GROUPS AND RINGS

DAVID PIERCE

CONTENTS

I originally created these notes for use in teaching a graduate course, Math 503 (Algebra I), at METU, fall semester, 2003/4. The main reference was [1], but I also consulted [3] and [6]. I aimed to cover material in [1] week by week roughly as follows; in brackets are exercises:

(1) I.1
(2) I.2, 3, 4 (§ 2: 2, 3, 5, 9, 11, 18; § 3: 1, 2, 4, 5, 9)
(3) I.5 (§ 4: 2, 3, 11, 12; § 5: 1, 7, 19, 20)
(4) I.6, 7 (§ 6: 1, 4, 7, 8, 9; § 7: 5)
(5) I.8, 9 (§ 8: 2, 3, 4, 5, 7, 9, 14)
(6) II.1, 2, 4
(7) II.5; first in-term examination
(8) II.6, 7 (solutions to exam problems)
(9) II.8 (§ 4: 3, 4, 5, 6, 7, 13; § 5: 3, 9, 10, 11; § 6: 9)
(10) (Şeker bayramı)
(11) III.1, 2 (II.7: 3, 4, 8, 9; II.8: 1, 5, 7, 13)
(12) III.3
(13) III.4; second in-term examination
(14) III.5
(15) III.6

Date: September 18, 2008.

0. Foundations of the mathematics

For every set A there is a set $A \cup \{A\}$, which we may call the **successor** of A and denote by A'.

0.1. **Axiom** (Infinity). *There are sets that contain $\varnothing$ and contain the successors of all of their elements.*

0.2. **Lemma.** *There is a unique smallest set with the closure properties of the Axiom of Infinity.*

The unique smallest set in the lemma is denoted by

$$\omega;$$

it is the set of **natural numbers.** By this definition, each natural number is also a *set* of natural numbers; namely, if $n \in \omega$, then

$$n = \{0, 1, 2, \dots, n-1\}.$$

For any set M, the Cartesian power M^n can be understood as the set of functions from n to M. Such a function can be denoted by $(a_0, \dots, a_{n-1})$ or just $\boldsymbol{a}$. An **n-ary operation** on M is a function from M^n to M. Operations that are 2-ary, 1-ary or 0-ary are also called **binary, singulary,**[1] or **nullary.** The set M^2 can be identified with the **Cartesian product** $M \times M$. The set M^1 has an obvious bijection with M. The set M^0 always consists of the unique element $\varnothing$, even if M is empty. Hence a singulary operation on M can be understood as a function from M to itself, and a nullary operation on M can be identified with an element of M. In particular, any set equipped with a nullary operation must be non-empty.

The set ω is equipped with:

(0) the nullary operation (or distinguished element) $\varnothing$;
(1) the singulary operation $x \mapsto x'$.

From these can be defined the usual binary operations of addition and multiplication. Also, ω has a binary relation $\subseteq$, usually written $\leqslant$.

A set equipped with some operations and relations is a **structure.** Some essential examples—all definable in terms of ω—are:

- $(\omega, \leqslant)$, a *well-ordered set;*
- $(\omega, +, 0)$, a *monoid;*
- $(\mathbb{Z}, +, -, 0)$, an *abelian group;*
- $(\mathbb{Z}, +, -, \times, 0, 1)$, a *ring;*
- $(\mathbb{Q}, +, -, \times, 0, 1)$, a *field.*

[1]The word **unary** is more common, but less etymologically correct.

Part 1. Construction of groups

1. Definition of groups

For any set A, we may refer to a bijection from A to itself as a **symmetry** or **permutation** of A. Let $\mathrm{Sym}(A)$ be the set of these symmetries. This is equipped with:

(0) the element id_A (the identity on A);
(1) the singulary operation $f \mapsto f^{-1}$ (functional inversion);
(2) the binary operation $(f, g) \mapsto f \circ g$ (functional composition).

Any subset of $\mathrm{Sym}(A)$ that is closed under these operations can be called a **group of symmetries** of A.

We isolate some algebraic properties of groups of symmetries and use them to define groups in general:

1.1. **Definition.** A **group** is a quadruple $(G, \times, {}^{-1}, 1)$, where G is a set, and $\times$, ${}^{-1}$ and 1 are binary, singulary and nullary operations respectively on G such that, for all a, b and c in G:

(0) $a \times (b \times c) = (a \times b) \times c$ (that is $\times$ is **associative**),
(1) $a \times 1 = a$ and $1 \times a = a$,
(2) $a \times a^{-1} = 1$ and $a^{-1} \times a = 1$.

It should be clear that a group of symmetries is in fact a group. Conversely, we shall show below that every group can be identified with a group of symmetries.

The group $(G, \times, {}^{-1}, 1)$ has the **universe** G. The group itself is more than its universe; we may indicate this by letting $\mathfrak{G}$ designate the group. However, most people do not distinguish in writing between a group and its universe; and it is not always practical to make the distinction in writing.

