \psi(Kab) = \psi(Ka \cdot Kb),$$
so ψ is indeed a homomorphism. □
- (ψ surjective): Whenever $g \in G'$, the surjectivity of φ implies that there exists $a \in G$ with $\psi(a) = g$. But $\psi(Ka) = \varphi(a)$, so there exists $Ka \in G/K$ with $\psi(Ka) = g$, and so ψ is surjective. □

- (ψ injective): Whenever $\psi(Ka) = \psi(Kb)$, one has $\varphi(a) = \varphi(b)$, whence $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e'$, so that $ab^{-1} \in K = \ker(\varphi)$. Thus $a \in Kb$ and $Ka = Kb$. So ψ is indeed injective. □

We have shown that ψ is a well-defined, injective and surjective homomorphism, and hence an isomorphism, from G/K onto G'. Thus $G' \cong G/K$. //

The first isomorphism theorem shows that if $K = \ker(\varphi)$ for a surjective homomorphism $\varphi: G \to G'$, then G/K is isomorphic to the whole group G'. But what happens with subgroups of G'? Theme is "$H/K \leftrightarrow H' \leq G$."

Theorem 2.7.2. (Correspondence Theorem). Let $\varphi : G \to G'$ be a surjective homomorphism of groups with kernel K. Suppose that $H' \leq G'$ and

$$H = \{ a \in G : \varphi(a) \in H' \}.$$

Then $H \leq G$, $K \subseteq H$ and $H/K \cong H'$. Also, whenever $H' \lhd G'$ one has $H \lhd G$.

Proof. We have several things to prove here:

(a) $H \leq G$: We have $e \in H$, so $H \neq \emptyset$. Also, whenever $a, b \in H$, one has $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} \in H'$, since $\varphi(a), \varphi(b) \in H'$. Thus $ab^{-1} \in H$, and so $H \leq G$ by subgroup criterion. □

(b) If $K = \ker(\varphi)$ then $a \in K \Rightarrow \varphi(a) = e' \in H'$, so $K \subseteq H$. □

(c) Observe next that since $K \lhd G$ and $K \subset H$, then the definition of normality implies that $K \lhd H$. Now consider the map

$$\varphi|_H : H \longrightarrow H', \quad h \longmapsto \varphi(h)$$

(the restriction of φ to H).

The map $\varphi|_H$ is a surjective homomorphism from H to H' with kernel K, so by the First Homomorphism Theorem we have $H/K \cong H'$. □

(d) When $H' \lhd G'$, then, whenever $g \in G$ we have

$$\varphi(g^{-1}Hg) = \varphi(g)^{-1}\varphi(H)\varphi(g) = \varphi(g)^{-1}H'\varphi(g) \leq H',$$

so $g^{-1}Hg \leq H$. Hence $H \lhd G$. □ //

We can identify subgroups from other subgroups in various ways. One such method is to take a subgroup $H \leq G$ and a normal subgroup $N \lhd G$, and then consider the set

$$HN = \{hn \in G : h \in H, n \in N\}.$$

It transpires that $HN \leq G$.

Proof: In order to confirm this assertion, observe that whenever $h_1, h_2 \in H$ and $n_1, n_2 \in N$, one has

$$(h_1n_1)(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1} = \underbrace{h_1h_2^{-1}}_{\in H}\underbrace{(h_2(n_1n_2^{-1})h_2^{-1})}_{h_2Nh_2^{-1} \leq N}$$

$$\in HN.$$

Thus $HN \leq G$ by the subgroup criterion. //

Theorem 2.7.3 (Second Homomorphism Theorem). Suppose that $H \leq G$ and $N \lhd G$. Then

$$H/(H \cap N) \cong (HN)/N.$$

[Note: We have left implicit here that $H \leq G$ & $N \lhd G \Rightarrow H \cap N \lhd H$, which is an easy exercise since normality is inherited from N].

Proof: Observe that $N \subset HN \leq G$, so $N \lhd HN$.

(43) We define a homomorphism of groups

$$\varphi : H \longrightarrow (HN)/N$$
$$a \longmapsto Na .$$

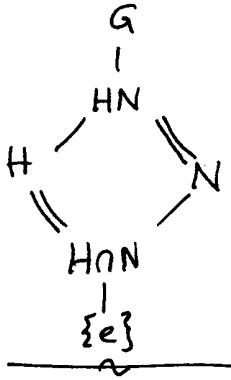
This map is well-defined, since for $a \in H$ one has $Na = aN \in HN$. Also, since $\varphi(ab) = Nab = Na\,Nb = \varphi(a)\varphi(b)$, for all $a, b \in H$, the map φ defines a homomorphism. To check surjectivity, observe that whenever $h \in H$ and $n \in N$, one has $hn \in hN = Nh$, so $hn = n'h$ for some $n' \in N$, whence $Nhn = Nn'h = Nh = \varphi(h)$. Since $\varphi : H \to (HN)/N$ is a surjective homomorphism, one has

$$(HN)/N \cong H / \ker(\varphi).$$

But $\ker(\varphi) = \{a \in H : aN = N\} = \{a \in H : a \in N\} = H \cap N$, so that

$$HN/N \cong H / H \cap N . \;//$$

We can draw a lattice of groups:



Each line represents an inclusion within a larger group.

Theorem 2.7.4. (Third Homomorphism Theorem). Suppose that $\varphi : G \to G'$ is a surjective homomorphism of groups with kernel K, and $N' \lhd G'$. Put $N = \{a \in G : \varphi(a) \in N'\}$. Then one has $G/N \cong G'/N'$, or equivalently $G/N \cong (G/K)/(N/K)$.

Proof As with previous arguments, the proof is focused on the construction of an appropriate homomorphism. Define

$$\psi : G \longrightarrow G'/N'$$
$$a \longmapsto N'\varphi(a).$$

Since $\varphi : G \to G'$ is surjective, and each element of G'/N' takes the form $N'b'$ for some $b' \in G'$, there exists $a \in G$ with

$\varphi(a) = b'$, whence $N'b' = N'\varphi(a)$. Thus ψ is surjective.

When $a, b \in G$, one has

$$\psi(ab) = N'\varphi(ab) = N'\varphi(a)\varphi(b) = (N'\varphi(a))(N'\varphi(b)) = \psi(a)\psi(b),$$

so ψ satisfies the homomorphism property. Moreover,

$$\ker(\psi) = \{ a \in G : \psi(a) = N'e' = N' \}$$

$$\psi(a) = N'\varphi(a)$$

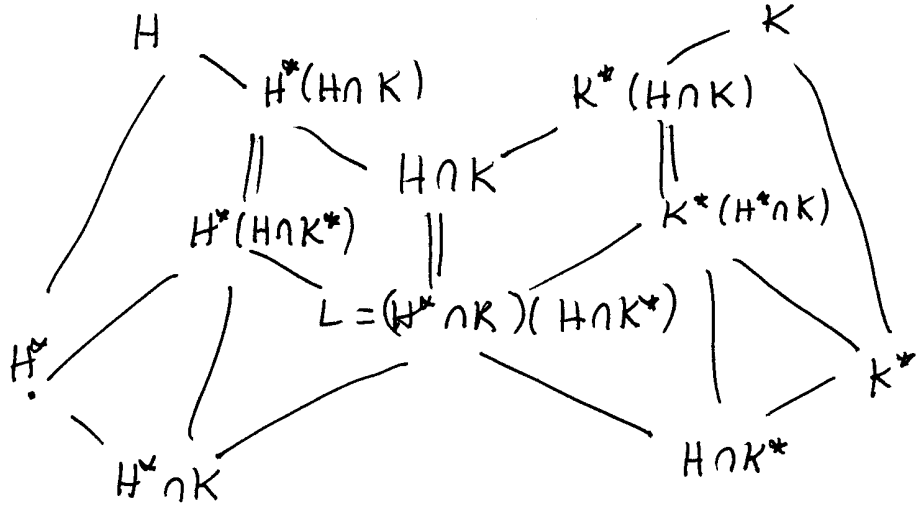
$$= \{ a \in G : \varphi(a) \in N' \} = N \quad \text{(by definition)}.$$

Then ψ is a surjective homomorphism of G to G'/N' with kernel N, so by the First Homomorphism Theorem, one has $G/N \cong G'/N'$. But we also have $G' \cong G/K$ (by the First Homomorphism theorem) and $N' \cong N/K$ (by the Correspondence Theorem), so $G/N \cong (G/K)/(N/K)$. //

Zassenhaus Lemma: (Later!) Suppose $\left\{ \begin{array}{l} H \leq G, \quad K \leq G \\ H^* \lhd H, \quad K^* \lhd K \end{array} \right\}$. Then

- $H^*(H \cap K^*) \lhd H^*(H \cap K)$
- $K^*(H^* \cap K) \lhd K^*(H \cap K)$
- $H^*(H \cap K)/H^*(H \cap K^*) \cong K^*(H \cap K)/K^*(H^* \cap K)$

$$\cong (H \cap K)/((H^* \cap K)(H \cap K^*))$$



§3.1, 3.2. The Symmetric Group S_n – Basics

Recall that if G is a finite group, then $G \cong H$ for some $H \leq S_n$, for some integer n (viewing $S_n = A(\{1,2,\dots,n\})$). — this was a consequence of Cayley's Theorem.

Recall the permutation notation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix} \in S_n,$$

where $\sigma(i) = a_i$ for each $1 \leq i \leq n$. Notice that no two a_i can be equal, for else this is not a bijective self-mapping of $\{1,2,\dots,n\}$.

Also,

$$\sigma^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Make sure you understand how to combine two mappings. For example

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}}_{\sigma} \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}}_{\tau} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$$

$1 \to 4 \to 5$
$2 \to 5 \to 4$

We read this right to left to determine $\sigma\tau(a)$, say, but other sources go left to right, so caution!

Cycle notation: (Cycle decomposition).

Definition. When $i_1, \dots, i_k$ are k distinct integers in $S = \{1,2,\dots,n\}$, we write $(i_1, i_2, \dots, i_k)$ to denote the permutation $\sigma \in S_n$ given by $\sigma(i_1) = i_2, \dots, \sigma(i_j) = i_{j+1}, \dots, \sigma(i_k) = i_1$ and $\sigma(s) = s$ for $s \in S \setminus \{i_1, \dots, i_k\}$.

Thus $\sigma = (1\ 3\ 2)(4\ 5)$, $\tau = (1\ 4\ 2\ 5\ 3)$.

- A permutation interchanging two elements, such as (i_1, i_2), is called a transposition.

- An m-cycle is a permutation of the shape $(i_1, i_2, \ldots, i_m)$.

- Two cycles are disjoint if they contain no common elements. Thus (132) and (45) are disjoint 3- and 2-cycles.

  Notice that disjoint cycles commute. (Lemma 3.2.1).

Caution: The product of cycles that are not disjoint can be written as the product of disjoint cycles: For example

$$(1\,3\,2\,4)\,(4\,5) = (4\,5\,1\,3\,2)$$

$$\left.\begin{array}{l} 4 \to 5 \to 5 \\ 5 \to 4 \to 1 \\ 1 \to 1 \to 3 \\ \vdots \\ 2 \to 2 \to 4 \end{array}\right\} \text{ Remember : right to left!}$$

Exercise A k-cycle has order k in S_n.

Theorem 3.2.2. Every permutation in S_n is the product of disjoint cycles.

Proof. Consider $\sigma \in S_n$. First determine the cycle defining the orbit of 1, namely $\tau_1 = (1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k-1}(1))$, where $\sigma^k(1) = 1$, and $\sigma^\ell(1) \neq 1$ for $1 \leq \ell < k$. Next take $j \in \{1, 2, \ldots, n\} \setminus \{1, \sigma(1), \ldots, \sigma^{k-1}(1)\}$, and consider the orbit of j, namely $\tau_2 = (j, \sigma(j), \ldots, \sigma^{\ell-1}(j))$, say. Repeat until all elements $1, 2, \ldots, n$ are contained in the union of the elements defining the cycles $\tau_1, \tau_2, \ldots, \tau_m$.

Then $\sigma = \tau_1 \tau_2 \cdots \tau_m$ as a product of disjoint cycles. //

Theorem 3.2.4. Let $\sigma \in S_n$ have a cycle decomposition $\tau_1 \tau_2 \cdots \tau_k$, where τ_j is an m_j-cycle for $1 \le j \le k$. Then $o(\sigma) = [m_1, \cdots, m_k]$, the lcm of $m_1, \cdots, m_k$.

Proof. Disjoint cycles commute, and hence if $(\tau_1 \tau_2 \cdots \tau_k)^M = e$, then $\tau_1^M \tau_2^M \cdots \tau_k^M = e$. Since the cycles are disjoint, the latter holds if and only if $\tau_j^M = e$ for each j, whence $m_j | M$ for each j. Hence $o(\sigma) = \text{lcm}(m_1, \cdots, m_k) = [m_1, \cdots, m_k]$. //

Theorem 3.2.5 Every permutation in S_n is the product of transpositions.

Proof. It suffices to prove the conclusion for a k-cycle, since every permutation is a product of disjoint cycles. Consider then

$$\sigma = (i_1, \cdots, i_k) \in S_n.$$

We have $\sigma = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_2)$, so σ is a product of transpositions, and hence so is any element of S_n. //

§3.3. Odd and even permutations.

We have shown that every permutation is a product of transpositions, but this might be the case in many different ways. One might enquire if there are any special properties of the decomposition into transpositions.

Theorem 3.3.1 A permutation σ in S_n is either odd or even, in the sense that if σ is a product of an odd number

of transpositions, then it is never a product of an even number of transpositions, and vice versa.

Proof. Consider the polynomial (in n variables $x_1, \dots, x_n$)

$$f(x) = \prod_{1 \le i < j \le n} (x_i - x_j) = \det (x_i^{j-1})_{1 \le i,j \le n} = \det \begin{pmatrix} x_1^{n-1} & \dots & x_n^{n-1} \\ x_1^{n-2} & \dots & x_n^{n-2} \\ \vdots & & \\ x_1 & \dots & x_n \\ 1 & \dots & 1 \end{pmatrix}$$

Vandermonde determinant.

We can consider the action of a permutation $\sigma \in S_n$ on $f(x)$. Thus

$$\sigma(f(x)) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}) = \det (x_{\sigma(i)}^{j-1})_{1 \le i,j \le n}.$$

Notice that this permutes the columns of the determinant.

Now suppose that we can write σ as the product of k transpositions, say $\sigma = \tau_1 \tau_2 \dots \tau_k$. Each transposition interchanges two columns of the determinant. So the determinant changes sign. Thus,

$$\begin{aligned} \sigma(f(x)) = \tau_1 \dots \tau_k (f(x)) &= -\tau_1 \dots \tau_{k-1} (f(x)) \\ &= (-1)^2 \tau_1 \dots \tau_{k-2} (f(x)) \\ &= \dots = (-1)^k f(x). \end{aligned}$$

Then if $\sigma = \tau_1 \dots \tau_k$ and $\sigma = \tau_1' \dots \tau_\ell'$, then

$$(-1)^k f(x) = \sigma(f(x)) = (-1)^\ell f(x),$$

whence $(-1)^k = (-1)^\ell$. That is, k and ℓ are either both odd or both even. //

Definition. The subset A_n of all even permutations of S_n is called the alternating group of degree n.

Implicit Claim: A_n is a group.

Proof. Since e is a product of 0 transpositions, we have $e \in A_n$ and A_n is non-empty.

Next, if $\sigma, \tau \in A_n$, then σ and τ are each a product of an even number of transpositions. In particular, if $\tau = \omega_1 \cdots \omega_k$ as a product of transpositions, then $\tau^{-1} = \omega_k^{-1} \omega_{k-1}^{-1} \cdots \omega_1^{-1}$ $= \omega_k \omega_{k-1} \cdots \omega_1$ is also a product of an even number of transpositions. Thus $\sigma\tau^{-1}$ is also a product of an even number of transpositions, so $\sigma\tau^{-1} \in A_n$. Thus, by the subgroup criterion, we have $A_n \leq G$. //

More is true:

Theorem: One has $A_n \lhd S_n$ for each n.

Proof: Let $\sigma \in A_n$ and $\tau \in S_n$, and write each as a product of transpositions, say $\sigma = \omega_1 \cdots \omega_k$ and $\tau = \nu_1 \cdots \nu_l$. Then

$$\tau^{-1}\sigma\tau = (\nu_1 \cdots \nu_l)^{-1} \omega_1 \cdots \omega_k (\nu_1 \cdots \nu_l)$$
$$= \nu_l \cdots \nu_1 \omega_1 \cdots \omega_k \nu_1 \cdots \nu_l$$

is a product of $k+2l$ transpositions. Then whenever k is even, which is the case when $\sigma \in A_n$, one has $\tau^{-1}\sigma\tau \in A_n$ (since $k+2l$ is even). Thus $\tau^{-1} A_n \tau \in A_n$ for all $\tau \in S_n$, whence $A_n \lhd S_n$. //

Natural question: how large is A_n? Here we can apply the First Homomorphism Theorem. Consider

$\varphi: S_n \longrightarrow E := \{1, -1\}$ as a multiplicative group.
$\sigma \longmapsto (-1)^k$ where k is odd if σ odd, k even if σ even.

This map φ is a homomorphism of groups. It is well defined (because permutations are either odd or even), and whenever $\sigma, \tau \in S_n$ then

$$\varphi(\sigma\tau) = (-1)^m, \quad \text{where } m \text{ is odd when } \sigma\tau \text{ is odd, and even when } \sigma\tau \text{ is even.}$$

$$\varphi(\sigma)\varphi(\tau) = (-1)^{k+l}, \quad \text{where } \begin{cases} k \text{ odd when } \sigma \text{ odd} \\ l \text{ odd when } \tau \text{ odd} \\ k \text{ even when } \sigma \text{ even} \\ l \text{ even when } \tau \text{ even.} \end{cases},$$

But $\sigma\tau$ is odd when σ and τ are not both odd, and not both even, and otherwise $\sigma\tau$ is even.

Then $m \equiv k+l \pmod 2$, so $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$. ✓

One has $\ker(\varphi) = \{\sigma \in S_n : \varphi(\sigma) = 1\}$

$= \{\sigma \in S_n : \sigma \text{ is even}\} = A_n$.

Then by the first isomorphism theorem, one has

$$S_n / A_n \cong E,$$

so $\dfrac{|S_n|}{|A_n|} = |E| = 2$, whence $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$

Theorem 3.3.3: For $n > 1$, the group A_n is a normal subgroup of S_n of order $\frac{1}{2}n!$

We shall see later that the group A_n is simple for $n \geq 5$. Note that $|A_5| = 60$, and A_5 is the smallest nonabelian example of a simple group.

---

§6.1. The group A_n is simple for $n \geq 5$.

Thus far, the only simple groups (groups having no proper normal subgroups) of which we know are isomorphic to $\mathbb{Z}_p$, for a prime number p (cyclic groups of prime order).

Any abelian groups that are simple must have no proper subgroups, so must be cyclic of prime order and hence isomorphic to $\mathbb{Z}_p$ (p prime). We now give a family of non-abelian simple groups.