For the group-element denoted by 1 above, some people write e. Usually, the **product** $a \times b$ is written as $a \cdot b$ or just ab. The operation itself can be called **multiplication.** Any group-element a determines two singulary operations, λ_a and ρ_a, given by

$$\lambda_a x = ax \qquad \text{and} \qquad \rho_a x = xa.$$

By Definition 1.1, both λ_1 and ρ_1 are the same operation, namely the identity; so 1 itself is called an **identity.**

In a group $\mathfrak{G}$, multiplication might be denoted by $\times^{\mathfrak{G}}$ (or $\cdot^{\mathfrak{G}}$, or $\times^G$, or…) if it should be distinguished from the multiplication in a different group.

In fact, suppose $\mathfrak{H}$ is another group. A function f from G to H is a **homomorphism** from $\mathfrak{G}$ to $\mathfrak{H}$ if it *preserves* the group-operations:

(0) $f(1) = 1$ (that is, $f(1^{\mathfrak{G}}) = 1^{\mathfrak{H}}$);
(1) $f(a^{-1}) = f(a)^{-1}$ (that is, $f(a^{-1^{\mathfrak{G}}}) = f(a)^{-1^{\mathfrak{H}}}$);
(2) $f(ab) = f(a)f(b)$ (that is, $f(a \times^{\mathfrak{G}} b) = f(a) \times^{\mathfrak{H}} f(b)$)

for all a and b in G. The homomorphism is called:

- a **monomorphism,** if it is injective;
- an **epimorphism,** if it is surjective;
- an **isomorphism,** if it is bijective.

A monomorphism is also called an **embedding.** Every group is isomorphic to its image under an embedding. There is no difference between isomorphic groups as such. A monomorphism of a group into itself is an **endomorphism;** an isomorphism of a group with itself is an **automorphism.**

1.2. **Lemma.** *In any group, the equations*

$$a \cdot X = b \quad \text{and} \quad Y \cdot a = b$$

have unique solutions, namely $a^{-1} \cdot b$ *and* $b \cdot a^{-1}$.

Proof. We have

$$\begin{aligned} a \cdot X = b &\implies a^{-1}(a \cdot X) = a^{-1}b \\ &\implies (a^{-1}a)X = a^{-1}b \\ &\implies 1 \cdot X = a^{-1}b \\ &\implies X = a^{-1}b; \end{aligned}$$

therefore the equation $a \cdot X = b$ has at most one solution, $a^{-1}b$; this *is* a solution, since $a(a^{-1}b) = (a \cdot a^{-1})b = 1 \cdot b = b$. □

Note how the proof of this lemma relies on each of the defining properties of groups.

1.3. **Theorem** (Cayley)**.** *Let* $\mathfrak{G}$ *be a group. If* $a \in G$, *then both* λ_a *and* ρ_a *are in* $\mathrm{Sym}(G)$. *The map* $x \mapsto \lambda_x$ *is a monomorphism from* $\mathfrak{G}$ *to* $(\mathrm{Sym}(G), \circ, {}^{-1}, \mathsf{id}_G)$.

Proof. By Lemma 1.2, the equations $\lambda_a X = b$ and $\rho_a X = b$ always have unique solutions, that is, λ_a and ρ_a are invertible—so they are in $\mathrm{Sym}(G)$. Also, the equations $\lambda_X a = b$ have unique solutions, so the map $x \mapsto \lambda_x$ is injective. Finally, $\lambda_{xy}a = (xy)a = x(ya) = (\lambda_x \circ \lambda_y)a$; we have already observed that $\lambda_1 = \mathsf{id}_G$; and Lemma 1.2 shows that $(\lambda_a)^{-1} = \lambda_{a^{-1}}$. □

The group-operation $x \mapsto x^{-1}$ can be called **inversion.** We now have, in any group:

- uniqueness of the identity and of inversion;
- left and right cancellation: $ax = ay \implies x = y$, and $xa = ya \implies x = y$.

2. Simplifications

In Definition 1.1, if we ignore the operation ${}^{-1}$, we have a **monoid;** if we ignore also the 1, we have a **semi-group.**

In particular, if $(G, \times, {}^{-1}, 1)$ is a group, then the *reduct* $(G, \times, 1)$ is a monoid, and $(G, \times)$ is a semi-group; but not every semi-group is the reduct of a monoid, and not every monoid is the reduct of a group.

2.1. **Example.** The set $\{1, 2, 3, \dots\}$ of positive integers is a semi-group when equipped with addition, but it has no identity.

2.2. **Example.** $(\omega, +, 0)$ is a monoid, but only 0 has an inverse.

2.3. **Lemma.** *In Definition 1.1, if we ignore the equations* $1 \times a = a$ *and* $a^{-1} \times a = 1$, *we still have a group. In other words, any semi-group with a left-identity and with left-inverses is a group.*

Proof. If $x \cdot x = x$, then $1 = (x \cdot x) \cdot x^{-1} = x \cdot (x \cdot x^{-1}) = x \cdot 1 = x$. But $(a^{-1} \cdot a) \cdot (a^{-1} \cdot a) = a^{-1} \cdot (a \cdot a^{-1}) \cdot a = a^{-1} \cdot a$, so $a^{-1} \cdot a = 1$. Finally, $1 \cdot a = (a \cdot a^{-1}) \cdot a = a \cdot (a^{-1} \cdot a) = a \cdot 1 = a$. □

The lemma has an obvious dual.