Theorem 6.1.9. When $n \geq 5$, the group A_n is simple.

The proof takes some development.

Theorem 6.1.2. A_n is generated by the 3-cycles in S_n.

Proof. If $\sigma \in A_n$, then σ is the product of an even number of transpositions, say $\sigma = (t_1, t_2)(t_3, t_4) \cdots (t_{2k-1}, t_{2k})$. Consider any pair of such transpositions (when $k \geq 1$). If the pair share no common elements, we may relabel entries to reduce to the situation $(1,2)(3,4) = (1,4,2)(1,4,3)$. If they share an entry, by relabelling we can consider $(1,2)(1,3) = (1,3,2)$. If $k = 0$ we have the identity $e = (1,2,3)(1,3,2)$. In all cases, each pair is a product of 3-cycles, so A_n is generated by 3-cycles. //

Theorem 6.1.8. The group A_5 is simple.

Proof. Observe that $|A_5| = \frac{1}{2} \cdot 5! = 60$. Then by Lagrange's theorem, the elements of A_5 have order dividing 60, namely 2, 3 or, 5... (or 1 in the case of the identity element).

(52)

Notice that there can be no elements of order 10, 15, 20, 30, since these would consist of 5-cycles with disjoint additional cycles, which is impossible (since there is insufficient room in A_5 or indeed S_5). Likewise, there is no element of order 12, since this would consist of disjoint 3- and 4-cycles, and there is insufficient room. Finally, any 6-cycle takes the shape (by relabelling) $(123)(45) = (13)(12)(45) \notin A_5$ (odd!) and any 4-cycle takes the shape $(1234) = (14)(13)(12) \notin A_5$. Thus the elements of A_5 have orders 2, 3 or 5.

Suppose, by way of seeking a contradiction, that N is a proper subgroup of A_5 with $N \triangleleft A_5$. Then N contains an element of order 2, 3 or 5. We claim that in fact N contains an element of order 3. For if N contains an element of order 2, we may relabel to assume it to be $(1,3)(2,4)$ (note that $(1,2)(1,3) = (1,3,2)$ has order 3). But then

$$\left.\begin{array}{l}(1,2,3,4,5)^{-1}\underbrace{(1,3)(2,4)}_{=(1,3)(2,5)}(1,2,3,4,5) \in N\end{array}\right\} \Rightarrow (1,3)(2,5)(1,3)(2,4) = (2,4,5) \in N \checkmark$$

(has order 3).

Also, if N contains an element of order 5, we may relabel elements to assume that it is $(1,2,3,4,5)$, and then

$$((1,3)(2,4))^{-1}(1,2,3,4,5)((1,3)(2,4)) = (1,2,5,3,4) \in N,$$

whence $(1,2,3,4,5)^{-1}(1,2,5,3,4) = (2,4,5) \in N$. $\checkmark$

By relabelling, we may now suppose that $(1,2,3) \in N$. But this implies that all 3-cycles lie in N. For we can replace $(1,2,3)$ by $(1,2,\alpha)$ for any α by conjugation, when $\alpha \in \{4,5\}$:

Note: In the proof of Theorem 6.1.8 one can get more rapidly to the point. We suppose that N is a proper subgroup of A_5 with $N \lhd A_5$. Then $|N|$ divides $|A_5| = 60$, so N contains an element of some order $d > 1$ dividing 60. Then $d \in \{2k, 3k, 5k\}$ for some $k \in \mathbb{N}$. If $a \in N$ has order lk, then a^k has order l, so N contains an element of order 2, 3 or 5.

$$(2,3,\alpha)^{-1}\ \underbrace{(1,2,3)^2}_{\in N}\ (2,3,\alpha) = (1,2,\alpha) \in N.$$

So whenever $(\alpha,\beta,\gamma) \in N$, then $(\alpha,\beta,\delta) \in N$ for any δ, and thus also $(\alpha,\delta,\beta) \in N$. By switching elements in this way, we see that all 3-cycles belong to N.

But A_5 is generated by the 3-cycles of S_5, so since N contains all 3-cycles, we have $N = A_5$. But then A_5 contains no proper subgroup of itself which is normal. Thus A_5 is simple. //

Theorem 6.1.9. For $n \geq 5$, the group A_n is simple.

Proof. In view of Theorem 6.1.8, we have that A_5 is simple. We proceed by induction, supposing that when $n > 5$, the group A_m is simple for $5 \leq m < n$. Let N be a normal subgroup of A_n with $N \neq \{e\}$.

We begin by showing that N contains an element σ which leaves an element of $\{1,2,\dots,n\}$ fixed. Suppose, by way of deriving a contradiction, that no such element σ exists. Then for $\sigma \in N$ there are distinct elements $a,b,c,d \in \{1,2,\dots,n\}$ such that

$$\sigma(a) = b, \quad \sigma(c) = d.$$

Since $n \geq 6$, there is an element $\tau \in A_n$ with

$$\tau = (a,b)(c,d,e,f)^{-1},$$

for some $e,f \notin \{a,b,c,d\}$ with $e \neq f$. Note that (c,d,e,f) is the product of 3 transpositions, so indeed $\tau \in A_n$. By normality of N in A_n, one has $\tau^{-1}\sigma\tau \in N$, and

$$\tau^{-1}\sigma\tau(b) = a, \quad \tau^{-1}\sigma\tau(d) = e.$$

Also, $\tau^{-1}\sigma\tau\sigma \in N$, and

$\tau^{-1}\sigma\tau\sigma(a) = a$, $\tau^{-1}\sigma\tau\sigma(c) = e$.

Thus $\tau^{-1}\sigma\tau\sigma$ is a non-trivial element of N leaving a fixed ※

This contradiction shows that N contains a non-trivial element fixing one of $1, 2, \ldots, n$. □

Suppose next that $\sigma \in N\setminus\{e\}$ and $\sigma(1) = 1$, as we can without loss of generality, from the previous paragraph. The elements of A_n which fix 1 form a subgroup $H_1 \leq A_n$ with $H_1 \cong A_{n-1}$. Thus $N \cap H_1 \neq \{e\}$ and $N \cap H_1 \lhd H_1$. But H_1 is simple, since the inductive hypothesis allows us to assume that A_{n-1} is simple. Hence $N \cap H_1 = H_1$, whence $H_1 \leq N$.

Let τ be any even permutation with $\tau(2) = 1$. Then $\tau^{-1}\sigma\tau(2) = \tau^{-1}\sigma(1) = \tau^{-1}(1) = 2$, so $H_2 := \tau^{-1} H_1 \tau$ is a subgroup of A_n that fixes 2. By normality of N in A_n, we have $\tau^{-1} H_1 \tau \leq N$ (since $H_1 \leq N$). But as above, we have $\tau^{-1} H_1 \tau \cong A_{n-1}$, and

$$H_1 \cap \tau^{-1} H_1 \tau \cong A_{n-2},$$

since $H_1 \cap \tau^{-1} H_1 \tau$ fixes both 1 and 2.

Consider now the group generated by the set $gp\{H_1, H_2\} = \{h_1 h_2 : h_1 \in H_1 \& h_2 \in H_2\}$. We have $gp(H_1 H_2) \leq N$. In order to compute the number of elements in $H_1 H_2$ observe that if $g_1, h_1 \in H_1$ and $g_2, h_2 \in H_2$, then

$gp(H_1, H_2)$

$g_1 g_2 = h_1 h_2$ if and only if $h_1^{-1} g_1 = h_2 g_2^{-1}$, and moreover, in such circumstances $h_1^{-1} g_1 \in H_1$ and $h_2 g_2^{-1} \in H_2$, so both left and right hand sides lie in $H_1 \cap H_2$. Say $h_1^{-1} g_1 = h_2 g_2^{-1} = t \in H_1 \cap H_2$. But then the multiplicity with which an element $k \in H_1 H_2$ is represented as a product $g_1 g_2$ with $g_i \in H_i$ is at most $|H_1 \cap H_2|$. Hence $|H_1 H_2| \geq |H_1| \cdot |H_2| / |H_1 \cap H_2|$.

Then $|N| \geq |H_1 H_2| \geq \dfrac{|A_{n-1}| \cdot |A_{n-1}|}{|A_{n-2}|} = \dfrac{\frac{1}{2}(n-1)! \cdot \frac{1}{2}(n-1)!}{\frac{1}{2}(n-2)!}$,

whence $|N| \geq \frac{1}{2}(n-1) \cdot (n-1)!$. But $|A_n| = \frac{1}{2} n!$, so

$$1 \leq |A_n / N| = \frac{|A_n|}{|N|} \leq \frac{\frac{1}{2} n!}{\frac{1}{2}(n-1)(n-1)!} = \frac{n}{n-1} < 2.$$

This delivers a contradiction unless $N = A_n$. Thus A_n has no proper normal subgroups, and hence is simple. //

---

§ 2.8. Cauchy's Theorem.

We earlier showed that when G is abelian and a prime p satisfies $p \mid |G|$, then G has an element of order p. We now extend this theorem to nonabelian groups. In the abelian case we used the idea that $H \leq G$ implies $H \trianglelefteq G$ to reduce to considering either a smaller subgroup H, or a "smaller quotient group G/H. A non-abelian group might not have a normal subgroup, however, so we must work differently.

One idea is to partition the elements of G in orbits.

Definition. Let S be a set and $f \in A(S)$. The orbit of an element $s \in S$ under the action of f is

$$\mathrm{Orb}_f(s) := \{ f^i(s) : i \in \mathbb{Z} \}.$$

Notice that we can define an equivalence relation on S by defining $s \sim t$ when $t = f^i(s)$ for some $i \in \mathbb{Z}$. (Check this is an equivalence relation). The equivalence classes $[s]$ are then orbits of s under f.

Lemma 2.8.1. Suppose that $f \in A(S)$ has order p, where p is a prime number. Then for all $s \in S$, one has

$$|\mathrm{Orb}_f(s)| = 1 \quad \text{or} \quad |\mathrm{Orb}_f(s)| = p.$$

Proof. Let $s \in S$. There are two cases to consider:

(a) If $f(s) = s$, then $\mathrm{Orb}_f(s) = \{s\}$ and so $|\mathrm{Orb}_f(s)| = 1$; □

(b) If $f(s) \neq s$, then

$$\mathrm{Orb}_f(s) = \{ s, f(s), \dots, f^{p-1}(s) \}.$$

We claim that the p elements listed are distinct. For otherwise we have $f^i(s) = f^j(s)$ for some $0 \leq i < j < p$, whence $f^{j-i}(s) = s$ with $1 \leq j-i \leq p-1$. Put $k = j-i$ and note that $(k,p) = 1$, whence there exist integers a and b with $ak + bp = 1$. Hence

$$f(s) = f^{ak+bp}(s) = f^{bp}(f^{km}(s)) = f^{bp}(s) = s. \quad \#$$

Then the p elements listed are indeed distinct, and hence $|\mathrm{Orb}_f(s)| = p$. □ //

Theorem 2.8.2. (Cauchy's Theorem) Suppose that p is a prime with $p \mid |G|$. Then G has an element of order p.

Proof. Two cases:

(a) $p = 2$. If $2 \mid |G|$, then — if it were the case that no element has order 2 — we would have $a^2 \neq e$ for all $a \in G \setminus \{e\}$, whence $a \neq a^{-1}$ for all $a \in G \setminus \{e\}$. By partitioning G into subsets $\{a_i, b_i\}$, where $a_i b_i = e$, we see that with the addition of the set $\{e\}$, we must have $|G|$ odd. #

Thus G contains an element a with $a^2 = e$ and $a \neq e$, so $o(a) = 2$. □

(b) $p > 2$. Let $S = \{ (a_1, a_2, \dots, a_p) \in G^p : a_1 a_2 \dots a_p = e \}$.

Note that given any $a_1, \dots, a_{p-1} \in G$, we have $(a_1, \dots, a_p) \in S$ if and only if $a_p = (a_1 a_2 \dots a_{p-1})^{-1} \in G$. Thus $|S| = |G|^{p-1}$.

The map $f : S \to S$ belongs to $A(S)$.

$$(a_1, \dots, a_p) \longmapsto (a_p, a_1, \dots, a_{p-1})$$

Moreover, one has $f \neq \mathrm{id}$ (since $p \neq 2$) and $f^p = \mathrm{id}$, so f has order p. Plainly, one has $f(s) = s$ if and only if $s = (a, \dots, a)$ for some $a \in G$. Notice that in the latter circumstances, one has $a^p = e$. Since p is prime, we have then that $o(a) = p$ or $o(a) = 1$ (in which case $a = e$). Thus, if we can show that $s = (a, \dots, a) \in S$ for some $a \in G$, which amounts to showing that $f(s) = s$ for some $s \in S$, then we can conclude that G has an element a of order p.

Let $m = \text{card}\{s \in S : f(s) = s\}$. Then $m \geq 1$ since $s = (e, e, \ldots, e)$ satisfies $f(s) = s$. But

$$|S| - m = \text{card}\{s \in S : f(s) \neq s\},$$

and for each $s \in S$ with $f(s) \neq s$, it follows from Lemma 2.8.1 that $|\text{Orb}_f(s)| = p$. But $|S| = |G|^{p-1}$ and p divides $\text{card}\{s \in S : f(s) \neq s\}$ (since the latter set is a union of orbits, each having cardinality p). Thus $|G|^{p-1} - m \equiv 0 \pmod{p}$. Since $p \mid |G|$, it follows that $m \equiv 0 \pmod{p}$. But $m \geq 1$, so $m \geq p$, and this shows that for some $a \in G \setminus \{e\}$, one has $(a, \ldots, a) \in S$, whence $a^p = e$. Thus G contains an element of order p. □ //

Cauchy's Theorem has a very powerful consequence for the structure of certain finite groups:

Theorem 2.8.5. Suppose that G is a group of order pq, where p and q are primes with $p > q$. Provided that $q \nmid (p-1)$, one has that G is cyclic.

Thus, for example, any group of order 15 is cyclic, since $15 = 5 \times 3$ and $3 \nmid (5-1)$. And any group of order 65 is cyclic.

In order to prove this result, we study normal subgroups associated with G.

Lemma 2.8.3. Let G be a group with $|G| = pq$, where p and q are primes with $p > q$. Whenever $a \in G$ has order p, then $\langle a \rangle \triangleleft G$.

Proof: We show that $A := \langle a \rangle$ is the only subgroup of G having order p, and the normality will follow. For if $B \leq G$ and $|B| = p$, then $AB = \{ab : a \in A \text{ and } b \in B\}$ is a subset of G

having cardinality $|AB| \leq |G| = pq < p^2$. Suppose that a_1, a_2 are distinct elements of A, and b_1, b_2 are distinct elements of B, and moreover $a_1 b_1 = a_2 b_2$. Then $\underset{A}{\underset{\cap}{a_2^{-1}a_1}} = \underset{B}{\underset{\cap}{b_2 b_1^{-1}}}$, whence $a_2^{-1}a_1 \in A \cap B$. But if $B \neq A$, then since $A \cap B \leq G$ and A has prime order, we must have $A \cap B = \{e\}$, whence $a_2^{-1}a_1 = e$, so that $a_1 = a_2$ and $b_1 = b_2$. Thus all products ab with $a \in A$ and $b \in B$ are distinct, whence $p^2 \leq |AB| < p^2$ ✗. Thus $B = A$, and indeed A is the only subgroup of G with $|A| = p$.

Now we can establish that $A \triangleleft G$. For whenever $g \in G$, the group $g^{-1}Ag \leq G$ and $|g^{-1}Ag| = p$, so $g^{-1}Ag = A$. Hence $A \triangleleft G$. //

Corollary. Under the assumptions of Lemma 2.8.3, we have that for each $g \in G$, $g^{-1}ag = a^i$ for some $i = i(g)$ with $1 \leq i < p$.

Proof. Since $g^{-1}Ag = A$, we have $g^{-1}ag \in \langle a \rangle$. //
Moreover, if $g^{-1}ag = e$ then $a = e$ ✗.

Theorem 2.8.5. Let G be a group of order pq, where p and q are prime numbers with $p > q$. Then whenever $q \nmid (p-1)$, the group G is cyclic.

Proof. By Cauchy's Theorem, G has an element a of order p and an element b of order q. The Corollary shows that $b^{-1}ab = a^i$ for some i with $1 \leq i < p$. Hence, for each $r \geq 0$, one has

$$b^{-r}ab^r = b^{1-r}a^i b^{r-1} = b^{2-r}(b^{-1}ab)^i b^{r-2} = b^{2-r}(a^i)^i b^{r-2}$$
$$= b^{2-r}a^{i^2}b^{r-2} = \ldots = a^{i^r}.$$

In particular, one has $a = b^{-q}ab^q = a^{i^q}$, so that $p \mid (i^q - 1)$. But by Fermat's Little Theorem (cf. Euler), one

has $i^{p-1} \equiv 1 \pmod{p}$ for $1 \le i < p$. Thus, since $q < p$ and $q \nmid (p-1)$, and $i^q \equiv 1 \pmod{p}$ and $i^{p-1} \equiv 1 \pmod{p}$, we have $i \equiv 1 \pmod{p}$. We therefore deduce that $i = 1$ and hence $ba = ab$.

But whenever $(ab)^m = e$, one has $a^m = b^{-m}$. Then $a^{mq} = (b^q)^{-m} = e$ which shows that $p \mid mq$ and thus $p \mid m$. Similarly, one has $q \mid m$, so $pq \mid m$. Moreover $(ab)^{pq} = (a^p)^q (b^q)^m = e$, so ab has order pq, whence $G = \langle ab \rangle$, since $|G| = pq$. //

It follows that every group of order 15 is cyclic (and hence abelian) since $15 = 3 \cdot 5$ and $3 \nmid (5-1)$, and likewise every group of order 33 is cyclic.

When G has order pq, with p, q primes and $p > q$, and $q \mid (p-1)$, then one can construct a non-abelian group of order pq.

Exercise 4 constructs a group of order 21 $\langle a, b : a^3 = b^7 = e,$ $ba = a^i b \rangle$, where i satisfies $i^3 \equiv 1 \pmod{7}$.

[This is a "semi-direct product" of C_7 and C_3, with C_7 and C_3 cyclic of order 7 and 3: $G \cong C_7 \rtimes C_3$.]

---

§2.9. Direct Products (Internal and External)

Suppose that $G_1, G_2, \ldots, G_n$ is any collection of n groups. The (external) direct product $G_1 \times G_2 \times \cdots \times G_n$ is the group

$$G = \{ (g_1, g_2, \ldots, g_n) : g_i \in G_i \text{ for } 1 \le i \le n \}$$

with the group operation

$$(g_1, g_2, \dots, g_n) * (h_1, h_2, \dots, h_n) = (g_1 h_1, g_2 h_2, \dots, g_n h_n).$$

Easy to check $G_1 \times \cdots \times G_n$ is a group with identity $(e_1, \dots, e_n)$ and inverse $(g_1^{-1}, \dots, g_n^{-1})$ for $(g_1, \dots, g_n)$.

When G is an external direct product of groups $G_1, \dots, G_n$, then its structure is transparent from that of each G_i, so it would be very convenient if we could somehow relate G to some kind of decomposition of this type.