2.4. **Lemma.** *If $\mathfrak{G}$ is a semi-group in which all equations*

$$a \cdot X = b \quad \text{and} \quad Y \cdot a = b$$

have solutions (not assumed unique), then $\mathfrak{G}$ can be expanded to a group (that is, can be given an identity and an inversion).

Proof. There are 1 and c such that $1 \cdot a = a$ and $a \cdot c = b$. Then $1 \cdot b = 1 \cdot (a \cdot c) = (1 \cdot a) \cdot c = a \cdot c = b$. So 1 is a left-identity. Since $X \cdot b = 1$ has a solution, left-inverses exist. Now use Lemma 2.3. $\square$

By Lemmas 1.2 and 2.4, we can characterize groups as those semi-groups that satisfy the axiom

$$\forall x\ \forall y\ \exists z\ \exists w\ (xz = y\ \&\ wx = y).$$

In particular, we don't need to talk explicitly about the identity and inversion in order to define a group. This is why statements like the following are true:

2.5. **Lemma.** *A map f from G to H is a group-homomorphism from $\mathfrak{G}$ to $\mathfrak{H}$, provided it preserves multiplication.*

3. Notation

If a_i are group-elements, then by

$$a_0 \cdot a_1 \cdots a_{n-1} \quad \text{or} \quad \prod_{i<n} a_i$$

we mean $(\cdots((a_0a_1)a_2)\dots,)a_{n-1}$. Recursively:

$$\prod_{i<0} a_i = 1 \quad \text{and} \quad \prod_{i<n+1} a_i = \Big(\prod_{i<n} a_i\Big)a_n.$$

3.1. **Lemma** (Associativity)**.** *No matter how parentheses are inserted into a list a_0, a_1, …, a_{n-1} of group-elements, the resulting group-element is the same.*

For $\prod_{i<n} a$ we write a^n. In particular, $a^0 = 1$. Also, $(a^n)^{-1}$ is written a^{-n}.

3.2. **Lemma.** *For any element a of a group $\mathfrak{G}$, the map $n \mapsto a^n$ from $\mathbb{Z}$ to G is a group-homomorphism: in particular,*

$$a^{n+m} = a^n a^m$$

for all integers n and m. Also,

$$a^{mn} = (a^n)^m$$

for all integers n and m.

(Note another way to express the latter point in the lemma. Each n in $\mathbb{Z}$ determines the map $x \mapsto x^n$ from G to itself. That is, we have a map Φ from $\mathbb{Z}$ to $F(G)$, where $F(G)$ is the set of singulary operations on G, and $\Phi(n)(a) = a^n$. Then $\Phi(mn) = \Phi(m) \circ \Phi(n)$, so Φ is a homomorphism from the monoid $(\mathbb{Z} \smallsetminus \{0\}, \times, 1)$ to $(F(G), \circ, \mathsf{id}_G)$.)

A group $(G, +, -, 0)$ is **abelian** if $a + b = b + a$ for all a and b in G. Abelian groups are generally written thus, 'additively'. For such groups we may write $a_0 + a_1 + \cdots + a_{n-1}$ or $\sum_{i<n} a_i$ for $(\cdots(a_0 + a_1) + \cdots + a_{n-2}) + a_{n-1}$; for $\sum_{i<n} a$ we write na; for $-(na)$, we write $(-n)a$; then $n(a + b) = na + nb$, so the maps $a \mapsto na$ are homomorphisms from an abelian group to itself.

4. New groups from old

If $\mathfrak{G}$ and $\mathfrak{H}$ are two groups, then we can define a multiplication on $G \times H$ termwise:

$$(g,h)\cdot(g',h') = (g \times^{\mathfrak{G}} g', h \times^{\mathfrak{H}} h').$$

The result is the group $\mathfrak{G}\times\mathfrak{H}$, the **direct product** of $\mathfrak{G}$ and $\mathfrak{H}$. (This is the **direct sum** $\mathfrak{G}\oplus\mathfrak{H}$, if $\mathfrak{G}$ and $\mathfrak{H}$ are abelian.)

If $\sim$ is an *equivalence-relation* on the set G, then we can form the **quotient** $G/{\sim}$, which contains, for each a in G, the set

$$\{x \in G \colon x \sim a\};$$

this is the *equivalence-class* or *$\sim$-class* of a and can be denoted by $[a]$ or $\overline{a}$. Any group-structure $\mathfrak{G}$ on G induces one on $G/{\sim}$, provided

$$a \sim a' \;\&\; b \sim b' \implies ab \sim a'b'.$$

Indeed, if $\sim$ meets this requirement, then it is called a **congruence-relation** on $\mathfrak{G}$, and a well-defined multiplication on $G/{\sim}$ is given by

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

4.1. **Example.** Let $n \in \mathbb{Z}$, and on $\mathbb{Z}$, let $a \sim b \iff n \mid a - b$; then $\mathbb{Z}/{\sim}$ has an induced group-structure, which may be written $\mathbb{Z}/\langle n\rangle$ (or $\mathbb{Z}_n$, or $\mathbb{Z}/n\mathbb{Z}$, or $\mathbb{Z}/(n)$). Note that Z_0 is isomorphic to $\mathbb{Z}$ itself.