Remark 1. Define $\overline{G}_i = \{(e_1, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_n) : g_i \in G_i\}$.

Then $G_i \cong \overline{G}_i \lhd G_1 \times \cdots \times G_n =: G$

Proof. Easy to check $G_i \leq G$. Indeed, if we define the (projection) mapping

$$\pi_i : \overline{G}_i \longrightarrow G_i$$
$$(e_1, e_2, \dots, g_i, \dots, e_n) \longmapsto g_i,$$

then π_i is a {surjective / injective} homomorphism from $\overline{G}_i$ to G_i, so $\overline{G}_i \cong G_i$.

Also, whenever $\gamma \in G$ then $\gamma^{-1}(e_1, e_2, \dots, g_i, \dots, e_n)\gamma = (e_1, \dots, h_i^{-1} g_i h_i, \dots, e_n)$, where the i-th coordinate of γ is h_i. $\in \overline{G}_i$.

Thus $\overline{G}_i \lhd G$. //

Remark 2. If $\gamma = (g_1, g_2, \dots, g_n) \in G$, then

$$\gamma = (g_1, e_2, \dots, e_n)(e_1, g_2, e_3, \dots, e_n) \cdots (e_1, e_2, \dots, e_{n-1}, g_n),$$

and one sees that $G = \overline{G}_1 \overline{G}_2 \cdots \overline{G}_n$. This representation is unique.

Definition. We say that G is the internal direct product of its normal subgroups $N_1, \ldots, N_n$ if every $g \in G$ has a unique representation in the form $g = g_1 g_2 \cdots g_n$ with $g_i \in N_i$ $(1 \le i \le n)$.

Lemma 2.9.1. If $G = G_1 \times G_2 \times \cdots \times G_n$ is the external direct product of $G_1, \ldots, G_n$, then G is the internal direct product of $\overline{G}_1, \overline{G}_2, \ldots, \overline{G}_n$.

Proof: See above. //

We aim to prove a converse type result:

Theorem 2.9.4. Let G be a group with normal subgroups $N_1, \ldots, N_n$. Then the map

$$\psi : N_1 \times N_2 \times \cdots \times N_n \longrightarrow G$$
$$(g_1, g_2, \ldots, g_n) \longmapsto g_1 g_2 \cdots g_n$$

is an isomorphism if and only if G is the internal direct product of $N_1, N_2, \ldots, N_n$.

The proof requires several intermediate steps.

Lemma 2.9.3 If G is the internal direct product of its normal subgroups $N_1, N_2, \ldots, N_n$, then for $i \neq j$ we have $N_i \cap N_j = \{e\}$.

Proof. Suppose that $a \neq e$ and $a \in N_i \cap N_j$ for some $i \neq j$. Then

$$a = e \cdot e \cdots e \cdot \underset{\text{ith place}}{\underset{\uparrow}{a}} \cdot e \cdots e = e \cdot e \cdots e \cdot \underset{\text{jth place}}{\underset{\uparrow}{a}} \cdot e \cdots e,$$

whence the uniqueness of direct product decompositions $G = N_1 \cdots N_n$ implies that $a = e$ #. So $N_i \cap N_j = \{e\}$, as required. //

Lemma 2.9.2. Let G be a group and suppose $M \trianglelefteq G$, $N \trianglelefteq G$ and $M \cap N = \{e\}$. Then for all $m \in M$ and $n \in N$, one has $mn = nm$.

Proof. Let $a = mnm^{-1}n^{-1}$. Then $a = (mnm^{-1})n^{-1} \in N$, and

$a = m(nm^{-1}n^{-1}) \in M$, so $a \in M \cap N$, whence $a = e$. Thus

$mnm^{-1}n^{-1} = e$, so that $mn = nm$. //

Corollary. If G is the internal direct product of its normal subgroups $N_1, N_2, \ldots, N_n$, then whenever $a_i \in N_i$ and $a_j \in N_j$ with $i \neq j$, one has $a_i a_j = a_j a_i$.

Proof of Theorem 2.9.4. ($\Rightarrow$) Suppose $\psi : N_1 \times \cdots \times N_n \to G$, $(g_1, \ldots, g_n) \longmapsto g_1 g_2 \cdots g_n$ is an isomorphism. Then each $g \in G$ has a representation $g = g_1 g_2 \cdots g_n = \psi(g_1, \ldots, g_n)$, because ψ is surjective. Also, since ψ is injective, whenever $g = g_1 g_2 \cdots g_n$ with $(g_1, \ldots, g_n) \in N_1 \times \cdots \times N_n$, each g_i is unique, so the representation is unique. Thus G is the internal direct product of $N_1, N_2, \ldots, N_n$. □

($\Leftarrow$) Suppose that G is the internal direct product of $N_1, N_2, \ldots, N_n$. Then each $g \in G$ has a representation $g = g_1 \cdots g_n$ with $g_i \in N_i$, so ψ is surjective. If $\psi(g_1, \ldots, g_n) = \psi(h_1, \ldots, h_n)$, then $g_1 \cdots g_n = h_1 \cdots h_n$. But this product representation is unique, by definition of the internal direct product, so $g_i = h_i$ $(1 \leq i \leq n)$, whence $(g_1, \ldots, g_n) = (h_1, \ldots, h_n)$. Thus ψ is injective. Finally we check that ψ is a homomorphism, and hence an isomorphism. Whenever $(g_1, \ldots, g_n), (h_1, \ldots, h_n) \in N_1 \times \cdots \times N_n$, we have

$$\psi((g_1, \ldots, g_n)(h_1, \ldots, h_n)) = \psi(g_1 h_1, \ldots, g_n h_n) = (g_1 h_1)(g_2 h_2) \cdots (g_n h_n)$$
$$= g_1 h_1 \cdots g_n h_n.$$

But the corollary above shows that g_2 commutes with h_1, so that

$$g_1 h_1 g_2 h_2 \cdots g_n h_n = g_1 g_2 h_1 h_2 g_3 h_3 \cdots g_n h_n$$

and g_3 commutes with h_1, h_2, and so on. Thus

$$g_1 h_1 g_2 h_2 \cdots g_n h_n = (g_1 \cdots g_n)(h_1 \cdots h_n) = \psi(g_1, \cdots, g_n)\psi(h_1, \cdots, h_n),$$

whence ψ satisfies the homomorphism property. $\square$ //

Convenient to drop the distinction between internal and external direct products, and to interpret $G = N_1 \times N_2$ as $G = N_1 N_2$ when $N_1 \cap N_2 = \{e\}$, for example.

Special Case: If G is a group with $N_1 \triangleleft G$, $N_2 \triangleleft G$, then G is the internal direct product of N_1 and N_2 if and only if $N_1 \cap N_2 = \{e\}$ and $G = N_1 N_2$.

Proof. Home $\psi : N_1 \times N_2 \longrightarrow G$ is an isomorphism if and only if
$(g_1, g_2) \longmapsto g_1 g_2$

$G = N_1 N_2$ and $N_1 \cap N_2 = \{e\}$. //

§2.10. Finite abelian groups.

We shall deviate considerably from the account of Herstein, although his approach remains valuable. Our goal is the Fundamental Theorem of Finite Abelian Groups:

Theorem 2.10.A Suppose that G is a finite abelian group. Then G is isomorphic to a direct product of cyclic groups of the shape

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}},$$

where the p_i are primes, not necessarily distinct, for $1 \le i \le r$, and

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Corollary 2.10.B. If G is a finite abelian group, then there are positive integers $m_1, \ldots, m_k$, with $1 < m_1 \le m_2 \le \cdots \le m_k$ and $m_i \mid m_{i+1}$ $(1 \le i < k)$, such that $G \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$.

Proof of corollary: We can collect the factors in the decomposition provided by the theorem to collect together like primes (using obvious notation)

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_1^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_1^{\alpha_{r_1}}}$$

$$\times \mathbb{Z}_{p_2^{\beta_1}} \times \mathbb{Z}_{p_2^{\beta_2}} \times \cdots \times \mathbb{Z}_{p_2^{\beta_{r_2}}}$$

$$\times \cdots$$

$$\times \mathbb{Z}_{p_\ell^{\omega_1}} \times \mathbb{Z}_{p_\ell^{\omega_2}} \times \cdots \times \mathbb{Z}_{p_\ell^{\omega_{r_\ell}}},$$

with $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_{r_1}$, $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_{r_2}$, $\ldots$, $\omega_1 \geq \omega_2 \geq \cdots \geq \omega_{r_\ell}$.

But since the primes p_i are pairwise coprime, we have

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_\ell^{\beta_1}} \times \cdots \times \mathbb{Z}_{p_\ell^{\omega_1}} \cong \mathbb{Z}_{m_1},$$

where $m_1 = p_1^{\alpha_1} p_\ell^{\beta_1} \cdots p_\ell^{\omega_1}$, and in general

$\mathbb{Z}_{p_1^{\alpha_j}} \times \mathbb{Z}_{p_2^{\beta_j}} \times \cdots \times \mathbb{Z}_{p_\ell^{\omega_j}} \cong \mathbb{Z}_{m_j}$, where any exponent θ_j is taken to be 0 if $j \geq r_i$ for p_i. Here, we have $m_j \mid m_{j-1}$ for $1 < j \leq k$ where $k = \max r_i$. Thus

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}, \quad \text{where}$$

$m_1 \geq m_2 \geq \cdots \geq m_k \geq 1$ and $m_j \mid m_{j-1}$ for $1 < j \leq k$. Reverse the roles of the suffices to obtain the stated corollary. //

Example. Classify all abelian groups of order 1400.

Solution: We have $1400 = 7 \cdot 200 = 2^3 \cdot 5^2 \cdot 7$.

Then by the Fundamental Theorem of Finite Abelian Groups, every abelian group of order 1400 is isomorphic to one of:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{70}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{10} \times \mathbb{Z}_{140}$$

$$\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_5 \times \mathbb{Z}_{280}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_7 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{350}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25} \times \mathbb{Z}_7 \cong \mathbb{Z}_2 \times \mathbb{Z}_{700}$$

$$\mathbb{Z}_8 \times \mathbb{Z}_{25} \times \mathbb{Z}_7 \cong \mathbb{Z}_{1400}.$$

6 isomorphism classes.

The proof of Theorem 2.10.A: (and we prove a little more)

We proceed in two steps:

Lemma 2.10.C. Let G be a finite abelian group of order $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where the p_i are distinct primes and $\alpha_i \in \mathbb{N}$. Then G is an internal direct product of subgroups $G_1, \ldots, G_k$, where G_i is the subgroup of G having all elements g of order $p_i^{r_i}$ for some $r_i(g) \geq 1$.

Proof. Let $G_i = \{ g \in G : g^{p_i^r} = e \text{ for some } r \in \mathbb{N} \}$. Then (as we have seen in a homework problem) one has $G_i \leq G$. For if $g \in G_i$ has order p_i^r, then g^{-1} has order p_i^r. Also, $e \in G_i$, and if h has order p_i^s, then $(gh^{-1})^{p_i^{r+s}} = (g^{p_i^r})^{p_i^s} (h^{p_i^s})^{-p_i^r} = e$. So $G_i \leq G$ by the subgroup criterion. Since G is abelian, moreover, we have $G_i \trianglelefteq G$. □

Next we show that when $g \in G_1$, then $g = g_1 g_2 \cdots g_k$ for some $g_i \in G_i$. We have $o(g) \mid |G|$, so $o(g) = p_1^{\beta_1} \cdots p_k^{\beta_k}$ for some $\beta_i \in \mathbb{Z}_{\geq 0}$ with $\beta_i \leq \alpha_i$ $(1 \leq i \leq k)$. Put $a_i = o(g) / p_i^{\beta_i}$, so $(a_1, \ldots, a_k) = 1$.

Then by the Euclidean Algorithm, we have that there exist $b_1, \ldots, b_k \in \mathbb{Z}$ with $a_1 b_1 + \cdots + a_k b_k = 1$, whence

$$g = (g^{a_1 b_1}) \cdots (g^{a_k b_k}).$$

But $(g^{a_i b_i})^{p_i^{\alpha_i}} = (g^{o(g)})^{b_i} = e$ $(1 \le i \le k)$, so $g^{a_i b_i} \in G_i$. Thus $g = g_1 \cdots g_k$ with $g_i = g^{a_i b_i}$ $(1 \le i \le k)$. □

To show that $G = G_1 \cdots G_k$ as an internal direct product, we must show that the above decomposition is unique, and this amounts to showing that $G_i \cap G_j = \{e\}$ for $i \neq j$. But if $g \in G_i \cap G_j$ then

$$g^{p_i^{\alpha_i}} = e \;\&\; g^{p_j^{\alpha_j}} = e \Rightarrow g^{(p_i^{\alpha_i}, p_j^{\alpha_j})} = e, \text{ so } g = e.$$
$$\| \\ g^1$$

Thus $G_i \cap G_j = \{e\}$ for $i \neq j$, and $G = G_1 \cdots G_k$ as an internal direct product. //

A group having order equal to a prime power is a special case of a <u>p-group</u> (a group in which every element has order a power of a fixed prime p). We must classify finite p-groups.

<u>Lemma 2.10.D.</u> Let G be a finite abelian p-group and suppose that $g \in G$ has maximal order. Then for some $H \le G$, one has

$$G \cong \langle g \rangle \times H. \quad \text{(as an internal direct product)}.$$

<u>Proof.</u> By Cauchy's Theorem, the order of G must be a power of a prime number p, say $|G| = p^n$ for some $n \in \mathbb{N}$. We apply induction on n.

<u>When $n = 1$</u>, the group G must be cyclic of order p, say $G = \langle g \rangle$ and we are done with $H = \{e\}$. □

Suppose now that $n > 1$, and that the desired conclusion holds for all groups G' of order p^k with $1 \le k < n$.

Let g be of maximal order in G, say $o(g) = p^m$ with $m < n$.

Put $A = \langle g \rangle$, and let $h \in G \setminus A$ be the element of least possible order (in $G \setminus A$), which is of course automatically a power of p. Note that we can assume $G \setminus A \neq \emptyset$, for otherwise $G \cong \langle g \rangle \times \{e\}$. □

Claim: $o(h) = p$.

Proof. The order of h is a power of p, so $o(h^p) = o(h)/p$. Then the minimality of the order of h within $G \setminus A$ implies that $h^p \in \langle g \rangle$, so $h^p = g^r$ for some $r \in \mathbb{Z}$. But $o(g) = p^m$, and

$$(g^r)^{p^{m-1}} = (h^p)^{p^{m-1}} = h^{p^m} = e \quad \text{(since } o(g) = p^m \text{ is maximal)},$$

whence $p^m \mid r p^{m-1} \Rightarrow p \mid r$, say $r = ps$ with $s \in \mathbb{Z}$.

Put $a = g^{-s} h$ and observe that if $a \in \langle g \rangle$ then $h \in \langle g \rangle$. *. So $a \notin \langle g \rangle$ and $a^p = g^{-sp} h^p = g^{-r} h^p = e$, so that $a \in G \setminus A$ and $o(a) = p$. Then the minimality of the order of h implies $o(h) = p$. □

• Now we study $H = \langle h \rangle$ and G/H (note $H \trianglelefteq G$). We claim that the order of Hg in G/H is $o(g) = p^m$. For $o(Hg) \mid p^m$ since $(Hg)^{p^m} = Hg^{p^m} = H$, and if $o(Hg) < o(g) = p^m$, then $H = (Hg)^{p^{m-1}} = Hg^{p^{m-1}}$, whence $g^{p^{m-1}} \in H$. This shows that $g^{p^{m-1}} = h^u$, some $u \in \mathbb{Z}$, whence $h = g^{vp^{m-1}}$ with $v \in \mathbb{Z}$ satisfying $uv \equiv 1 \pmod{p}$ if $p \nmid u$. But $h \notin \langle g \rangle$, so $u = 0$ and $g^{p^{m-1}} = e$ #. This contradicts $o(g) = p^m$. Then Hg has order p^m in G/H. But no element in G/H can have order larger than the maximal order of any element in G, which is p^m. So Hg has maximal order in G/H, yet $|G/H| = |G|/|H| < |G|$, so by the inductive hypothesis, one has $G/H \cong \langle Hg \rangle \times T$ (direct product) for some $T \leq G$. By the Correspondence Theorem, moreover, one has $T = K/H$ for some $H \trianglelefteq K \leq G$.

• At this point we have shown that $G/H \cong \langle Hg \rangle \times K/H$. We now aim to prove that $G \cong \langle g \rangle \times K$. The first observation

is that $a \in G \Rightarrow aH \in \langle Hg \rangle \times K/H$, so $aH \in g^r k H$, some $r \in \mathbb{Z}$ and $k \in K$, whence $a = g^r k h' = g^r k'$, some $h' \in H$ and $k' \in K$. So $G = \langle g \rangle K$. If $\langle g \rangle \cap K \neq \{e\}$, say $b \in \langle g \rangle \cap K$, then $Hb \in \langle Hg \rangle \cap K/H$, (trivial intersection) so $Hb = H$ (since $G/H = \langle Hg \rangle \times K/H$ as a direct product). Then $b \in H = \langle h \rangle$ and $b \in \langle g \rangle$. We have seen already that this implies $b = e$ (since otherwise $h \in \langle g \rangle$ #). Thus $G = \langle g \rangle \times K$ and $\langle g \rangle \cap K = \{e\}$, so $G = \langle g \rangle \times K$ as a direct product. //

We can now prove Theorem 2.10.A. From Lemma 2.10.C we see that if G is a finite abelian group, then G is a direct product $G = G_1 G_2 \cdots G_k$, where each G_i is a p_i-group, for distinct primes $p_1, \ldots, p_k$. Fix a p_i for i. Then Lemma 2.10.D shows that G_i has an element $g_i \in G_i \setminus \{e\}$ of maximal order, and a subgroup H_i such that $G_i = \langle g_i \rangle H_i$, with H_i a p_i-group. By induction, one finds that

$$G_i = \langle g_{i1} \rangle \langle g_{i2} \rangle \cdots \langle g_{ir_i} \rangle,$$

where $o(g_{ij}) = p^{n_j}$, say, and $n_1 \geq n_2 \geq \cdots \geq n_{r_i} \geq 1$. Thus $G_i \cong \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_{r_i}}}$. Hence G is a direct product of cyclic groups of prime power order, as required, //

---

§2.11. Conjugacy and the Sylow Theorems. (extended version of Herstein)

Recall: We say a is conjugate to b in G if there exists $g \in G$ with $b = g^{-1}ag$. (Equivalence relation).

Define $cl(a) = \{b \in G : b \text{ is conjugate to } a\}$.

Recall that we showed that the centralizer of a, namely

$$C(a) = \{ g \in G : ga = ag \}$$

is a subgroup of G.