4.2. **Example.** On $\mathbb{Q}$, let $a \sim b \iff a - b \in \mathbb{Z}$; then $\mathbb{Q}/{\sim}$ has an induced group-structure, which can be written $\mathbb{Q}/\mathbb{Z}$. Note

$$a \mapsto \exp(2\pi i a)\colon (\mathbb{Q}/\mathbb{Z}, +) \to (\mathbb{C}^{\times}, \times).$$

an embedding.

A **subgroup** of a group is a subset containing the identity that is closed under multiplication and inversion. Every group has both itself and $\{1\}$ as subgroups.

4.3. **Lemma.** *A subset of a group is a subgroup if and only if it is non-empty and closed under the binary operation $(x,y) \mapsto xy^{-1}$.*

If $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$, we write[2] $\mathfrak{H} \leqslant \mathfrak{G}$.

4.4. **Lemma.** *If $\sim$ is a congruence-relation on $\mathfrak{G}$, then the $\sim$-class of 1 is a subgroup of $\mathfrak{G}$.*

It is important to note that the converse of the lemma is false in general: not every subgroup of a group determines a congruence-relation. (see Theorem 7.1.)

If f is a homomorphism from G to H, then its **kernel** is the set

$$\{x \in G \colon f(x) = 1\},$$

denoted by $\ker f$. The **image** of f is

$$\{y \in H \colon y = f(x) \text{ for some } x \text{ in } G\},$$

denoted by $\operatorname{im} f$.

4.5. **Lemma.** *Let f be a homomorphism from G to H.*

(0) $\ker f \leqslant G$.

[2] Or simply $\mathfrak{H} < \mathfrak{G}$, if one is not worried about having a way to distinguish *proper* subgroups.

(1) *f is a monomorphism* $\iff \ker f = \{1\}$.
(2) $\operatorname{im} f \leqslant H$.
(3) *f is an epimorphism* $\iff \operatorname{im} f = H$.

4.6. **Lemma.** *An arbitrary intersection of subgroups is a subgroup.*

Given a subset A of (the universe of) a group $\mathfrak{G}$, we can 'close' under the three group-operations, obtaining a subgroup, $\langle A\rangle$. For a formal definition, we let

$$\langle A\rangle = \bigcap \mathcal{S},$$

where $\mathcal{S}$ is the set of all subgroups of $\mathfrak{G}$ that include A.

If $\mathfrak{G} = \langle A\rangle$, then $\mathfrak{G}$ is **generated** by A. If $A = \{a_0, \dots, a_{n-1}\}$, we may write

$$\langle a_0, \dots, a_{n-1}\rangle$$

for $\langle A\rangle$, and say that $\mathfrak{G}$ has the n **generators** a_0, …, a_{n-1}.

5. Cyclic groups

The **order** of a group is its size (or cardinality). The order of G is therefore denoted by

$$|G|\,.$$

A group is called **cyclic** if generated by a single element. If a is an element of a group G, then $\langle a\rangle$ is a cyclic subgroup of G, and the **order** of a, denoted by

$$|a|\,,$$

is just the order of $\langle a\rangle$.

5.1. **Lemma.** *If a is an element of a group G, then*

$$\langle a\rangle = \{x \in G \colon x = a^n \text{ for some } n \text{ in } \mathbb{Z}\}.$$

Proof. Let f be the homomorphism $n \mapsto a^n$ from $\mathbb{Z}$ to G. We have to show $\langle a\rangle = \operatorname{im} f$. Since $\langle a\rangle$ is a group, we know that $a^0 \in \langle a\rangle$. If $a^n \in \langle a\rangle$, then $a^{n+1} \in \langle a\rangle$ and $a^{-n} \in \langle a\rangle$. Hence, by induction, $\operatorname{im} f \subseteq \langle a\rangle$. Since $a \in \operatorname{im} f$, we have $\langle a\rangle \subseteq \operatorname{im} f$ by definition of $\langle a\rangle$. □

5.2. **Lemma.** *If a is a group-element of finite order, then $a^{|a|} = 1$.*

Proof. The subset $\{1, a, a^2, \dots, a^{|a|}\}$ of $\langle a\rangle$ has size at most $|a|$. Hence we have $0 \leqslant i < j \leqslant |a|$ but $a^i = a^j$ for some i and j. Therefore $1 = a^{j-i}$, and $a^k = a^n$ as long as $k \equiv n \pmod{j-i}$. This means $|a| \leqslant j-i$ and hence $|a| = j-i$. □

5.3. **Lemma.** *All subgroups of $\mathbb{Z}$ are cyclic. All non-trivial subgroups of $\mathbb{Z}$ are isomorphic.*

Proof. Say $G \leqslant \mathbb{Z}$ and $G \neq \langle 0\rangle$. As a set, G has a greatest common divisor, n. That is, if we write G as $\{a_i \colon i \in \omega\}$, then

$$n = \min\{\gcd(a_0, \dots, a_m) \colon m \in \omega\}.$$

Then $G \leqslant \langle n\rangle$. Also, for some m and some b_0, …, b_{m-1} in $\mathbb{Z}$, we have

$$n = b_0 a_0 + \dots + b_{m-1} a_{m-1};$$

so $\langle n\rangle \leqslant G$. The map $x \mapsto nx$ from $\mathbb{Z}$ to G is an epimorphism, by Lemma 5.1; but its kernel is trivial; so it is an isomorphism, by Lemma 4.5. □

5.4. **Theorem.** *Every cyclic group is isomorphic to some $\mathbb{Z}/\langle n\rangle$.*

Proof. Say $G = \langle a\rangle$. By Lemma 5.3, the epimorphism $x \mapsto a^x$ from $\mathbb{Z}$ to G has kernel $\langle n\rangle$ for some n; therefore

$$a^r = a^s \iff a^{r-s} = 1 \iff r - s \in \langle m\rangle \iff m \mid r - s.$$

Hence the map $x \mapsto a^x$ is well-defined on $\mathbb{Z}/\langle n\rangle$ and has trivial kernel. □

6. Cosets

Suppose $H \leqslant G$. If $a \in G$, let

$$aH = \lambda_a[H],$$
$$Ha = \rho_a[H].$$

Each of the sets aH is a **left co-set** of H, and the set of these is denoted by

$$G/H.$$

Each of the sets Ha is a **right co-set** of H, and the set of these is denoted by

$$H\backslash G.$$

6.1. **Lemma.** *The left cosets of H in G are the classes determined by an equivalence-relation on G. Likewise for the right cosets. All cosets of H have the same size; also, G/H and $H\backslash G$ have the same size.*

Proof. We have $a \in aH$. All cosets of H have the same size as H, since the maps λ_a and ρ_a are bijections by Cayley's Theorem (1.3). If $aH \cap bH \neq \varnothing$, then $ah \in bH$ for some h in H, so $a \in bHH^{-1} \subseteq bH$, whence $aH \subseteq bH$, so $aH = bH$. Hence the left cosets compose a partition of G, and therefore determine an equivalence-relation. Inversion is a permutation of G taking aH to Ha^{-1}, so G/H and $H\backslash G$ have the same size. □

The size of G/H (or $H\backslash G$) is the **index** of H in G and can be denoted by

$$[G : H].$$

6.2. **Theorem** (Lagrange). *$|H|$ divides $|G|$ if both are finite.*

Proof. $|G| = [G : H] \cdot |H|$. □

In fact, if also $K \leqslant H$, then $[G : K] = [G : H] \cdot [H : K]$.

6.3. **Theorem.** *Groups of prime order are cyclic.*

Proof. Say $|G| = p$. There is a in $G \smallsetminus \langle 1\rangle$, so $|a| > 1$; but $|a| \mid p$, so $|a| = p$, that is, $G = \langle a\rangle$. □

6.4. **Lemma.** *If G is finite and $a \in G$, then $a^{|G|} = 1$.*

Proof. $a^{|G|} = a^{[G:\langle a\rangle]\cdot|a|} = (a^{|a|})^{[G:H]} = 1^{[G:H]} = 1$. □

The set $\mathbb{Z}$ of integers is a semi-group with respect to multiplication. The non-zero integers form a multiplicative monoid. This multiplication is well-defined on $\mathbb{Z}/\langle n\rangle$ for any integer n, and the non-zero elements of this compose a monoid. Let

$$(\mathbb{Z}/\langle n\rangle)^\times$$

comprise the invertible elements of this monoid; so $(\mathbb{Z}/\langle n\rangle)^\times$ is a group.

6.5. **Lemma.** $(\mathbb{Z}/\langle n\rangle)^\times = \{[x] \in \mathbb{Z}/\langle n\rangle \colon \gcd(x, n) = 1\}$.

Proof. $\gcd(m, n) = 1$ if and only if $am + bn = 1$ for some integers a and b; but this just means $[a][m] = 1$ for some a. □

6.6. **Theorem** (Fermat). *If the prime p is not a factor of a, then*
$$a^{p-1} \equiv 1 \pmod{p}.$$
Hence $a^p \equiv a \pmod{p}$ for any integer a.

Proof. The order of $(\mathbb{Z}/\langle p\rangle)^\times$ is $p - 1$, and $[a] \in (\mathbb{Z}/\langle p\rangle)^\times$. This proves the first claim. The second claim is trivial if $p \mid a$. □

If $n \neq 0$, let the order of $(\mathbb{Z}/\langle n\rangle)^\times$ be denoted by
$$\phi(n).$$

6.7. **Theorem** (Euler). *If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

7. Normal subgroups

A subgroup H of G is **normal** if its left and right cosets determine the same equivalence-relation, that is,
$$aH = Ha$$
for all a in G. There are various alternative formulations, most notably
$$aHa^{-1} \subseteq H.$$
If H is a normal subgroup of G, then one writes
$$H \trianglelefteqslant G.$$
Of abelian groups, all subgroups are normal.

7.1. **Theorem.** *Suppose $H \leqslant G$. Then $H \trianglelefteqslant G$ if and only if the equivalence-relation determined by the left cosets of H is a congruence-relation, that is, H/G is a well-defined group.*

Proof. Suppose G/H is a group. Then
$$a_0H = a_1H \;\&\; b_0H = b_1H \implies b_0a_0H = b_1a_1H.$$
In particular, say $a_0 = a_1 = a$ and $b_0 = b \in H$ and $b_1 = 1$. then $baH = aH$, so $a^{-1}baH = H$.