Theorem 2.11.2. Let G be a finite group and $a \in G$. Then

$$|cl(a)| = i_G(C(a)) = |G| / |C(a)|.$$

Proof. Suppose that $b \in cl(a)$, so that $b = gag^{-1}$ for some $g \in G$. If also $b = hah^{-1}$ for some $h \in G$, then $gag^{-1} = b = hah^{-1}$, whence $h^{-1}ga = ah^{-1}g$, so $h^{-1}g \in C(a)$, and thus $g \in hC(a)$. This argument shows in fact that $gag^{-1} = hah^{-1}$ if and only if $g \in hC(a)$. Then the number of conjugates of a in G is equal to $\text{card}\{ hC(a) \in G/C(a) : h \in G \} = |G| / |C(a)| = i_G(C(a))$. //

Theorem 2.11.3. (The Class Equation). If G is a finite group, then

$$|G| = \sum_a i_G(C(a)) = \sum_a \frac{|G|}{|C(a)|},$$

where the summation is over distinct conjugacy class representatives.

Proof. Using the equivalence relation of conjugacy in G, we partition G into conjugacy classes and obtain the stated relation immediately. //

Corollary 2.11.4. Suppose that G is a group of order p^n, where p is prime and $n \in \mathbb{N}$. Then $Z(G) \neq \{e\}$.

Proof. If $z \in Z(G)$, then every element of G commutes with z (one has $C(z) = G$), so $\frac{|G|}{|C(z)|} = |cl(z)| = 1$. If $a \in G \setminus Z(G)$, meanwhile, then $C(a) \leq G$ and $C(a) \neq G$, so $|C(a)|$ is a divisor d of p^n with $d < p^n$, say $|C(a)| = p^{n_a}$ with $0 \leq n_a < n$ (as a consequence of Lagrange's Theorem). Then

the Class Equation yields

$$p^n = |G| = |Z(G)| + \sum_{a \in G \setminus Z(G)} \frac{|G|}{|C(a)|} = |Z(G)| + \sum_{\substack{a \in G \\ n_a < n}} \frac{p^n}{p^{n_a}},$$

in which we sum over distinct conjugacy class representatives. Thus

$|Z(G)| \equiv 0 \pmod{p}$, and yet since $e \in Z(G)$ one has $|Z(G)| \geq 1$. Then $|Z(G)| \geq p$, whence $Z(G) \neq \{e\}$. //

Corollary 2.11.5. If G is a group of order p^2, with p prime, then G is abelian.

Hence, a group of order p^2, with p prime, is isomorphic to one of $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof of corollary 2.11.5. By Corollary 2.11.4, we have $Z(G) \neq \{e\}$, so by Cauchy's Theorem $Z(G)$ contains an element a of order p. Put $\langle a \rangle =: A \leq G$, so $A \leq C(x)$ for all $x \in G$. If $x \notin A$, then $x \in C(x)$ and $A \leq C(x)$, so $|C(x)| \geq |A| + 1 > p$. Then by Lagrange's Theorem, one has $|C(x)| \mid p^2$ and $|C(x)| \geq p+1$, so that $|C(x)| = p^2$. Then $G = C(x)$, so $x \in Z(G)$. Thus all elements of G lie in $Z(G)$, and so G is abelian.

If G has prime power order p^n with $n > 2$, then less is certain. However, it is at least possible to unravel a large part of the structure of G.

Theorem 2.11.6. Suppose that G is a group of order p^n, with p prime. Then G contains a normal subgroup of order p^{n-1}.

Proof. By induction. When $n=1$ the conclusion is trivial, since $\{e\} \lhd G$. □

Suppose the conclusion has been proved for all groups of order p^k, with $1 \le k < n$ and $n > 1$, and consider a group G of order p^n.

We know that $Z(G) \neq \{e\}$, so $|Z(G)| = p^m$ for some integer m with $1 \le m \le n$ (Corollary 2.11.4). By Cauchy's Theorem, therefore, $Z(G)$ contains an element a of order p, and $A := \langle a \rangle \lhd G$. We now consider the group $H = G/A$, noting that $|H| = |G|/|A| = p^{n-1}$. By the inductive hypothesis, the group H has a normal subgroup M of order p^{n-2}, and so the Correspondence Theorem shows that there exists $A \lhd N \lhd G$ with $N/A = M$. Thus we have

[Use $\varphi : G \to G/A = H$, $\varphi(N) = M$] $\quad p^{n-2} = |M| = |N/A| = \dfrac{|N|}{|A|} = \dfrac{|N|}{p}$,

so that $|N| = p^{n-1}$. So $N \lhd G$ satisfies $|N| = p^{n-1}$, completing the induction.

Theorem 2.11.7 (First Sylow Theorem). Let G be a group of order $p^n m$, where p is a prime and $p \nmid m$. Then G has a subgroup of order p^n.

Proof. We can assume that $n \ge 1$, and we again proceed by induction, assuming that the desired conclusion holds for all groups H with $|H| < |G|$. Our starting point is the Class Equation:

$$p^n m = |G| = |Z(G)| + \sum_{a \notin Z(G)} i_G(C(a)). \qquad (*)$$

Suppose that G has no subgroup of order p^n. Then by the inductive hypothesis, whenever $H \le G$ one has $p^n \nmid |H|$. Then if $a \notin Z(G)$, so that $C(a) \neq G$, one has $p^n \nmid |C(a)|$. Hence $p \mid i_G(C(a)) = |G|/|C(a)|$ for $a \notin Z(G)$.

We therefore conclude from (*) that $p \mid |Z(G)|$, so $Z(G)$ contains an element of order p, by Cauchy's theorem. But then $A := \langle a \rangle \trianglelefteq G$, and we can put $K = G/A$.

Notice that $|K| = |G|/|A| = p^n m/p = p^{n-1} m$ and $|K| < |G|$, so our inductive hypothesis implies that K has a subgroup M of order p^{n-1}. Again applying the correspondence theorem, there exists $P \leq G$ such that $A \trianglelefteq P \leq G$ and $P/A = M$. Hence $|P| = |M| \cdot |A| = p^{n-1} \cdot p = p^n$, and P is the subgroup of G of order p^n which we sought. This completes the inductive step. //

Definition. A **Sylow p-subgroup** P of a group G is a maximal p-subgroup of G. Thus, if $|G| = p^n m$ with p prime and $(p, m) = 1$, then G has a Sylow p-subgroup of order p^n.

[$\mathrm{Syl}_p(G)$ = set of all Sylow p-subgroups of G].

Theorem 2.11.8. (Second Sylow Theorem). Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G.

Proof. Let P be a Sylow p-subgroup of a group G of order $p^n m$ with $(m, p) = 1$. We suppose that Q is another Sylow p-subgroup of G with $Q \neq x^{-1} P x$ for any $x \in G$, and derive a contradiction.

Define $S = \{ y^{-1} Q y : y \in G \}$, and define a relation $\sim$ on S by taking $Q_1 \sim Q_2$ when $Q_2 = a^{-1} Q_1 a$ for some $a \in P$. One can check easily that this gives an equivalence relation on S. How many elements are there in a given equivalence class?

We have

$$a^{-1}Q_1 a = b^{-1}Q_1 b \iff (ab^{-1})^{-1} Q_1 (ab^{-1}) = Q_1$$
$$\iff ab^{-1} \in N(Q_1) \cap P$$
$$\iff a \in (N(Q_1) \cap P)b.$$

Then for a fixed choice of $b \in P$, the number of distinct choices for a with $a^{-1}Q_1 a = b^{-1}Q_1 b$ is $|N(Q_1) \cap P|$, and for each distinct coset $(N(Q_1) \cap P)b$ we obtain a distinct element Q_2 of S with $Q_2 \sim Q_1$. Then each equivalence class contains $|P/(N(Q_1) \cap P)|$ elements. We now seek to show that this is a power of p, say p^m, with $m \geq 1$. Since S is then a union of equivalence classes each containing a number of elements divisible by p, we shall have shown that $|S| \equiv 0 \pmod p$.

But since $|P| = p^n$, we have that $|P/(N(Q_1) \cap P)|$ is not divisible by p if and only if $|P/(N(Q_1) \cap P)| = 1$, and this can happen if and only if $P \leq N(Q_1)$. But then $P \leq N(Q_1)$. Moreover, from HW Q 2.11.9 we have $Q_1 \trianglelefteq N(Q_1)$. Thus $PQ_1 \leq N(Q_1)$, and by the Second Homomorphism Theorem we have $PQ_1/Q_1 = P/(P \cap Q_1)$ (working inside $N(Q_1)$), whence $|PQ_1| = |Q_1| \cdot |P| / |P \cap Q_1|$. But every element of $P \cap Q_1$ has order a power of p, and likewise for Q_1 and P, so each group has order a power of P. Then PQ_1 is a p-group and contains the (maximal) p-group P. Thus $P = PQ_1$, and hence $Q_1 \leq P$. Since $|Q_1| = |P|$, it follows that $Q_1 = P$, and hence $a^{-1}Qa = P$ for some $a \in P$, whence $Q = P$. ※

We conclude that $|S| \equiv 0 \pmod p$. But by HW Q 2.11.13, the number of distinct subgroups $x^{-1}Qx$ of G is equal to

$|S| = i_G(N(Q)) = \dfrac{|G|}{|N(Q)|}$. Since $Q \lhd N(Q)$, we have $|Q| \mid |N(Q)|$, whence $p^n \mid |N(Q)|$. But $|G| = p^n m$ with $(m,p)=1$, so $p \nmid \dfrac{|G|}{|N(Q)|}$, whence $|S| \not\equiv 0 \pmod p$. This contradiction shows that $Q = x^{-1}Px$ for some $x \in G$, whence any two Sylow p-subgroups are conjugate. //

Theorem 2.11.9. (Third Sylow Theorem). The number of Sylow p-subgroups of a group G of order $p^n m$, with p prime and $p \nmid m$, is equal to $1 + kp$ for some $k \in \mathbb{Z}$, and divides $|G|$.

Proof. We argue as in the proof of the Second Sylow Theorem, using the same notation. If there is only one Sylow p-subgroup P of G, then we are done. Otherwise, each equivalence class of $S \setminus \{P\}$ (of conjugate groups to a Sylow p-subgroup $Q \neq P$) has a number of elements divisible by p. So $|S \setminus \{P\}| = kp$ for some $k \in \mathbb{Z}_{\geq 0}$. The number of Sylow p-subgroups conjugate via the action of P to P is just 1 however, since $a^{-1}Pa = P$ whenever $a \in P$. Thus the number of Sylow p-subgroups of G is $1 + kp$ for some $k \in \mathbb{Z}$.

We must still show that $1 + kp$ divides $|G|$. Suppose that P is any Sylow p-subgroup of G. If Q is any Sylow p-subgroup of G (possibly P itself) then $Q = g^{-1}Pg$ for some $g \in G$. With what multiplicity is Q represented? Well, if $h^{-1}Ph = Q = g^{-1}Pg$, then $(hg^{-1})^{-1}P(hg^{-1}) = P$, so $hg^{-1} \in N(P)$, whence $h \in N(P)g$. Thus there are $|N(P)|$ elements $g \in G$ with $Q = g^{-1}Pg$, for each $Q \in S \cup \{P\}$. Then $|G| = (1+kp)|N(P)|$, whence $(1+kp) \mid |G|$. //

§ 2.12. Small Groups.

The tools provided by the Sylow theorems offer powerful approaches to understanding groups of small order. Of course, we understand abelian groups comprehensively, and we know that G is abelian when $|G|$ is equal to p or p^2 (p prime), and also when $|G| = pq$ with $p > q$ and $q \nmid (p-1)$ (p, q prime).

Non-abelian groups of small order:

$|G| = 2p$ (p prime). G has a Sylow p-subgroup of order p, and since $(kp+1) \nmid 2p$ for $k \geq 1$, there is precisely 1 such subgroup P. Then P is fixed by conjugation, whence $P \triangleleft G$. Say $P = \langle a \rangle$ with $a^p = e$. If $b \in G \setminus P$, then b has order 2, and so

$$b^{-1}ab = a^r, \quad \text{some } 1 \leq r \leq p-1,$$

whence $b^{-2}ab^2 = a^{r^2}$, so that $r^2 \equiv 1 \pmod{p}$ and $r \neq 1$ (else a abelian).

So $b^{-1}ab = a^{-1}$, and $G \cong D_{2p}$, the Dihedral group of order $2p$.

Similar ideas can be applied in some other instances – it is always useful (if possible) to find a normal subgroup of G to assist the discussion. Fortunately, as is seen in HW9, the only simple groups having order smaller than $60 = |A_5|$ are cyclic groups having prime order.

Here is a list of groups having order at most 20:

Order	Abelian Groups	Non-abelian Groups
1	$\mathbb{Z}_1$	none
2	$\mathbb{Z}_2$	none
3	$\mathbb{Z}_3$	none
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$	none
5	$\mathbb{Z}_5$	none
6	$\mathbb{Z}_6$	$S_3 \cong D_6$
7	$\mathbb{Z}_7$	none
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_8, Q_8
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$	none
10	$\mathbb{Z}_{10}$	D_{10}
11	$\mathbb{Z}_{11}$	none
12	$\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_3$	A_4, D_{12}, $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$
13	$\mathbb{Z}_{13}$	none
14	$\mathbb{Z}_{14}$	D_{14}
15	$\mathbb{Z}_{15}$	none
16	$\mathbb{Z}_{16}$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_{16}, $\mathbb{Z}_2 \times D_8$, $\mathbb{Z}_2 \times Q_8$, Q_{16}, $\mathbb{Z}_4 \rtimes \mathbb{Z}_4$, M_{16}, SD_{16}, G_1, G_2 (two others!)
17	$\mathbb{Z}_{17}$	none
18	$\mathbb{Z}_{18}$, $\mathbb{Z}_6 \times \mathbb{Z}_3$	D_{18}, $S_3 \times \mathbb{Z}_3$, $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$
19	$\mathbb{Z}_{19}$	none
20	$\mathbb{Z}_{20}$, $\mathbb{Z}_{10} \times \mathbb{Z}_2$	D_{20}, $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$, F_{20}

(7)

$Q_{16} = \langle a, b \mid a^8 = b^4 = e, \quad a^4 = b^2, \quad b^{-1}ab = a^{-1} \rangle$.

$\mathbb{Z}_4 \rtimes \mathbb{Z}_4 = \langle a, b \mid a^4 = b^4 = e, \quad bab^{-1} = a^3 \rangle$

$M_{16} = \langle a, b \mid a^8 = b^2 = e, \; bab^{-1} = a^5 \rangle$

$SD_{16} = \langle a, b \mid a^8 = b^2 = e, \; bab^{-1} = a^3 \rangle$

$G_1 =$ Small Group $(16, 3) = \langle a, b, c \mid a^4 = b^2 = c^2 = e, \; ab = ba, \; bc = cb, \; cac^{-1} = ab \rangle$

$G_2 =$ central product $(D_8, \mathbb{Z}_4) = \langle a, b, c \mid a^4 = b^2 = e, \; a^2 = c^2, \; bab^{-1} = a^{-1}, \; bc = cb, \; ac = ca \rangle$

$F_{20} =$ Frobenius group of order 20

$= \langle a, b \mid a^4 = b^5 = e, \quad aba^{-1} = b^2 \rangle$

$\mathbb{Z}_5 \rtimes \mathbb{Z}_4 = \langle a, b \mid a^4 = b^5 = e, \quad a^{-1}ba = b^{-1} \rangle$

$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2 = \langle a, b, c \mid a^2 = b^3 = c^3 = e, \; bc = cb, \; a^{-1}ba = b^{-1}, \; a^{-1}ca = c^{-1} \rangle$

$\mathbb{Z}_3 \rtimes \mathbb{Z}_4 = \langle a, b \mid a^4 = b^3 = e, \quad a^{-1}ba = b^{-1} \rangle$.

$Q_8 = \langle a, b \mid a^4 = e, \quad a^2 = b^2, \quad ba = a^{-1}b \rangle$

or

$Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$ (Quaternion Group).

$(-1)^2 = 1$
$i^2 = j^2 = k^2 = ijk = -1.$

So $ij = k, \; jk = i, \; ki = j$
$ji = -k, \; kj = -i, \; ik = -j$

§4.1 Ring Theory : definitions, examples.

So far, with the notion of a group, we have a set with a binary operation satisfying the group axioms. We now explore a set with two binary operations.

Definition. Let R be a non-empty set. Then R is a ring if there are two binary operations (traditionally) denoted $+$ and $\cdot$ satisfying the following properties:

(A0) $a, b \in R$ implies $a+b \in R$
(A1) $a + b = b+a$ for all $a,b \in R$
(A2) $(a+b)+c = a+(b+c)$ for all $a,b,c \in R$
(A3) there exists $0 \in R$ such that $a+0 = a$ for all $a \in R$
(A4) whenever $a \in R$, there exists $b \in R$ such that $a+b=0$.
(and we write $-a$ for b)

} $(R,+)$ forms an abelian group.

(M0) $a, b \in R$ implies $a \cdot b \in R$
(M1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a,b,c \in R$

} multiplication is an associative binary operation

(D1) $a \cdot (b+c) = a \cdot b + a \cdot c$
$(b+c) \cdot a = b \cdot a + c \cdot a$
for all $a,b,c \in R$

} Distributive laws connect $+$ and $\cdot$.

Example $(\mathbb{Z}, +, \cdot)$ is a (familiar!) ring
Also $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$.

Note: People do investigate non-associative rings where the axiom (M1) is deleted — scary algebra!!

Example Trivial $R = \{0\}$. (no room for things to go wrong).

Short Version of Definition of a Ring: R is a non-empty set with two binary operations $+$ and $\cdot$ satisfying:

(1) $(R,+)$ is an abelian group
(2) $\cdot$ is associative
(3) $(R,+,\cdot)$ satisfies distributive laws $a \cdot (b+c) = a \cdot b + a \cdot c$, $(b+c) \cdot a = b \cdot a + c \cdot a$.

Rings with extra properties:

(a) Rings with unity

If $(R, +, \cdot)$ satisfies the extra axiom:

(M2) there exists $1 \in R$ with $1 \neq 0$ such that $a \cdot 1 = 1 \cdot a = a$, for all $a \in R$,

then $(R, +, \cdot)$ is called a *Ring with a unit*.

[Some sources insist that *any* ring should have a 1].

(b) Commutative Rings

If $(R, +, \cdot)$ satisfies the extra axiom:

(M3) for all $a, b \in R$, one has $a \cdot b = b \cdot a$,

then R is a *commutative ring*.

(c) Domains.

If $(R, +, \cdot)$ satisfies:

(M4) Whenever $a \cdot b = 0$ then $a = 0$ or $b = 0$,

then R is called a *domain*

(d) Integral domains.