Conversely, suppose $H \trianglelefteqslant G$ and $a_0H = a_1H$ and $b_0H = b_1H$. Then $b_0a_0H = b_0Ha_0 = b_1Ha_0 = b_1a_0H = b_1a_1H$. □

If $N \trianglelefteqslant G$, then the group G/N is the **quotient-group** of G by N.

7.2. **Theorem.** *Normality is preserved in subgroups, that is, if $N \trianglelefteqslant G$ and $H \leqslant G$, then $N \cap H \trianglelefteqslant H$.*

Proof. The defining property of normal subgroups is universal, that is, $N \trianglelefteqslant G$ means $(G, N) \models \forall x\ \forall y\ (x \in N \to yxy^{-1} \in N)$. □

7.3. **Theorem.** *If $N \trianglelefteqslant G$, then $\langle N \cup H\rangle = NH$ for all subgroups H of G.*

Proof. If $N \trianglelefteqslant G$, then $NH = HN$, so if $n_0h_0, n_1h_1 \in NH$, then $n_0h_0h_1^{-1}n_1^{-1} \in NHHN = NHN = NNH = NH$. □

Does the converse hold? *Does it?*

7.4. **Theorem.** *The normal subgroups of a group are precisely the kernels of homomorphisms on the group.*

Proof. If f is a homomorphism from G to H, then $f(ana^{-1}) = f(a)f(n)f(a)^{-1} = 1$ for all n in $\ker f$, so $a(\ker f)a^{-1} \subseteq \ker f$.

If $N \trianglelefteqslant G$, then the map $x \mapsto xN$ from G to G/N is a homomorphism with kernel N. □

In the proof, the map $x \mapsto xN$ is the **canonical projection** of G onto G/N; it may be denoted by π.

7.5. **Lemma.** *If f is a homomorphism from G to H, and N is a normal subgroup of G such that $N \leqslant \ker f$, then there is a unique homomorphism $\tilde{f}$ from G/N to H such that $f = \tilde{f} \circ \pi$.*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, dotted, "\exists!"'] & \end{tikzcd}$$

Proof. If $\tilde{f}$ exists, it must satisfy $\tilde{f}(xN) = f(x)$ for all x in G. Such $\tilde{f}$ does exist, since if $xN = yN$, then $xy^{-1} \in N \leqslant \ker f$, so $f(xy^{-1}) = 1$ and $f(x) = f(y)$. □

7.6. **Theorem** (First Isomorphism). *$G/\ker f \cong \operatorname{im} f$ for any homomorphism f on G.*

Proof. In Lemma 7.5, let $N = \ker f$; then $\tilde{f}$ is the desired homomorphism. □

7.7. **Theorem** (Second Isomorphism). *If $H \leqslant G$ and $N \trianglelefteqslant G$, then*

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

Proof. The map $h \mapsto hN$ from H to HN/N is surjective with kernel $H \cap N$. □

7.8. **Example.** In $\mathbb{Z}$, since $\langle n\rangle \cap \langle m\rangle = \langle \gcd(n,m)\rangle$ and $\langle n\rangle \langle m\rangle = \langle \operatorname{lcm}(n,m)\rangle$, we have

$$\frac{\langle n\rangle}{\langle \gcd(n,m)\rangle} \cong \frac{\langle \operatorname{lcm}(n,m)\rangle}{\langle m\rangle}.$$

7.9. **Theorem** (Third Isomorphism). *If N and K are normal subgroups of G and $N \leqslant K$, then $K/N \trianglelefteqslant G/N$ and*

$$\frac{G/N}{K/N} \cong G/K.$$

Proof. By Lemma 7.5, the map $xN \mapsto xK$ from G/N to G/K is a well-defined epimorphism. The kernel contains xN if and only if $x \in K$, that is, $xN \in K/N$. □

8. Finite groups

By Cayley's Theorem, we know that any finite group embeds in the group of symmetries of a finite set, namely the universe of the group itself.

8.1. **Theorem.** *Suppose A is a set, and G is a* finite *subgroup of* $\operatorname{Sym}(A)$. *Then there is a* finite *subset B of A such that $\phi \restriction B \in \operatorname{Sym}(B)$ whenever $\phi \in G$, and the map $\phi \mapsto \phi \restriction B$ is an embedding of G in* $\operatorname{Sym}(B)$.

Proof. For any finite subset C of A, each ϕ in G permutes the finite subset
$$\{\xi(a)\colon \xi \in G \;\&\; a \in C\}$$
of A. Call this set $G(C)$. Then the map
$$\phi \mapsto \phi \restriction G(C)$$
from G to $\mathrm{Sym}(G(C))$ is a homomorphism. The set C can be chosen so that for each ϕ in G there is a in C so that $\phi(a) \neq a$; then the homomorphism is an embedding. □