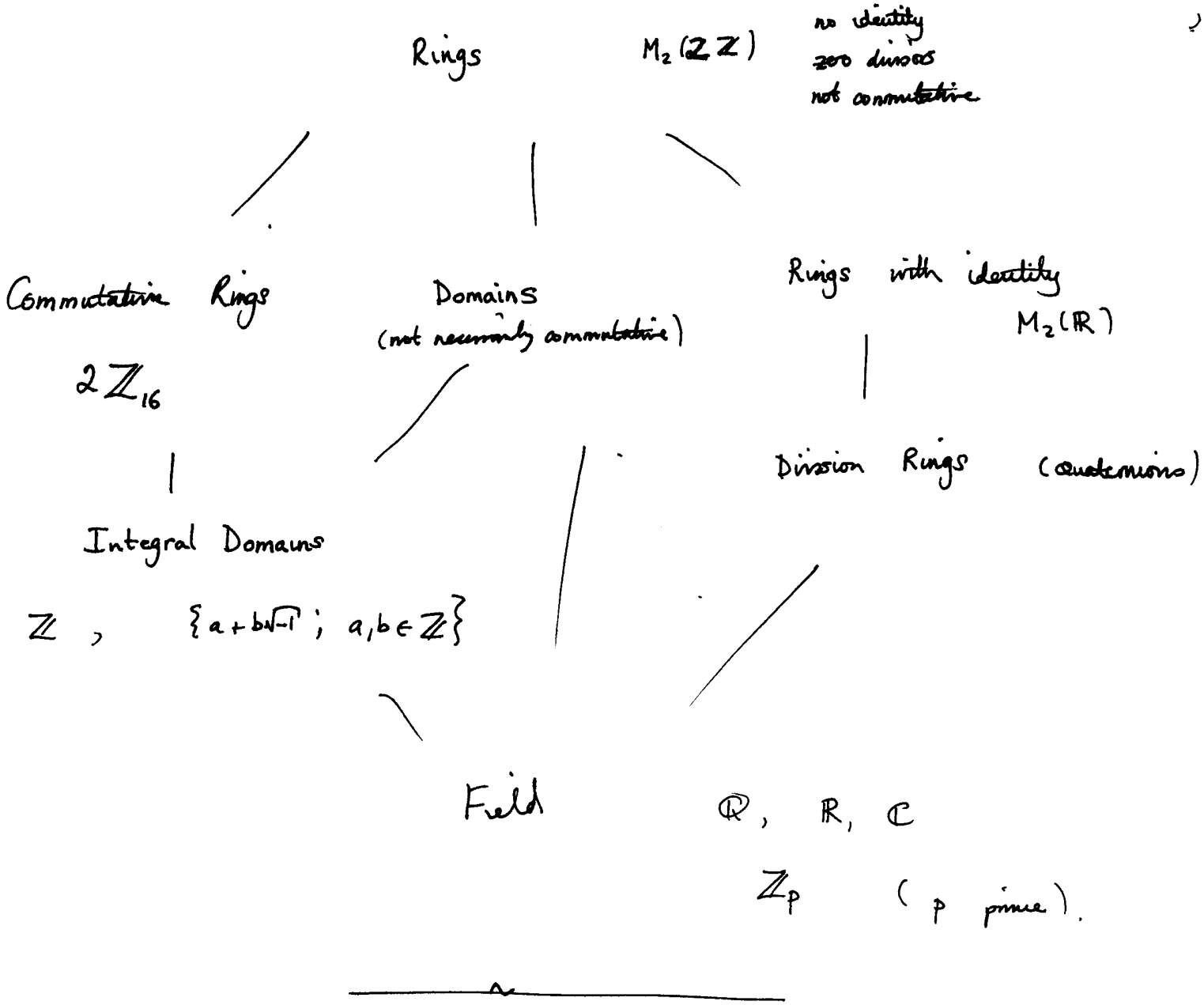
If $(R, +, \cdot)$ is a commutative ring satisfying (M4), then it is an *integral domain*.

(e) Division Rings.

A ring R with a unit is a *division ring* if for all $a \neq 0$ in R, there exists $b \in R$ (written as a^{-1}) such that $a \cdot b = b \cdot a = 1$.

(f) Fields

A ring R is a *field* if it is a commutative division ring



Quaternions: (example of a non-commutative division ring).

Consider $\mathbb{H} = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k : \alpha_i \in \mathbb{R}\}$

subject to: + defined by $(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) + (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k)$

$= (\alpha_0+\beta_0) + (\alpha_1+\beta_1) i + (\alpha_2+\beta_2) j + (\alpha_3+\beta_3) k$

- defined via distributive law using relations

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \ jk = i, \ ki = j$$

Thus $(\alpha_0+\alpha_1 i + \alpha_2 j + \alpha_3 k)(\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k) = (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3)$

$+ (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2) i$

$+ \ldots$

Can check that $(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k)$

$$= \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2,$$

so $A = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ has a multiplicative inverse B with $AB = 1$.

One can then check that $\mathbb{H}$ forms a non-commutative division ring.

Examples.

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with $+$ and $\cdot$ defined mod n.

$n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$ with $+$ and $\cdot$ inherited from $\mathbb{Z}$.

Can check both are rings, and $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.

They are both commutative rings.

- When n is prime, say $n = p$, then $\mathbb{Z}_n$ forms a field: it is commutative and a division ring, since if $a \in \mathbb{Z}_p \setminus \{0\}$, then there exists $b \in \mathbb{Z}_p$ with $ab = 1$ (i.e. $ab \equiv 1 \pmod p$).
This follows from Euclid's Algorithm: $(a, p) = 1$, so there exist $u, v \in \mathbb{Z}$ with $au + pv = 1 \Rightarrow au \equiv 1 \pmod p$.

- When $n = ab$ is composite with $a > 1$ & $b > 1$, then $\mathbb{Z}_n$ has zero divisors, since $ab \equiv 0 \pmod n$.

Examples $M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$ (or any ring).

with matrix $+$, $\times$ forms a ring.

Definition. If R is a ring, then $S \subseteq R$ is a *subring* of R if S is a ring with respect to the operations $+$ and $\cdot$ inherited from R.

Remark. If R is a ring and $S \subseteq R$, then S is a subring if and only if:
(1) $S \neq \emptyset$; (2) for all $a, b \in S$, one has ab, $a \pm b \in S$.

Definition. If $a \in R$ (R a ring) satisfies $a \neq 0$, and there exists $b \in R \setminus \{0\}$ with $ab = 0$, then a is a zero-divisor of R.

Example: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z})$ is a zero divisor, since

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \underline{0} \in M_2(\mathbb{Z}).$$

---

§4.2. Simple Properties.

Lemma 4.2.1. Let R be a ring and let $a, b \in R$. Then

(a) $a0 = 0a = 0$

(b) $a(-b) = (-a)b = -(ab)$

(c) $(-a)(-b) = ab$

(d) If $1 \in R$ then $(-1)a = -a$.

Proof. (a) Since $0 = 0+0$, then $a0 = a(0+0) = a0 + a0 \Rightarrow a0 = 0$.
Similarly $0a = 0$. □

(b) We have $ab + a(-b) = a(b + (-b)) = a0 = 0 \Rightarrow a(-b) = -(ab)$.
Similarly $(-a)b = -(ab)$. □

(c) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

(d) $(-1)a + a = (-1)a + (1)a = (-1+1)a = 0a = 0$. □ //

Lemma 4.2.3 If R is a ring with a 1, ~~without the~~ axiom $a+b=b+a$ for all $a,b \in R$, then R is a ring.

Proof. We have

$$(a+b)(1+1) = (a+b)1 + (a+b)1 = a+b+a+b$$
$$\parallel$$
$$a(1+1) + b(1+1) = a+a+b+b.$$

Then $b+a = a+b$. $\square$.

Boolean Rings. A ring with $x^2 = x$ for all $x \in R$.

Lemma 4.2.4. Boolean Rings are commutative.

Proof. Let $x, y \in R$. Then

$$(x+y)^2 = x+y$$
$$\parallel$$
$$x(x+y) + y(x+y) = x^2 + xy + yx + y^2 = x + xy + yx + y.$$

Then $xy + yx = 0$

$$\Downarrow$$

$$0 = x^2y + xyx = xy + xyx$$
$$\parallel$$
$$xyx + yx^2 = xyx + yx$$

$\Big\}$ $xy + xyx = xyx + yx$ $\Rightarrow$ $xy = yx$.

So R is commutative. //

§ 4.3. Ideals, Homomorphisms and Quotient Rings.

The existence of subrings S of a given ring R should make us consider the potential for analogs of normal subgroups, homomorphisms and their kernels, and quotient (or factor) groups. This all works very nicely, but one should pay attention to minor differences in substance and language!

Definition. Let R and R' be rings. Then $\varphi : R \to R'$ is a **homomorphism** when:

(a) for all $a, b \in R$, one has $\varphi(a+b) = \varphi(a) + \varphi(b)$

(b) for all $a, b \in R$, one has $\varphi(ab) = \varphi(a)\varphi(b)$.

Remember: • $(R, +)$ and $(R', +)$ are (commutative) abelian groups, so φ is a homomorphism of these groups $\leftrightarrow$ (a).

• φ preserves structure with respect to $+$ and $\cdot$.

Definition If $\varphi : R \to R'$ is a homomorphism of rings, then the **kernel** of φ is

$$\ker(\varphi) := \{ x \in R : \varphi(x) = \underset{\uparrow}{0} \}.$$

(some authors would write $0_{R'}$).

Remark: Superficially, the kernel is only concerned with the identity 0 in the additive group $(R, +)$, but the homomorphism φ "knows" about multiplicative structure also. **Note:** Easy to check $\varphi(R)$ is a subring of R'

Easy Example: Let p be a prime, and consider

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_p \quad \text{(integers modulo } p\text{)}$$

defined by $n \longmapsto n \pmod p$ (identified with $\{0, 1, \ldots, p-1\}$).

Then φ is a homomorphism of rings (check – but inherited by what we all know about modular arithmetic), and

$$\ker(\varphi) = \{ n \in \mathbb{Z} : n \equiv 0 \pmod{p} \}$$
$$= \{ mp : m \in \mathbb{Z} \} = p\mathbb{Z}.$$

Note: If $k \in \mathbb{Z}$, then $k \cdot \ker(\varphi) = kp\mathbb{Z} \subseteq p\mathbb{Z}$ — multiplication by k does not change that we have set of multiples of p. This idea generalises:

Definition. Let R be a ring. An ideal of R is a non-empty subset I of R satisfying:

(a) I is an additive subgroup of R

(b) For all $r \in R$ and $a \in I$, one has $ra \in I$ and $ar \in I$.

[I is a subring of R possibly without a unit].

In the example, we see that $p\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

- Property (a) here implies that $I \lhd R$ (I is a normal subgroup of R) as additive groups — why? because $(R,+)$ is abelian
- Property (b) comes from properties of $\cdot$ in R.

The relation $I \lhd R$ as additive groups should suggest:

Lemma 4.3.1 If $\varphi : R \to R'$ is a homomorphism of rings, then $\ker(\varphi)$ is an ideal of R.

Proof: We know from groups that $\ker(\varphi)$ satisfies $\ker(\varphi) \neq \emptyset$ and $\ker(\varphi)$ satisfies property (a) of an ideal (in fact $\ker(\varphi) \lhd R$). For property (b), note that whenever $a \in \ker(\varphi)$, one has $\varphi(a) = 0$, whence for all $r \in R$ one has $\varphi(ar) = \varphi(a)\varphi(r) = 0\,\varphi(r) = 0$,

so $ar \in \ker(\varphi)$, and similarly $ra \in \ker(\varphi)$. //

Note 1: Some authors write $I \lhd R$ to denote I is an ideal of R.

Note 2: Can define left ideal L and right ideal M

$\forall r \in R, a \in L$, have $ra \in L$ $\forall r \in R, a \in M$, have $ar \in M$.

In the easy example, have $p\mathbb{Z} = \ker(\varphi) \lhd \mathbb{Z}$.

Since ideals are analogues of normal subgroups, this motivates the definition of a set of cosets (for $K \lhd R$):

$$R/K = \{ a + K : a \in R \}.$$

↑ remember K is an additive subgroup of R.

But we need to check that addition and multiplication can be defined respecting ring axioms & this is going to form a ring (analogous to quotient (factor) group G/N when $N \lhd G$).

Theorem 4.3.2. Let R be a ring and K an ideal of R. The additive (quotient) group R/K is a ring when endowed with multiplication defined by

$$(a + K)(b + K) = ab + K.$$

Moreover, the map $\varphi : R \longrightarrow R/K$ is a homomorphism

$$a \longmapsto a + K$$

of R onto R/K with $\ker(\varphi) = K$.

Thus $R/K = \mathrm{Im}(\varphi)$.

Proof: There are two things to check here:

(1) We know from (additive) groups that addition is well-defined on R/K, but need to check multiplication well-defined.

Suppose $a+K = a'+K$ and $b+K = b'+K$. Then $a-a' \in K$ and $b-b' \in K$, so $(a-a')b \in K$ and $a'(b-b') \in K$ (ideal property)

$$\Rightarrow \quad \begin{array}{c} (a-a')b + a'(b-b') \in K \\ \| \\ ab - a'b + a'b - a'b' \\ \| \\ ab - a'b' \end{array} \Rightarrow \quad ab + K = a'b' + K,$$

So multiplication well-defined (ie. independent of coset representatives). □

[Notice analogy with "congruence modulo p" $\longleftrightarrow$ "congruence modulo K"].

(2) We still need to prove that R/K is a ring — this is a consequence of the second assertion that $\varphi : R \to R/K$, $a \mapsto a+K$ is a surjective homomorphism

To check the latter, observe that the additive property of homomorphism follows from group theory, and for all $a, b \in R$ we have

$$\varphi(ab) = ab + K = (a+K)(b+K) = \varphi(a)\varphi(b). \checkmark$$

Moreover, one has $\ker(\varphi) = \{a \in R : \varphi(a) = \underset{R/K}{0}\} = \{a \in R : a+K = K\}$

$$= \{a \in R : a \in K\} = K.$$

Plainly, also, the map φ is surjective. Since $R/K = \varphi(R)$, we have that R/K is a ring. □ //

Back to easy example: Recall that $p\mathbb{Z} \lhd \mathbb{Z}$.

Then the quotient group $\mathbb{Z}/p\mathbb{Z}$ (as an additive group) forms a ring under multiplication modulo p: $(a+p\mathbb{Z})(b+p\mathbb{Z}) = ab+p\mathbb{Z}$.

Moreover, one has $\varphi(\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$ when

$$\varphi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$
$$a \mapsto a+p\mathbb{Z}.$$

There is the usual Greek lexicon of types of morphisms, especially:

homomorphism – done!
isomorphism – a bijective homomorphism.
automorphism – an isomorphism from R to R.

Also: R is isomorphic to R' when there exists an isomorphism $\varphi : R \to R'$ as rings.

Not surprisingly, there are analogues of (group) homomorphism theorems:

Theorem 4.3.3. (First Homomorphism Theorem).

Let $\varphi : R \longrightarrow R'$ be a surjective homomorphism of rings with $\ker(\varphi) = K$. Then $R' \cong R/K$, and indeed the map

$$\begin{aligned} \psi : R/K &\longrightarrow R' \\ a+K &\longmapsto \varphi(a) \end{aligned}$$

defines an isomorphism.

Proof. Most of the work is done by the First Homomorphism of group theory. The map ψ is thus well-defined, surjective, injective, and the additive part of the homomorphism property holds. We need only check now that for all $a, b \in R$ one has

$$\psi((a+K)(b+K)) = \psi(ab+K) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(a+K)\psi(b+K)$$

to see that ψ is an isomorphism, and thus $R' \cong R/K$. //

Back to the simple example: Have $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_p$

$$n \longmapsto n \pmod p$$

$$\ker(\varphi) = p\mathbb{Z}.$$

Then from First Homomorphism Theorem, we have

$$\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}.$$

[In fact, many mathematicians would only ever write down $\mathbb{Z}/p\mathbb{Z}$ for the ring of integers modulo p].

Analogues of the remaining Homomorphism theorems are no more difficult to prove, as you can check yourselves:

Theorem 4.3.4. (Correspondence Theorem) Let $\varphi : R \to R'$ be a surjective homomorphism of rings with $\ker(\varphi) = K$.

Given $I' \lhd R'$ define

$$I = \{ a \in R : \varphi(a) \in I' \} \quad \left(= \varphi^{-1}(I') \right).$$

Then $K \subseteq I \lhd R$ and $I' \cong I/K$.

Define $$A + I = \{ a + i : a \in A \text{ and } i \in I \}.$$

Theorem 4.3.5. (Second Homomorphism Theorem). Suppose that A is a subring of R and $I \lhd R$. Then $A + I$ is a subring of R with $I \lhd A + I$ and satisfies

$$(A+I)/I \cong A/(A \cap I).$$

Theorem 4.3.6. If $K \lhd R$ and $I \lhd R$ with $I \supseteq K$, then $R/I \cong (R/K)/(I/K)$.

Variant on Easy Example: Consider p a prime,

$$R = \mathbb{Z}, \quad K = p^2\mathbb{Z}, \quad I = p\mathbb{Z}.$$

Then $p^2\mathbb{Z} \lhd \mathbb{Z}$, $p\mathbb{Z} \lhd \mathbb{Z}$, $p\mathbb{Z} \supseteq p^2\mathbb{Z}$ (possibly confusing to class!)

and $$\mathbb{Z}/p\mathbb{Z} \cong (\mathbb{Z}/p^2\mathbb{Z}) \Big/ (p\mathbb{Z}/p^2\mathbb{Z}).$$

More examples:

(a) Fields F (important). Of course, as is the case for all rings, the trivial subring $\{0\}$ is an ideal.

If $I \neq \{0\}$ is an ideal of F, so $a \in I \setminus \{0\}$, then $a^{-1} \in F$, whence $1 = a^{-1}a \in I$. But then, whenever $r \in F$ we have $r = r \cdot 1 \in I \Rightarrow I = F$. Thus the only ideals of F are $\{0\}$ and F.

Consequence: Suppose that $\varphi : F \to R$ is a homomorphism of rings, and F is a field. Then either φ is trivial, or $F \cong R$. For $\ker(\varphi) \lhd F$, so $\ker(\varphi) = \{0\}$ or $\ker(\varphi) = F$. In the latter case the map is trivial, and in the former case φ is a bijective homomorphism.

(b) Commutative Rings R with 1.

If $a \in R$, then $\langle a \rangle = \{xa : x \in R\}$ forms an ideal of R.

For whenever $w, z \in \langle a \rangle$, there exist $u, v \in R$ with $w = ua, z = va$, whence

$$w \pm z = ua \pm va = (u \pm v)a \in \langle a \rangle,$$

and for all $r \in R$ we have for all $w \in \langle a \rangle$, (that $w = ua$ some $u \in R$)

$$rw = r(ua) = (ru)a \in \langle a \rangle.$$

Then $\langle a \rangle \lhd R$.

Example: $6\mathbb{Z} = \langle 6 \rangle \lhd \mathbb{Z}$

Check: If $R = \{a + b\sqrt{-1} : a, b \in \mathbb{Z}\}$ with obvious addition and multiplication, then $\langle 1 + \sqrt{-1} \rangle \lhd R$.

(C) A polynomial example.

Consider the set $\mathbb{R}[t]$ of real polynomials

$$\{ a_0 + a_1 t + \cdots + a_n t^n : \ n \geq 0, \ a_m \in \mathbb{R} \},$$

and

$$\begin{aligned} \varphi : \mathbb{R}[t] &\longrightarrow \mathbb{C} \\ t &\longmapsto \sqrt{-1} = i. \end{aligned}$$

Can check $\ker(\varphi) = \{ f(t) \in \mathbb{R}[t] : f(\sqrt{-1}) = 0 \}$

$= \{ f(t) \in \mathbb{R}[t] : t^2+1 \text{ is a factor of } f \}$

$t^2+1 = (t+\sqrt{-1})(t-\sqrt{-1})$

↑ ↗

both give roots of f by complex conjugation.

Then φ is a surjective homomorphism, using $\varphi(a+bt) = a+b\sqrt{-1}$, and checking the homomorphism properties. Then

$$\mathbb{C} \cong \mathbb{R}[t] / \langle t^2+1 \rangle,$$

where $\langle t^2+1 \rangle$ is the ideal $(t^2+1)\mathbb{R}[t]$.

We'll see more on this kind of example later!

§ 4·4. Maximal Ideals.

We saw in example (a) concerning fields that the only ideals of a field F are $\{0\}$ and F. (in a sense, fields are "simple" rings). This property in fact characterises fields: (necessary to be a field)

Lemma 4·4·1. Let R be a commutative ring with 1 whose only ideals are $\{0\}$ and R. Then R is a field.

Proof. This is a nice application of properties of ideals. We need to show that each $a \in R \setminus \{0\}$ has a multiplicative inverse a^{-1}. But $\langle a \rangle = \{ xa : x \in R \} \lhd R$, so $\langle a \rangle = \{0\}$ or $\langle a \rangle = R$. Since $a = 1a \in \langle a \rangle$, we must have $\langle a \rangle = R$, whence $1 = xa$ for some $x \in R$, so a has a multiplicative inverse. //

The correspondence theorem shows that if $\varphi : R \to R'$ is a surjective homomorphism of rings, then the ideals of R' are in 1-1 correspondence with ideals of R containing $\ker(\varphi)$.

Thought experiment: Suppose that $\ker(\varphi)$ is maximal in the sense that there are no ideals I with $\ker(\varphi) \subsetneq I \subsetneq R$.

Then R' has as ideals only the trivial ideals $\{0\}$ and R'.

If R' is commutative with 1, then R' is a field.

But then R is a ring that "simplifies" under the action of φ to a field, so presumably is easier to understand.

Definition If $M \lhd R$ satisfies $\{0\} \subsetneq M \subsetneq R$ and, whenever $I \lhd R$ and $M \subseteq I \subseteq R$ one has $I = M$ or $I = R$, say M is maximal ideal.

Worth pausing to digest this definition:

Big theorem for today about commutative rings with a 1.

Theorem 4.4.2/3 Let R be a commutative ring with a 1, and let $M \triangleleft R$. Then

R/M is a field if and only if M is a maximal ideal of R.

Proof. ($\Rightarrow$) Since R/M is a field, the only ideals of R/M are $\{0\}$ and R/M (see example (a) from earlier). Consider the surjective homomorphism (canonical) $\varphi : R \to R/M$, $a \mapsto a+M$. Then by the correspondence theorem, one has that there is no ideal I intermediate between $\ker(\varphi) = M$ and R, so M is a maximal ideal of R. □

($\Leftarrow$) Suppose that M is a maximal ideal of R, and consider the same map φ as above. The ring R/M has $1+M$ as its unit, so is a commutative ring with unit. But M is maximal, so there is no ideal I between M and R, so by the correspondence theorem, there is no ideal between $\{0\}$ and R/M in R/M. Thus (Lemma 4.4.1) the ring R/M is a field. □ //

Examples (a) Consider $\mathbb{Z}$ and the ideal $n\mathbb{Z}$.

• If $n = ab$, then $n\mathbb{Z} \lhd b\mathbb{Z} \lhd \mathbb{Z}$, so whenever n is composite (not prime) one sees that $n\mathbb{Z}$ is not a maximal ideal of $\mathbb{Z}$, so $\mathbb{Z}/n\mathbb{Z}$ is not a field.

• If $n = p$ with p prime, then whenever I is an ideal of $\mathbb{Z}$ with $p\mathbb{Z} \lhd I \lhd \mathbb{Z}$, we must have $I = m\mathbb{Z}$ with $m \mid p$, so $m = 1$ or p, and hence $I = p\mathbb{Z}$. Thus $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, and $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ is a field.

Notice: $\mathbb{Z}_9$ does not form a field.

But (fact) there is a finite field of p^n elements for all $n \geq 1$ and all primes p — and no other finite fields.

Example (b) Consider the ring $R = \mathbb{Z}_3[t]$, consisting of polynomials $a_0 + a_1 t + \cdots + a_n t^n$, with $n \geq 0$ and $a_i \in \{0,1,2\}$, with addition and multiplication defined modulo 3.

One ideal is $I = \langle t \rangle = tR$, the set of all such polynomials with 0 constant term. One has $R/I = \{a + tR : a \in R\}$ $= \{a + tR : a \in \mathbb{Z}_3\} \cong \mathbb{Z}_3$, a field having 3-elements.

Another ideal is $J = \langle t^2+1 \rangle = (t^2+1)R$. In this case $R/J = \{a + (t^2+1)R : a \in R\} = \{(c+dt) + (t^2+1)R : c,d \in \mathbb{Z}_3\}$.

How does multiplication work in R/J? We have

$$((a+bt) + (t^2+1)R)((c+dt) + (t^2+1)R) = ((ac-bd) + (bc+ad)t + bd(t^2+1)) + (t^2+1)R$$

$$= \big((ac-bd)1 + (bc+ad)t + (t^2+1)R\big),$$

so it is almost as if t behaves like $\sqrt{-1}$ in R/J. This is not so surprising, given that $(t^2+1)1 + (t^2+1)R = (t^2+1)R$ is the 0-element in R/J.

Suppose $x \in R/J$ is non-zero, say $x = (a+bt)+(t^2+1)R$ with $(a,b) \neq (0,0)$. Then $a^2+b^2 \not\equiv 0 \pmod 3$ [check: 1^2+1^2, 1^2+2^2, 0^2+1^2, 2^2+2^2 are all non-zero modulo 3]. But then

$$\left(\frac{a-bt}{a^2+b^2} + (t^2+1)R\right)\big((a+bt) + (t^2+1)R\big) = \left(\frac{a^2-b^2t^2}{a^2+b^2} + (t^2+1)R\right)$$

$$= \frac{a^2+b^2}{a^2+b^2} + \frac{b^2(t^2+1)}{a^2+b^2} + (t^2+1)R$$

$$= 1 + (t^2+1)R,$$

so that x has a multiplicative inverse in R/J. Then R/J is a field having $3 \times 3 = 9$ elements, and

(3 = # choices for a; 3 = # choices for b)

hence $J = \langle t^2+1 \rangle$ is a maximal ideal.

The first field $\mathbb{Z}_3 \cong R/I$ is usually written $\mathbb{F}_3$ in modern text-books, and the second field R/J is usually written $\mathbb{F}_9$ (but one must take care with issues about other fields that might have 9 elements — isomorphisms...!)

What made this example work, by the way, is that the polynomial congruence $t^2+1 \equiv 0 \pmod 3$ has no solutions, and further t^2+1 does not factorise over $\mathbb{Z}_3$.

§4.5. Polynomial Rings.

The last example motivates a more serious discussion of polynomials whose coefficients are elements of a ring R. The theory is simplest when R is a field F, and here it is good to keep in mind

$\mathbb{Z}$ analogous to $F[x]$

$= \{a_0 + a_1 x + \cdots + a_n x^n : n \geq 0,\ a_i \in F\}$

Dictionary

a_i are "coefficients".

(a) $F[x]$ forms a commutative ring with unit.

Consider $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$ and $q(x) = b_0 + b_1 x + \cdots + b_m x^m \in F[x]$ with $n \geq m \geq 0$, say.

- $p(x) = q(x)$ if and only if $a_0 = b_0, a_1 = b_1, \ldots, a_m = b_m$, and $a_j = 0$ for $j > m$.
- $p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_n x^n \in F[x]$
- $p(x)q(x) = c_0 + c_1 x + \cdots + c_r x^r \in F[x]$, where for $0 \leq i \leq n+m$,

$$c_i = a_i b_0 + a_{i-1} b_1 + \cdots + a_1 b_{i-1} + a_0 b_i \in F,$$

and adopt convention $a_i = 0$ for $i > n$, $b_j = 0$ for $j > m$.

- Additive identity 0.
- Additive inverses $-p(x) = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n$.
- Associativity, Commutativity } of addition inherited from F.
- Multiplicative unit 1

- $p(x)\,q(x) = q(x)\,p(x)$ for all $p, q \in F[x]$, so commutative.

Upshot: When F is a field, then $F[x]$ is a commutative ring with a unit.

More is true, but this requires additional work.

Polynomials in $F[x]$ come equipped with a measure of size analogous to $|n|$ for $n \in \mathbb{Z}$.

Definition. Suppose that $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$ (as we may assume without loss of generality). Then the degree of $p(x)$, written $\deg(p)$ or $\deg p(x)$, is n.
[By convention, we put $\deg(0) = -\infty$.]

Example. Consider $3x^2 + 2 \in \mathbb{Z}_5[x]$. One has

$$\deg(3x^2+2) = 2$$
$$\deg(2) = 0$$

Careful: $\deg(5x^2+2x) \neq 1$. One should be careful about writing this, since $5 \equiv 0 \pmod 5$, so strictly speaking $5 \notin \mathbb{Z}_5$. The appropriate object to write down is $0x^2+2x$, and $\deg(0x^2+2x) = 1$.

Exercise. One has $\deg(p(x)+q(x)) \leq \max\{\deg p(x), \deg q(x)\}$

$$\deg(p(x)\,q(x)) = \deg p(x) + \deg q(x).$$

[Compare $\log(ab) = \log a + \log b$].

Lemma 4.5.4. When F is a field, the ring $F[x]$ is an integral domain.

Proof. We know already that $F[x]$ is a commutative ring with a unit. It remains to show that whenever $p(x)q(x)=0$, then either $p(x)=0$ or $q(x)=0$. But if $p(x)q(x)=0$, then

$$-\infty = \deg(0) = \deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)),$$

whenever this makes sense. If $\deg p(x) \geq 0$ and $\deg q(x) \geq 0$, this is impossible. So $p(x)q(x)=0$ if and only if $\deg(p) = -\infty$ or $\deg(q) = -\infty$, in which case $p(x)=0$ or $q(x)=0$. //

We are now equipped to consider the arithmetic of polynomial rings analogous to that of $\mathbb{Z}$, developing divisibility, congruences, and so on. An important stepping stone in this direction is:

Theorem 4.5.5 (Division Algorithm).

Suppose that $f(x), g(x) \in F[x]$, and that $g(x) \neq 0$. Then

$$f(x) = q(x)g(x) + r(x),$$

where $q(x)$, $r(x) \in F[x]$, and $r(x) = 0$ or
"quotient" "remainder"

$$\deg r(x) < \deg g(x).$$

Proof. If $\deg f(x) < \deg g(x)$ or $f(x) = 0$, then take $q(x)=0$ and $r(x) = f(x)$, and we're done. □

Otherwise we may suppose that $\deg f(x) \geq \deg g(x)$, say

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m$$
$$g(x) = b_0 + b_1 x + \cdots + b_n x^n \quad \text{(with } m \geq n \geq 0\text{)}.$$

$a_m \neq 0$, $b_n \neq 0$.

We proceed by induction, supposing that the conclusion has been proved for all $M < M$, for some $M \geq 1$, and seek to prove the desired conclusion for $m = M$. Given polynomials as above, we have

$$f(x) - \frac{a_m}{b_m} x^{m-n} g(x) = \left(a_{m-1} - \frac{a_m}{b_n} b_{n-1}\right) x^{m-1} + \cdots + \left(a_{m-n} - \frac{a_m}{b_n} b_0\right) x^{m-n} + a_{m-n-1} x^{m-n-1} + \cdots + a_1 x + a_0$$

$$\in F[x]$$

$$= h(x), \text{ say},$$

where $\deg(h(x)) \leq m-1 < \deg(f(x))$. Thus, by the inductive hypothesis, one has

$$h(x) = q_1(x)\, g(x) + r_1(x),$$

where $q_1(x), r_1(x) \in F[x]$ and $r_1(x) = 0$ or $\deg r_1(x) < \deg g$.

But then

$$f(x) = \left(\frac{a_m}{b_m} x^{m-n} + q_1(x)\right) g(x) + r_1(x)$$

$$= q(x)\, g(x) + r_1(x), \text{ say},$$

where $q(x), r_1(x) \in F[x]$ and $\deg r_1(x) < \deg g(x)$ or $r_1(x) = 0$. But this confirms the inductive hypothesis for $M = m$, and the conclusion follows. //

The situation in which $f(x) = q(x)\, g(x) + r(x)$ with $r(x) = 0$ has special significance, for then $f(x) = q(x)\, g(x)$ and hence $f(x) \in g(x) F[x] = \langle g(x) \rangle$ and $f(x)$ is "divisible" by $g(x)$. This line of thinking leads to analogues of prime factorisations, as we shall see in the coming classes.

Theorem 4.5.6. Suppose that $I \neq \langle 0 \rangle$ is an ideal of $F[x]$. Then $I = \{ f(x)\, g(x) : f(x) \in F[x] \}$ for some polynomial $g(x) \in F[x]$.

Proof. The theorem claims that all polynomials in I are multiples of a polynomial $g(x)$, and hence that all polynomials in I have degree at least $\deg(g(x))$. This suggests defining

$$d = \min \{ \deg(h(x)) : h(x) \in I \ \& \deg h(x) \geq 0 \} \geqslant 0$$

and taking $g(x)$ to be any polynomial of degree d. It then remains to show that whenever $h(x) \in I$ then $h(x) = f(x)g(x)$ for some $f \in F[x]$. By the division algorithm, we have $h(x) = q(x)g(x) + r(x)$, with $q(x) \in F[x]$, $r(x) \in F[x]$ and $\deg(r(x)) < \deg(g(x))$. But then

$$r(x) = h(x) - q(x)g(x) \in I \quad (\text{since } h, g \in I).$$

The minimality of $\deg g(x)$ then implies that $r(x) = 0$, whence $h(x) = q(x)g(x)$. Hence all elements of I are multiples of $g(x)$. //

Definition: A **principal ideal domain** (PID) is an integral domain R satisfying the condition that whenever I is an ideal of R, then $I = \langle a \rangle = \{ xa : x \in R \}$ for some $a \in I$.

[$\exists$ R a PID: $I \triangleleft R$ is generated by a single element].

Thus, whenever F is a field, then $F[x]$ is a PID.

Notice that the generator of an ideal need not be unique:

$$(x^2 + 2) \in \mathbb{F}_3[x], \quad (\text{principal})$$

$$\| \\ (2x^2 + 1)$$

But this can be resolved by focusing on monic polynomials with lead coefficient 1.

If $I \trianglelefteq F[x]$ and $(p(x)) = I = (\overbrace{x^n + a_{n-1}x^{n-1} + \cdots + a_0}^{m(x)})$,

then $p(x) = c(x^n + a_{n-1}x^{n-1} + \cdots + a_0)$, where c is the lead coefficient of $p(x)$. Thus monic generators of principal ideals are unique.

To see this, note that $p(x) \in (m(x))$, so $p(x) = c(x^n + \ldots + a_0)$ for some $c \in F$.

We are now equipped to develop notions analogous to divisibility, gcds, factorisation and congruences.

Definition: (a) When $f, g \in F[x]$ and $g \neq 0$, we say $g(x)$ divides $f(x)$, and write $g(x) \mid f(x)$, when $f(x) = a(x)g(x)$ for some $a(x) \in F[x]$.

(b) The greatest common divisor of $f(x)$ and $g(x)$ is the monic divisor $d(x) \in F[x]$ of both $f(x)$ and $g(x)$ divisible by all other such common divisors.

[Thus $\gcd(f(x), g(x))$ · (written (f, g)) is the polynomial $d(x)$ satisfying: $d(x) \mid f(x)$ & $d(x) \mid g(x)$, and $d(x)$ monic, and $\deg(d(x))$ maximal amongst all common divisors of f and g.].

Theorem 4.5.7. (Analogue of correctness of Euclid's Algorithm). Let $f(x), g(x) \in F[x]$, and suppose that $g(x) \neq 0$. Then $d(x) = (f(x), g(x))$ exists, and there exist $a(x), b(x) \in F[x]$ such that $d(x) = a(x)f(x) + b(x)g(x)$.

Proof. We use ideals to establish this result — and Theorem 4.5.6.

Let

$$I = \{ uf + vg : u, v \in F[x] \}.$$

We claim that $I \trianglelefteq F[x]$. To check that this is the case, note that whenever $a, b \in I$, say $a = u_1 f + v_1 g$ and $b = u_2 f + v_2 g$, then $a + b = (u_1 + u_2)f + (v_1 + v_2)g \in I$, and for all $t \in F[x]$

one has $t(u_1 f + v_1 g) = (tu_1) f + (tv_1) g \in I$. So $I \trianglelefteq F[x]$.

Since $g \in I$, we have $I \neq 0$.

Now we apply Theorem 4.5.6: since $0 \neq I \trianglelefteq F[x]$, we have $I = \langle d(x) \rangle$ for some unique monic polynomial $d \in F[x]$. Then $f(x)$ and $g(x)$ are multiples of $d(x)$, since $f, g \in I$. Thus $d(x) | f(x)$ and $d(x) | g(x)$, so d is a common divisor of f and g.

The definition of I now shows that $d(x) = u(x) f(x) + v(x) g(x)$ for some $u, v \in F[x]$. Thus, whenever $h(x) | f(x)$ and $h(x) | g(x)$, we have $h(x) | d(x)$, so that d is the greatest common divisor of $f(x)$ and $g(x)$. //

Notice that this gcd is unique: d is monic, so if $d_1(x)$ and $d_2(x)$ are two such common divisors we have $d_1 | d_2$ and $d_2 | d_1 \Rightarrow d_1 = d_2$.

Definition We say $f(x), g(x) \in F[x]$ are relatively prime when $(f(x), g(x)) = 1$.

Thus $f(x)$ and $g(x)$ are relatively prime if and only if there exist $u(x), v(x) \in F[x]$ s.t. $uf + vg = 1$.

($(\Rightarrow)$ is Theorem 4.5.7; $(\Leftarrow)$ if $d | f$ & $d | g$ then $d | (\ldots)$ $\square$)

Lemma 4.5.10. Suppose that $(q(x), f(x)) = 1$ and $q(x) | f(x) g(x)$. Then $q(x) | g(x)$.

Proof. We have that there exist $a, b \in F[x]$ s.t. $af + bq = 1$.

Thus $g = a(fg) + b(qg)$, so $q | g$. //

($a(fg)$: div by $q(x)$)

This conclusion helps to derive an analogue of a prime factorization.

Definition. We say $p(x) \in F[x]$ is irreducible if (i) $\deg p \geq 1$, and (ii) whenever $f \in F[x]$, one has $p | f$ or $(p, f) = 1$.

Consequence: p is irreducible $\Leftrightarrow$ there do not exist $f, g \in F[x]$ such that $\deg f \geq \deg g \geq 1$ and $p = fg$.