We may consider any finite group as a subgroup of some $\mathrm{Sym}(n)$. (This is also denoted by S_n, although most writers may consider this as $\mathrm{Sym}(\{1, 2, \dots, n\})$.) An element σ of $\mathrm{Sym}(n)$ can be denoted by
$$\begin{pmatrix} 0 & 1 & \cdots & n-1 \\ \sigma(0) & \sigma(1) & \cdots & \sigma(n-1) \end{pmatrix}.$$
In particular, the permutation
$$\begin{pmatrix} 0 & 1 & \cdots & n-2 & n-1 \\ 1 & 2 & \cdots & n-1 & 0 \end{pmatrix}.$$
can be called a *cycle*. More generally, if $m \leqslant n$, then the permutation
$$\begin{pmatrix} 0 & 1 & \cdots & m-2 & m-1 & m & \cdots & n-1 \\ 1 & 2 & \cdots & m-1 & 0 & m & \cdots & n-1 \end{pmatrix}$$
can be called an *m-cycle*. If for the moment we call this permutation σ_m, then any σ in $\mathrm{Sym}(n)$ is an m-**cycle** or a cycle of **length** m if
$$\sigma = \tau\sigma_m\tau^{-1}$$
for some τ in $\mathrm{Sym}(n)$. The length of a cycle is its order. Also, σ can be written
$$\begin{pmatrix} \tau(0) & \tau(1) & \cdots & \tau(m-2) & \tau(m-1) & \tau(m) & \cdots & \tau(n-1) \\ \tau(1) & \tau(2) & \cdots & \tau(m-1) & \tau(0) & \tau(m) & \cdots & \tau(n-1) \end{pmatrix},$$
or more neatly as
$$\begin{pmatrix} \tau(0) & \tau(1) & \cdots & \tau(m-1) \end{pmatrix}.$$
In this notation, the same cycle σ can be written in m different ways, as
$$\begin{pmatrix} \tau(i) & \tau(i+1) & \cdots & \tau(i+m-1) \end{pmatrix},$$
for any i in n, where the arguments of τ are understood *modulo m*. If also σ' is a cycle $\begin{pmatrix} \tau'(0) & \cdots & \tau'(m'-1) \end{pmatrix}$ in $\mathrm{Sym}(n)$, then the two cycles are **disjoint** if $\tau(i) \neq \tau'(i')$ for any i in m and i' in m'. In this case, $\sigma\sigma' = \sigma'\sigma$.

8.2. **Theorem.** *Every element of* $\mathrm{Sym}(n)$ *is a product of disjoint cycles, uniquely up to order of factors.*

Proof. Let $\sigma \in \mathrm{Sym}(n)$. Then σ determines a partition of n whose elements are the subsets $\{\sigma^i(x)\colon i \in n\}$ of n, where $x \in n$. If such a subset has size $n(x)$, then σ is the product of the distinct (and therefore disjoint) cycles
$$\begin{pmatrix} x & \sigma(x) & \cdots & \sigma^{n(x)-1}(x) \end{pmatrix}.$$
Any factorization of σ into disjoint cycles determines the same partition and hence the same factors. □

8.3. **Corollary.** *The order of a finite permutation is the least common multiple of the orders of its disjoint cyclic factors.*

A 2-cycle is also called a **transposition.**

8.4. **Corollary.** *Every finite permutation is a product of transpositions.*

Proof. $\begin{pmatrix}0 & 1 & \cdots & m-1\end{pmatrix} = \begin{pmatrix}0 & m-1\end{pmatrix} \cdots \begin{pmatrix}0 & 2\end{pmatrix} \begin{pmatrix}0 & 1\end{pmatrix}$. □

8.5. **Theorem.** *If a finite permutation is factored into transpositions, the number of these transpositions is uniquely determined* modulo 2.

Proof. Let $\mathbb{Q}^\times$ be the set of multiplicatively invertible elements in $\mathbb{Q}$. Then $\mathbb{Q}^\times$ is a group, with subgroup $\langle -1 \rangle$. There is a homomorphism $x \mapsto \operatorname{sgn}(x)$, the **sign** or **signum,** from $\mathbb{Q}^\times$ to $\langle -1 \rangle$; it is given by

$$\operatorname{sgn}(x) = \begin{cases} -1, & \text{if } x < 0; \\ 1, & \text{if } 0 < x. \end{cases}$$

Then there is a homomorphism with the same name from $\operatorname{Sym}(n)$ to $\langle -1 \rangle$ given by

$$\operatorname{sgn}(\sigma) = \prod_{i<j<n} \operatorname{sgn}(\sigma(j) - \sigma(i)).$$

Also, $\operatorname{sgn}(\sigma) = -1$ if σ is a transposition. Hence an arbitrary permutation is the product of an odd number of transpositions if and only if $\operatorname{sgn}(\sigma) = -1$. □

A finite permutation σ can be called **even** if it is a product of an even number of transpositions, that is, $\operatorname{sgn}(\sigma) = 1$; otherwise $\operatorname{sgn}(\sigma) = -1$, and σ is **odd.**

8.6. **Remark.** For an alternative proof, let $f(X_0, \dots, X_{n-1})$ be the polynomial

$$\prod_{i<j<n} (X_j - X_i).$$

For any polynomial $g(X_0, \dots, X_{n-1})$, if $\sigma \in \operatorname{Sym}(n)$, then we may define

$$\sigma(g(X_0, \dots, X_{n-1})) = g(X_{\sigma(0)}, \dots, X_{\sigma(n-1)}).$$

In particular, σ permutes the 2-element set $\{f, -f\}$, so $\operatorname{Sym}(n)$ maps homomorphically into $\operatorname{Sym}(\pm f)$. The transposition $\begin{pmatrix}0 & 1\end{pmatrix}$ takes $\pm f$ to $\mp f$; hence the same is true for any transposition. Hence $\sigma f = f$ if and only if σ is a product of an even number of transpositions.