($\Rightarrow$) Suppose p irreducible and $p = fg$ with $\deg f \geq \deg g \geq 1$. Then either $p \mid f$ or $(p, f) = 1$, in which case $p \mid g$. But then $\deg(p) \geq \deg(p) + \min\{\deg f, \deg g\} > \deg(p)$. $\#$. So there do not exist $f, g \in F[x]$ s.t. $p = fg$, and $\deg f \geq \deg g \geq 1$. □

($\Leftarrow$) Suppose $p(x)$ cannot be written as $p = fg$ with $\deg f \geq \deg g \geq 1$, and yet $\deg p \geq 1$. Suppose that $h \in F[x]$. Then either $(p, h) = 1$, or else $(p, h) = cp$ for some $c \in F$. Then $(p, h) = 1$ or $p \mid h$, so p is irreducible. □ //

Lemma 4.5.10a. Suppose that $p \in F[x]$ and p is irreducible. Then whenever $p \mid a_1 a_2 \cdots a_k$, with $a_i \in F[x]$, one has $p \mid a_i$ for some index i.

Proof. We proceed inductively, noting that the conclusion is trivial for $k = 1$. Suppose that the conclusion has been proved for $1 \leq k < K$ with $K \geq 2$, and that $p \mid a_1 a_2 \cdots a_K$. Then $p \mid (a_1 \cdots a_{K-1}) a_K$, so either $p \mid a_K$ or $p \mid a_1 \cdots a_{K-1}$, whence the inductive hypothesis shows $p \mid a_i$ some i. This completes the induction. //

Analogue of the Fundamental Theorem of Arithmetic.

Theorem 4.5.12: Suppose that $f(x) \in F[x]$ has degree at least 1. Then $f(x)$ is the product of irreducible polynomials in $F[x]$, and this product is unique in the following sense. One has

$$f(x) = c\, p_1(x)^{m_1} p_2(x)^{m_2} \cdots p_k(x)^{m_k},$$

where c is the leading coefficient of f, the polynomials $p_1(x), \ldots, p_k(x)$ are distinct, monic and irreducible in $F[x]$, and the integers $m_1, \ldots, m_k$ are positive, and up to reordering of the p_i, the tuples $\underline{m}$ and $\underline{p}$ are unique.

Proof. We proceed by induction on $n = \deg(f)$. When $\deg(f) = 1$, we have $f(x) = ax + b$ for some $a, b \in F$, and thus $f(x) = a(x + b/a)$ with $x + b/a$ irreducible. □

Now suppose that the conclusion holds whenever $\deg(f) < n$, with $n \geq 2$. If $f(x)$ is irreducible, we are done. Otherwise, we have $f(x) = a(x)b(x)$, some $a, b \in F[x]$ with $\deg(b) \geq \deg(a) \geq 1$ and $\deg(b) < \deg(f)$. By induction, both a and b factor into a product of irreducibles, and so therefore does f. This completes the inductive step showing that f factors as a product of irreducibles. □

Now we consider the uniqueness claim. Suppose that f has two representations of the claimed type. Say

$$c\, p_1(x)^{m_1} p_2(x)^{m_2} \cdots p_k(x)^{m_k} = f(x) = c'\, p_1'(x)^{m_1'} p_2'(x)^{m_2'} \cdots p_{k'}'(x)^{m_{k'}'};$$

with p_i, p_i' monic and irreducible, $m_i, m_i' \in \mathbb{N}$ and $c, c' \in F$. Then we have $p_k(x) \mid c'\, p_1'(x)^{m_1'} \cdots p_{k'}'(x)^{m_{k'}'}$, whence $p_k(x) \mid p_i'(x)$ for some index i. But q_i is monic and irreducible, so $p_k(x) = p_i'(x)$. Dividing left and right hand sides by $p_k(x) = p_i'(x)$, we find that $f(x)/p_k(x)$ has two factorizations as a product of irreducibles. But $\deg(f(x)/p_k(x)) < \deg f(x)$, so by induction we see that $f(x)/p_k(x)$ and hence also $f(x)$ have unique factorization.

One can use these ideas to develop arithmetic over $F[x]$. For example (Fact) if F is a finite field having p (a prime) elements, then $\operatorname{card}\{f(x) \in F[x] : \deg(f) \leq n,\ f \text{ monic},\ f \text{ irreducible}\}$ is approximately p^n/n. Analogous to Prime Number Theorem $\#\{\text{primes } p \leq x\} \sim x/\log x$. $[x \leftrightarrow p^n]$.

Irreducible polynomials can be used to generate new fields:

Theorem 4.5.11. Suppose that $p(x) \in F[x]$. Then $(p(x))$ is a maximal ideal of $F[x]$ if and only if $p(x)$ is irreducible over $F[x]$.

Proof. ($\Leftarrow$) Suppose $p(x)$ is irreducible over $F[x]$. We try to show that $(p(x))$ is a maximal ideal of $F[x]$ by considering what it means for some other ideal N to satisfy $(p(x)) \subseteq N$. But $N = (f(x))$ for some $f \in F[x]$, and since $p(x) \in (p(x)) \subseteq N$, we have $p(x) = a(x)f(x)$ for some $a \in F[x]$. By the irreducibility of p, we see that either a or f is constant, whence $f(x) = a^{-1}p(x)$ for some $a \in F \setminus \{0\}$, or $f(x) = f_0 \in F$. In the first case we have $f(x) \in (p(x))$, so $N \subseteq (p(x))$, which yields $N = (p(x))$. In the second case we have $1 = f_0^{-1} f_0 \in (f(x))$, whence $g(x) \in (f(x))$ for all $g \in F[x]$, yielding $(f(x)) = F[x]$. Hence $(p(x))$ is a maximal ideal, since whenever $(p(x)) \subseteq N$, we have $N = (p(x))$ or $N = F[x]$. □

($\Rightarrow$) Suppose that $(p(x))$ is a maximal ideal of $F[x]$. Suppose, by way of deriving a contradiction, that $p(x) = f(x)g(x)$ with $\deg f \geq \deg g \geq 1$. Let $N = (f(x))$. Then we have $p(x) \in N$, since $p(x) = g(x) \cdot f(x)$, and thus $(p(x)) \subseteq N$. By the maximality of the ideal $(p(x))$, it follows that $N = (p(x))$ or $N = F[x]$. The latter is impossible, since $N = (f(x))$, and hence $N = (p(x))$. But then $f(x) \in (p(x))$, which implies that $f(x) = u(x)p(x)$ for some $u \in F[x]$. Hence $p(x) = f(x)g(x) = u(x)g(x)p(x)$ ⁂ since then $\deg(p) = \deg(p) + \deg(u(x)g(x)) > \deg(p)$. Thus $p(x)$ must be irreducible over $F[x]$. □ //

This conclusion has the consequence that

$F[x]/(p(x))$ is a field if and only if $p(x)$ is irreducible.

Note that if $p(x)$ is irreducible of degree d, then

$$F[x]/(p(x)) = \{ a_0 + a_1 * + \cdots + a_{d-1} *^{d-1} + (p(x)) : a_i \in F \}$$

Here, the element $* + (p(x))$ "solves" $p(x)$, since

$$p(x + (p(x))) = p(x) + (p(x)) = (p(x)),$$

which is the zero element in $F[x]/(p(x))$.

Notice that, since there are infinitely many (monic) irreducible polynomials over $F[x]$ (this is an exercise), we can find infinitely many fields of the shape $F[x]/(p(x))$, (can take $\deg p > 1$ when F is not "algebraically closed").

We have used the division algorithm (which can be used to generate the Euclidean Algorithm) to establish results on divisibility in $F[x]$. This is not the only route, but it is convenient algorithmically when available. This motivates:

Definition. An integral domain R is called a Euclidean ring when there exists a function $d : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ satisfying:

(i) For all $a, b \in R \setminus \{0\}$, one has $d(a) \leq d(ab)$;

(ii) Whenever $a, b \in R \setminus \{0\}$, there exist $q, r \in R$ such that $b = qa + r$, where $r = 0$ or $d(r) < d(a)$.

Examples: $\mathbb{Z}$, $F[x]$, $\mathbb{Z}[\sqrt{-1}] = \{ a + b\sqrt{-1} : a, b \in \mathbb{Z} \}$

$d(a + b\sqrt{-1}) = a^2 + b^2$

Non-example: $\mathbb{Z}[\sqrt{-5}]$.

§4.6. More on polynomials: $\mathbb{Q}[x]$.

We develop the theory of (irreducible) polynomials further in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. Our first goal is to show that irreducibility over $\mathbb{Z}[x]$ is sufficient to guarantee irreducibility over $\mathbb{Q}[x]$.

Definition. A **primitive polynomial** $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is a polynomial in which $(a_n, a_{n-1}, \ldots, a_0) = 1$.

Theorem 4.6.3. (Gauss' Lemma). Let $f(x) \in \mathbb{Z}[x]$ be a primitive polynomial, and suppose that $f(x) = A(x)B(x)$, where $A(x), B(x) \in \mathbb{Q}[x]$. Then there exist primitive polynomials $a(x), b(x) \in \mathbb{Z}[x]$ for which $f(x) = a(x)b(x)$, where $\deg(a) = \deg(A)$ and $\deg(b) = \deg(B)$.

Proof. Let $f(x) \in \mathbb{Z}[x]$ be primitive of degree at least 2, for otherwise there is nothing to prove. Suppose that $f(x) = A(x)B(x)$, where $A(x), B(x) \in \mathbb{Q}[x]$. By considering the least common multiple of the denominators of the coefficients of $A(x)$, we can write

$$A(x) = \frac{u_1}{v_1}\, a(x),$$

where $a(x) \in \mathbb{Z}[x]$ is primitive and $u_1, v_1 \in \mathbb{Z}$ satisfy $(u_1, v_1) = 1$. Similarly, we can write

$$B(x) = \frac{u_2}{v_2}\, b(x),$$

where $b(x) \in \mathbb{Z}[x]$ is primitive and $u_2, v_2 \in \mathbb{Z}$ satisfy $(u_2, v_2) = 1$. Thus, there exist integers $u, v \in \mathbb{Z}$ with $(u, v) = 1$ for which

$$f(x) = \frac{u}{v}\, a(x)b(x),$$

where, we emphasize, the polynomials a and b are primitive in $\mathbb{Z}[x]$.

We claim that $u = v = 1$ or $u = v = -1$. Otherwise, there is a prime p with $p \mid u$, or a prime r with $p \mid v$.

First consider the scenario with $p \mid v$, in which case

$$u\, a(x)\, b(x) = v f(x), \qquad \text{with } p \mid v,$$

so since $(u, p) = 1$ we see that all coefficients of $a(x)\, b(x)$ are divisible by p. Let the highest degree term of $a(x)$ with coefficient not divisible by p be $a_r x^r$, and the highest degree term of $b(x)$ with coefficient not divisible by p be $b_s x^s$. Then we see that

$$a(x)\, b(x) = a_r b_s x^{r+s} + c_{r+s-1} x^{r+s-1} + \cdots + c_0 + p\, h(x),$$

for some $h(x) \in \mathbb{Z}[x]$ and some $c_i \in \mathbb{Z}$. But all coefficients of $a(x)\, b(x)$ are supposed to be divisible by p, so either all coefficients of $a(x)$ are divisible by p, contradicting primitivity of $a(x)$, or all coefficients of $b(x)$ are divisible by p, contradicting primitivity. Thus $v = \pm 1$. □

When $p \mid u$, we see that all coefficients of $f(x)$ are divisible by p, contradicting primitivity of f. Hence $u = \pm 1$. □.

Then we conclude that $f(x) = \pm a(x)\, b(x)$ with a, b primitive, and $\deg(a) = \deg(A)$, $\deg(b) = \deg(B)$. This suffices to prove the lemma. //

Already this is useful in finding irreducible polynomials over $\mathbb{Q}[x]$. Thus, for example, the polynomial $x^3 - x - 1$ is irreducible over $\mathbb{Q}[x]$. For if not, it would have a factor of degree 1 over $\mathbb{Q}[x]$, and Gauss' Lemma shows then that such a factor (primitive) exists over $\mathbb{Z}[x]$. This factor

takes the form $ax+b$ with $a, b \in \mathbb{Z}$. But then

$$x^3 - x - 1 = (ax+b)\,g(x),$$

for some $g \in \mathbb{Z}[x]$, and we must have:

leading coefficient: $a \mid 1 \Rightarrow a = \pm 1$

final coefficient: $b \mid (-1) \Rightarrow b = \pm 1$.

But by trial and error, none of $\pm(x \pm 1)$ is a factor of $x^3 - x - 1$, so $x^3 - x - 1$ is irreducible over $\mathbb{Q}[x]$.

Notice that the final part of the argument applied in the proof of Gauss' Lemma could have been made more concise by reducing modulo p. We had, for example

$$u\,a(x)\,b(x) = v\,f(x) \qquad \text{with } p \mid v \text{ and } p \nmid u.$$

So in a sense $a(x)\,b(x) \equiv 0 \pmod{p}$. But we are working with polynomials, so need to be more careful.

Lemma 4.6.2. Suppose that R is a ring and $I \lhd R$. Then:

(a) $I[x] \lhd R[x]$, and

(b) $R[x] / I[x] \cong (R/I)[x]$.

Proof. Write $\bar{R} = R/I$. Recall that there exists a homomorphism

$$\varphi : R \to R/I = \bar{R}$$
$$a \longmapsto a + I$$

having kernel I. We now define

$$\Phi : R[x] \to (R/I)[x]$$
$$a_n x^n + \dots + a_0 \longmapsto \varphi(a_n)x^n + \dots + \varphi(a_0).$$

It is easy to show that Φ is a surjective homomorphism of $R[x]$ into

$\bar{R}[x]$, and

$$\ker(\Phi) = \{ f(x) \in R[x] : \varphi(a_n)x^n + \cdots + \varphi(a_0) = 0 \}$$

$$= \{ f(x) \in R[x] : \varphi(a_n), \ldots, \varphi(a_0) = 0 \}$$

$$\Downarrow$$

$$a_n, \ldots, a_0 \in I = \ker(\varphi)$$

$$\subseteq I[x].$$

But $\Phi(I[x]) = \{0\}$, so $I[x] \subseteq \ker(\Phi)$, whence $\ker(\Phi) = I[x]$.

But now by the First Isomorphism Theorem, we have

$$(R/I)[x] \cong R[x]/\ker(\Phi) = R[x]/I[x]. \quad //$$

If we apply this lemma with $R = \mathbb{Z}$ and $I = (p)$, we find that

$$\mathbb{Z}[x]/(p)[x] \cong \mathbb{Z}_p[x].$$

Now, in the proof of Gauss' Lemma noted above, we have

$$u\, a(x) b(x) = v\, f(x) \quad \text{(recall that } f \text{ is primitive.)}$$

$$\Downarrow$$

$$u\, \bar{a}(x)\bar{b}(x) \in (p)[x], \quad \text{where } \bar{a}(x) = a(x) + (p)[x]$$

$$\bar{b}(x) = b(x) + (p)[x].$$

But $\mathbb{Z}_p[x]$ is a PID and an integral domain, so this relation shows that $u \in (p)[x]$ (no, since $(u,p)=1$), or $\bar{a}(x) \in (p)[x]$ or $\bar{b}(x) \in (p)[x]$. The latter two properties contradict the primitivity of $a(x)$ and $b(x)$.

Theorem 4.6.4 (Eisenstein's criterion). Suppose that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ has degree at least 1. Suppose also that there is a prime number p with $p \nmid a_n$, $p \mid a_{n-1}, \ldots, p \mid a_1$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}[x]$.

Proof: Suppose that f satisfies the hypotheses of the theorem, and $f(x) = u(x)v(x)$, where $\deg(u) \geq \deg(v) \geq 1$ and $u, v \in \mathbb{Z}[x]$, as we may assume on account of Gauss' Lemma. We can assume, moreover, that since $p \nmid a_n$, then u and v each have lead coefficients not divisible by p. We put $I = (p)$, and work not in $\mathbb{Z}[x]$ but in $\mathbb{Z}[x]/I[x] \cong \mathbb{Z}_p[x]$. Then since $f = uv$, we have $\bar{f} = \bar{u}\bar{v}$, where $\bar{f} + I[x]$ is the polynomial representative of the class $f + I[x]$ (reduction of f modulo p), and likewise for $\bar{u}$ and $\bar{v}$. But then $\bar{f} = a_n \cdot x^n$, so $\bar{f} = \bar{u}\bar{v}$ implies that $\bar{u} = \bar{b}_r x^r$ and $\bar{v} = \bar{c}_{n-r} x^{n-r}$ for some $\bar{b}_r, \bar{c}_{n-r}$ not 0 in $\mathbb{Z}_p$, with $1 \leq r < n$. Thus $u(x) = b_r x^r + p\,w(x)$ and $v(x) = c_{n-r} x^{n-r} + p\,z(x)$, for some integers b_r and c_{n-r} not divisible by p, and for some polynomials w, z in $\mathbb{Z}[x]$. This shows that $f(x) = u(x)v(x)$ has constant term divisible by p^2, contradicting the hypotheses of the theorem. Hence $f(x)$ is irreducible. //

Example (1) Consider $f(x) = x^n - p$, with p prime.

(2) Consider $f(x) = 2x^5 - 15x^2 + 10$.

(3) Consider $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, with p prime.

Observe that $g(x) = f(x+1) = (x+1)^{p-1} + \cdots + 1$

$$= \frac{(x+1)^p - 1}{(x+1) - 1}$$

$$= \frac{1}{x}\left(x^p + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{1} x + 1 - 1 \right)$$

§4.7. Field of quotients of an integral domain.

How do we create new fields from other objects, such as other fields or rings? We have seen one approach — consider a field F, the associated polynomial ring $F[x]$ and an irreducible $p(x) \in F[x]$, and then introduce $F[x]/(p(x))$, which is a field in general distinct from F itself.

We now consider an approach of making a field from an integral domain (remember: no zero divisors!). We are already familiar with this idea — we start with the integral domain $\mathbb{Z}$, and then generate the field $\mathbb{Q}$ from this by formally considering fractions m/n with $n \neq 0$, observing that this generates multiplicative inverses for non-zero elements. But we must be careful to disambiguate: even if $m_1/n_1 = m_2/n_2$, we should be working with just one element. We do this through the use of an equivalence relation.

Let D be an integral domain (consider $\mathbb{Z}$, or $F[x]$ with F a field). Motivated by the above discussion, define

$$S = D \times (D \setminus \{0\}) = \{(a,b) : a,b \in D,\ b \neq 0\} \subseteq D \times D$$

↑ Think of this as "a/b".

We define a binary relation on S by taking

$$(a,b) \sim (c,d) \quad \text{if and only if} \quad ad = bc.$$

Claim: This relation $\sim$ defines an equivalence relation on S.

(i) Reflexivity: $(a,b) \sim (a,b) \Leftrightarrow ab = ba$ ✓

(ii) Symmetry: $(a,b) \sim (c,d) \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow (c,d) \sim (a,b)$ ✓

(iii) Transitivity: $(a,b) \sim (c,d)$ & $(c,d) \sim (f,g) \Leftrightarrow ad = bc$ & $cg = df$

$\Rightarrow adg = bcf = bdf \Leftrightarrow ag = bf$ since $d \neq 0$.

Then $(a,b) \sim (c,d)$ & $(c,d) = (f,g) \iff (a,b) \sim (f,g)$ ✓

We write $[a,b] = \{(c,d) \in S : (c,d) \sim (a,b)\}$

↑ equivalence class of (a,b). - think of this as "$\frac{a}{b}$".

We now define $F = \{[a,b] : (a,b) \in S\}$, and shows that F forms a field when endowed with addition and multiplication defined by

$$[a,b] + [c,d] = [ad+bc, bd]$$

(Think: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$)

$$[a,b] \cdot [c,d] = [ac, bd]$$

(Think: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$).

We need to check that with $+$ & $\times$ defined in this way:

(a) $+$ & $\times$ are well-defined, so that they do not depend on which representative we choose for the equivalence classes involved in the definitions;

(b) $(F, +, \times)$ forms a field, satisfying the field axioms.

To check this is the case is not difficult, but it is tedious. We sketch how to do this momentarily. For now we state the conclusion:

Theorem 4.7.1. Let D be an integral domain. Then there exists a field F with $D \subseteq F$ consisting of fractions $a/b = [a,b]$, identifying $n \in D$ with $[an, a]$ $(a \neq 0)$.

This field F is called the *field of fractions* associated with D, or the *field of quotients* of D.

Check well-defined $+$ & $\times$:

Start with $+$: Suppose $[a,b] = [a',b']$ and $[c,d] = [c',d']$.

Then $[a,b] + [c,d] = [ad+bc, bd]$ and $ab' = a'b$ and $cd' = c'd$,

so

$$[ad+bc, bd] = [(ad+bc)b'd', bdb'd'] = [a'bdd' + bb'c'd, bdb'd']$$

$$= [a'd' + b'c', b'd'] = [a',b'] + [c',d']. \checkmark$$

Then $\times$: Similarly,

$$[a,b][c,d] = [ac, bd] = [acb'd', bdb'd']$$

$$= [a'bc'd, bdb'd'] = [a'c', b'd'] = [a',b'][c',d']. \checkmark$$

Next, we must check the field axioms:

First we check that $(F,+)$ forms an abelian group. The closure follows from $[a,b] + [c,d] = [ad+bc, bd]$ and $b \neq 0, d \neq 0 \Rightarrow bd \neq 0$. Let $\alpha \in F \setminus \{0\}$.

The additive identity of F is $[0, \alpha]$, addition is plainly commutative, the inverse of $[a,b]$ is $[-a,b]$, and the associative law follows a quick expansion (exercise) $\checkmark$.

Next, we check that $(F, \times)$ forms an abelian group. Closure again follows easily, the multiplicative identity of F is $[\alpha,\alpha]$, multiplication is plainly abelian, the inverse of $[a,b]$ is $[b,a]$ whenever $a \neq 0$ and $b \neq 0$ (and $[a,b] = [0,\alpha]$ whenever $a=0$). The associative law is also easily checked. $\checkmark$

Finally, one must check the distributive laws:

$$[e,f]([a,b]+[c,d]) = [e,f][ad+bc, bd] = [e(ad+bc), bdf]$$

$$[ead^{(1)}f + ebcf, bdf^{(2)}]$$

$$[e,f][a,b] + [e,f][b,d] = [ea, bf] + [ec, df]$$

and similarly

$$([a,b]+[c,d])[e,f] = [a,b][e,f] + [c,d][e,f]. \checkmark$$

So F forms a field.

Finally, we observe that F contains a copy of D isomorphically embedded. For we can define

$$\varphi : D \longrightarrow F$$

$$d \longmapsto [\alpha d, \alpha].$$

This is a well-defined map, and satisfies the homomorphism properties, since

$$\varphi(d_1) + \varphi(d_2) = [\alpha d_1, \alpha] + [\alpha d_2, \alpha]$$

$$\varphi(d_1 + d_2) = [\alpha(d_1 + d_2), \alpha]$$

and

$$\varphi(d_1)\varphi(d_2) = [\alpha d_1, \alpha][\alpha d_2, \alpha] = [\alpha d_1 d_2, \alpha] = \varphi(d_1 d_2).$$

This is an injective mapping, since $\varphi(d_1) = \varphi(d_2) \Leftrightarrow [\alpha d_1, \alpha] = [\alpha d_2, \alpha]$ $\Leftrightarrow d_1 = d_2$ $\Leftrightarrow \alpha d_1 = \alpha d_2$. Thus φ is an injective homomorphism from D into F, whence $D \cong \varphi(D) \subseteq F$.

It is clear enough how this all works for $\mathbb{Z}$ and $\mathbb{Q}$. But observe also that there is a field of fractions, called $F(x)$, associated with the integral domain $F[x]$ when F is a field.

§5.1 Fields.

Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

$\mathbb{Q}(\sqrt{-1}) = \{ a + b\sqrt{-1} : a, b \in \mathbb{Q} \}$.

$\mathbb{Z}_p$ (p prime)

$\mathbb{Z}_p[x]/(x^2+1)$ $\quad p = 3$, say

↑ finite field with 9 elements.

$\mathbb{R}(t)$, $\mathbb{Z}_p(t)$ (fields of fractions of $\mathbb{Q}[t]$, $\mathbb{Z}_p[t]$).

Important feature of fields.

Given a field F, there is a 0 element and a 1 element (identities in $(F,+)$ and $(F^\times, \times)$ respectively).

From these elements we can generate further elements of the field, for example $\underbrace{1+\ldots+1}_{n \text{ times}}$ for any $n \in \mathbb{N}$.

Question: are these elements necessarily distinct?

Alternative A: The elements $\underbrace{1+\ldots+1}_{n\text{-times}} \in F$ are all distinct, for all $n \in \mathbb{N}$.

Then F contains $n = n1$, for each $n \in \mathbb{N}$, and hence also $-n$ (additive inverses), so F contains a copy of $\mathbb{Z}$. But then (multiplicative inverses), one has $ab^{-1} = a/b \in F$ for each $b \in \mathbb{Z} \setminus \{0\}$, so F contains a copy of $\mathbb{Q}$.

Examples. $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{R}(t)$.

Alternative B: The elements $\underbrace{1+\ldots+1}_{n\text{-times}} \in F$ are not all distinct, for all $n \in \mathbb{N}$, so there exist $n_1, n_2 \in \mathbb{N}$ with $n_2 > n_1$ and

$n_2 1 = n_1 1 \Rightarrow (n_2 - n_1)1 = 0$. Thus, there exists $m \in \mathbb{N}$ with $m \cdot 1 = 0$.

Claim: If the elements $\underbrace{1+\dots+1}_{n}$ are not all distinct in F, for $n \in \mathbb{N}$, then $p \cdot 1 = 0$ for some prime p.

Proof. Let n be the smallest positive integer with $n \cdot 1 = 0$ in F. If $n = uv$ for some integers $u \geq v \geq 2$, then we have $0 = n \cdot 1 = uv \cdot 1 = (u \cdot 1)(v \cdot 1)$, so $u \cdot 1 = 0$ or $v \cdot 1 = 0$ (since F is an integral domain) #, contradicting the minimality of n. We therefore have that n is prime. //

In this situation, the field F contains a copy of $\mathbb{Z}_p$.

Definition: A field F has characteristic p (with $p \neq 0$) when p is the least positive integer satisfying $p \cdot 1 = 0$, in which case p is necessarily prime. If no such integer exists, then F has characteristic 0.

Notice that if F has characteristic p, then $px = (p \cdot 1)x = 0$ for all $x \in F$.

Alternative A: F has characteristic 0 and contains a copy of $\mathbb{Q}$

Alternative B: F has characteristic p and contains a copy of $\mathbb{F}_{p^n}$.

$\mathbb{Z}_p$

Examples of fields of characteristic p: $\mathbb{Z}_p$, $\mathbb{Z}_p(t)$, $\mathbb{Z}_p[t]/(t^2+1)$ when $p \equiv 3 \pmod 4$, ...

§6.2 – 6.4. Finite fields.

We concentrate on fields having characteristic p with p prime, and in particular finite fields (which necessarily have prime characteristic). Our goal will be to summarise their basic properties – about which one can say a great deal. Our first goal concerns $K^\times$ = multiplicative group of non-zero elements of a field K.

Theorem 6.2.4. Suppose that K is a finite field. Then $K^\times = K \setminus \{0\}$ is a cyclic group.

Proof. We know already that if K is a finite field, then it has characteristic p for some prime number p, and then (Cauchy) $|K| = p^n$, for some $n \in \mathbb{N}$. Thus $|K^\times| = p^n - 1$, and we have $a^{p^n-1} = 1$ for all $a \in K^\times$. Write $m = p^n - 1$, and note that in $K^\times$, the order of every element is a divisor of m.

Suppose that a has order d. Then we have seen (a homework problem) that the elements $1, a, a^2, \dots, a^{d-1}$ are distinct solutions of the equation $x^d = 1$ in $K^\times$, and there are $\varphi(d)$ elements here (in fact a^r with $0 \le r < d$ and $(r,d) = 1$) having order d. But using the field property of K, we then have

$$x^d - 1 = (x-1)(x-a)\cdots(x-a^{d-1})$$

since a polynomial of degree d over K has at most d roots. Then the number of elements of $K^\times$ having order d is either 0 (if no such element a exists) or $\varphi(d)$.

Every element b of $K^\times$ has order dividing m, so if $\psi(d)$ is the number of elements having order d, we have

$$m = \sum_{d|m} \psi(d) \le \sum_{d|m} \varphi(d).$$

But $\sum_{d|m} \varphi(d) = m$ (consider a cyclic group of order m),

so we must have $m = \sum_{d|m} \psi(d) \le \sum_{d|m} \varphi(d) = m$ gives that the central inequality holds with equality. Thus $\psi(d) = \varphi(d)$ for all $d|m$, and

in particular $\psi(m) = \varphi(m) \geq 1$. Thus $K^\times$ contains an element a of order $m = |K^\times|$, whence $K^\times = \langle a \rangle$ is cyclic. //

The element a is known as a primitive root, especially in case $K = \mathbb{Z}_p$. with $K^\times = \langle a \rangle$

Recall that $U_n = \{ 1 \leq a \leq n : (a,n) = 1 \}$ forms a multiplicative group modulo n. Two facts:

(1) U_{p^2} is cyclic, say $U_{p^2} = \langle g \rangle$, for all primes p.
↕ same!

(2) U_{p^n} is cyclic, say $U_{p^n} = \langle g \rangle$, for all odd primes p.

Theorem 6.3.4 (Existence of finite fields) Let p be prime and $n \in \mathbb{N}$. Then there exists a finite field F having p^n elements.

Proof. Let $m = p^n$, and consider the polynomial

$$f(x) = x^m - x \in \mathbb{Z}_p[x].$$

We can factor $f(x)$ into monic irreducible factors, say

$$f(x) = g_1(x) \cdots g_r(x).$$

Now take any factor, say wlog $g_1(x)$, of maximal degree at least 2, and consider the field $K_1 = \mathbb{Z}_p[x] / (g_1(x))$. Inside $K_1[x]$, the polynomial $f(x) = x^m - x$ factors as a product of irreducibles, but $g_1(x)$ has an extra linear factor since $x + (g_1(x))$ is a root of $g_1(x)$ in K_1. Then, as a product of irreducibles, we have

$$f(x) = h_1(x) \cdots h_s(x),$$

say, where the maximal degree (or multiplicity of this degree) decreases. By iterating this process, next looking at $K_2 = K_1[x]/(h_1(x))$, etc, we eventually obtain a field K in which

$$f(x) = x^m - x = (x - \alpha_1) \cdots (x - \alpha_m), \text{ for}$$

some $\alpha_1, \ldots, \alpha_m \in K$.

We claim that none of these roots has multiplicity exceeding 1. For suppose α has multiplicity $k \geq 2$, say, so that

$$x^m - x = (x-\alpha)^k u(x),$$

for some $\alpha \in K$, $u(x) \in K[x]$. By formal differentiation, we then have

$$m x^{m-1} - 1 = k(x-\alpha)^{k-1} u(x) + (x-\alpha)^k u'(x),$$

where if $u(x) = a_r x^r + \ldots + a_0$, we put $u'(x) = r a_r x^{r-1} + \ldots + a_1$.
[Note: need to check the rules of formal differentiation here].
Hence

$$m \alpha^{m-1} - 1 = 0,$$

whence

$$\alpha = m \alpha^m = m \alpha,$$

so that $m = 1$. ※ So all roots of $f(x)$ have multiplicity 1.

Let $A = \{ a \in K : a^m = a \}$, so $|A| = m$.

We now see that A is a non-empty subset of K, and is hence a subfield provided that:

(1) whenever $a, b \in A$, we have $a+b \in F$;
(2) whenever $a, b \in A$, we have $ab \in F$.

But whenever $a, b \in A$, we have

$$a + b = a^m + b^m = (a+b)^m, \quad \text{since } m = p^n \text{ and } \operatorname{char}(K) = p.$$

and

$$ab = a^m b^m = (ab)^m,$$

whence $a+b \in A$ and $ab \in A$. Since A is a subfield of K, it is itself a field with $m = p^n$ elements, and is the field asserted in the statement of the theorem. //

As you will learn if you take the course MA 454 in Galois Theory, all fields F having p^n elements are in fact isomorphic. So we can study the properties of any field having p^n elements by studying our favorite version of this field. This is:

Theorem 6.4.3. For any prime p and any $n \in \mathbb{N}$, there (up to isomorphism) a unique field having p^n elements.

The standard notation is to refer to $\mathbb{F}_{p^n}$ as this field, though in older texts the notation $GF(p^n)$ is also used.

Extra Topic: Every PID is a UFD. (Sketch). We assume $1 \in R$ throughout.

Recall: A Principal Ideal Domain (PID) is an integral domain in which every ideal is principal.

Definition. Suppose R is a commutative ring. Then P is a prime ideal if $P \neq R$ and whenever $a, b \in R$ and $ab \in P$, then one of a and b lies in P.

Ex. $P \lhd R$ (with R commutative) $\Leftrightarrow$ R/P is an integral domain.

Corollary: Suppose R commutative. Then maximal ideals of R are prime ideals.

Proposition A. Every non-zero prime ideal in a PID is a maximal ideal.

Proof. Let (p) be a non-zero prime ideal in the PID R, and let $I = (m)$ be any ideal containing (p). We have $p \in (m)$, so $p = rm$ for some $r \in R$. But (p) is a prime ideal and $rm \in (p)$, so $r \in (p)$ or $m \in (p)$. If $m \in (p)$, then $(p) = (m)$; and if $r \in (p)$ then $r = ps$, some $s \in R$, whence $p = rm = psm$, so $sm = 1 \Rightarrow (m) = R$.

Thus $(m) = (p)$ or $(m) = R$, and thus (m) is maximal. //

Definition Let R be an integral domain.

(a) • If $r \in R \setminus \{0\}$ and r is not a unit (a unit is a divisor of 1), then r is irreducible in R if, whenever $r = ab$ with $a, b \in R$, one at least of a and b is a unit of R.

• If r is not irreducible in R, then it is reducible in R.

(b) The element $p \in R \setminus \{0\}$ is prime in R if (p) is a prime ideal. Thus, p is prime if it is not a unit, and whenever $p \mid ab$ then $p \mid a$ or $p \mid b$.

(c) If $a, b \in R$, then a and b are associates if $a = ub$ for some unit $u \in R$.

Proposition B. Let R be an integral domain. Then if $p \in R$ is a prime element, then p is irreducible.

Proof: Suppose (p) is a non-zero prime ideal and $p = ab$. Then $ab \in (p)$, so one of a and b lies in (p). Thus $a = pc$ for some $c \in R$, whence $p = ab = pcb$, whence $cb = 1$ and b is a unit. Thus p is irreducible. //

Proposition C. In a PID, a non-zero element is prime if and only if it is irreducible.

Proof. ($\Rightarrow$) ✓ Prop B. □

($\Leftarrow$) Suppose $p \in R$ is irreducible. If $(p) \subseteq M \lhd R$, then $M = (m)$ is a principal ideal and $p \in (m)$, so $p = rm$ for some $r \in R$.

But p is irreducible, so either r or m is a unit, whence $(p) = (m)$ or $(m) = (1)$. Then the only ideals containing (p) are (p) and (1), so (p) is maximal. But maximal ideals are prime ideals. □ //

Definition A unique factorisation domain (UFD) is an integral domain R in which every non-zero element $r \in R$ which is not a unit satisfies:

(a) $r = p_1 p_2 \cdots p_n$, for some $n \in \mathbb{N}$, $p_i \in R$ irreducible.

(b) this decomposition is unique up to associates, so if $r = q_1 \cdots q_m$, with $m \in \mathbb{N}$ and $q_i \in R$ irreducible, then each p_i is an associate of some q_j.

Proposition D. In a UFD R, a non-zero element is prime if and only if it is irreducible.

Proof. Exercise — compare to conclusion for primes in $\mathbb{Z}$.

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

//

Theorem E. Every PID is a UFD.

Proof. (Sketch) Analogous to prime factor decompositions of integers — first prove that elements are the finite product of irreducibles.

Suppose R is a PID and $r \in R \setminus \{0\}$ is not a unit. If r is irreducible, then we are done. Otherwise, we have $r = r_1 r_2$, where neither r_1 nor r_2 is a unit. If both are irreducible then we are done. Otherwise, decompose r_1 into r_{11}, r_{12}, say, with each r_{1j} not units. We claim that by repeating this process, we ultimately decompose r as a product of irreducibles. If not, then we have (by relabelling) a proper inclusion of ideals

$$(r) \subset (r_1) \subset (r_{11}) \subset (r_{111}) \subset \cdots \subset R.$$

Then by the Axiom of Choice an infinite chain exists. We can show that in such a chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$, in a PID, we eventually have $I_k = I_n$ for all $k \geq n$. Let $I = \bigcup_{i=1}^{\infty} I_i$. Then I is an ideal (exercise), so $I = (a)$ (using PID property). Thus $a \in I_n$ for some n, when $I_n \subseteq I = (a) \subseteq I_n$, and thus $I = I_n$, so $I_k = I_n = I$ for $k \geq n$. Hence we cannot have such a proper inclusion of ideals, and every $r \in R \setminus \{0\}$ not a unit has a factorisation as a product of irreducibles in R. $\square$

Finally, we can show that this decomposition is essentially unique — similar to proof of uniqueness of prime factorisations in $\mathbb{Z}$. If

$$r = p_1 \cdots p_n = q_1 \cdots q_m \quad \text{with } m \geq n,$$

with p_i, q_j irreducible, then $p_1 \mid q_1 \cdots q_m$, so by Prop D we see that $p_1 \mid q_j$ for some j, so p_1 is an associate of q_j. Then proceed by induction, noting next that

$$p_2 \cdots p_n = u\, q_1 \cdots q_{j-1}\, q_{j+1} \cdots q_m,$$

where $p_1 = u q_j$ and u is a unit. In this way we show that the factorisation here is essentially unique. $\square$ //