The **alternating group** of degree n is the kernel of $x \mapsto \operatorname{sgn}(x)$ on $\operatorname{Sym}(n)$ and is denoted by

$$A_n.$$

A group is **simple** if it has no proper non-trivial normal subgroups.

8.7. **Example.** $\mathbb{Z}/\langle n \rangle$ is simple just in case $|n|$ is prime. Hence the only simple Abelian groups are the $\mathbb{Z}/\langle p \rangle$, where p is prime.

8.8. **Lemma.** *A_n is generated by the 3-cycles.*

Proof. $\begin{pmatrix}0 & 1 & 2\end{pmatrix} = \begin{pmatrix}0 & 2\end{pmatrix} \begin{pmatrix}0 & 1\end{pmatrix}$ and $\begin{pmatrix}0 & 1\end{pmatrix} \begin{pmatrix}2 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 0\end{pmatrix} \begin{pmatrix}2 & 3 & 1\end{pmatrix}$. □

8.9. **Lemma.** *A_n is generated by the 3-cycles $\begin{pmatrix}0 & 1 & k\end{pmatrix}$, where $1 < k < n$.*

Proof. $\begin{pmatrix}0 & 2 & 3\end{pmatrix} = \begin{pmatrix}0 & 1 & 3\end{pmatrix}\begin{pmatrix}0 & 1 & 2\end{pmatrix}^{-1}$ and
$\begin{pmatrix}2 & 3 & 4\end{pmatrix} = \begin{pmatrix}0 & 1 & 2\end{pmatrix}^{-1}\begin{pmatrix}0 & 1 & 4\end{pmatrix}\begin{pmatrix}0 & 1 & 3\end{pmatrix}^{-1}\begin{pmatrix}0 & 1 & 2\end{pmatrix}$. □

8.10. **Lemma.** *Any normal subgroup of A_n containing a* 3*-cycle* is A_n.

Proof. $\begin{pmatrix}0 & 1 & 3\end{pmatrix} = \begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}0 & 1 & 2\end{pmatrix}^{-1}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix}$. □

8.11. **Lemma.** *If $n > 4$, then a normal subgroup of A_n contains a* 3*-cycle, provided it has a non-trivial element whose factorization into disjoint cycles contains one of the following:*

(1) *a cycle of order at least* 4*;*
(2) *two cycles of order* 3*;*
(3) *only one* 3*-cycle, and no cycles of order at least* 4*; or*
(4) *no cycles of length* 3 *or more.*

Proof. Suppose $N \trianglelefteqslant A_n$ and $\sigma\tau \in N$, where σ and τ are disjoint products of disjoint cycles. For any ζ in A_n, we have

$$\zeta(\sigma\tau)\zeta^{-1} \in N,$$

whence $\zeta(\sigma\tau)\zeta^{-1}(\sigma\tau)^{-1} \in N$. Assume ζ is disjoint from τ. Then

$$\zeta\sigma\zeta^{-1}\sigma^{-1} = \zeta(\sigma\tau)\zeta^{-1}(\sigma\tau)^{-1} \in N.$$

So it is enough now to note the following:

(1) $\begin{pmatrix}0 & 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1 & \dots & r-1\end{pmatrix}\begin{pmatrix}0 & 1 & 2\end{pmatrix}^{-1}\begin{pmatrix}0 & 1 & \dots & r-1\end{pmatrix}^{-1} =$
$\begin{pmatrix}0 & 1 & 3\end{pmatrix}$, if $r \geqslant 4$.
(2) $\begin{pmatrix}0 & 1 & 3\end{pmatrix}\begin{pmatrix}0 & 1 & 2\end{pmatrix}\begin{pmatrix}3 & 4 & 5\end{pmatrix}\begin{pmatrix}0 & 1 & 3\end{pmatrix}^{-1}\begin{pmatrix}3 & 4 & 5\end{pmatrix}^{-1}\begin{pmatrix}0 & 1 & 2\end{pmatrix}^{-1} =$
$\begin{pmatrix}0 & 1 & 4 & 2 & 3\end{pmatrix}$.
(3) If τ is disjoint from $\begin{pmatrix}0 & 1 & 2\end{pmatrix}$, then $(\begin{pmatrix}0 & 1 & 2\end{pmatrix}\tau)^2 = \begin{pmatrix}0 & 1 & 2\end{pmatrix}^{-1}\tau^2$.
(4) We can eliminate all but two transpositions, since

$$\begin{pmatrix}0 & 1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}0 & 1 & 2\end{pmatrix}^{-1}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 2\end{pmatrix}\begin{pmatrix}1 & 3\end{pmatrix}.$$

Also $\begin{pmatrix}0 & 2 & 4\end{pmatrix}\begin{pmatrix}0 & 2\end{pmatrix}\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}0 & 2 & 4\end{pmatrix}^{-1}\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}0 & 2\end{pmatrix} = \begin{pmatrix}0 & 4 & 2\end{pmatrix}$.

This completes the proof. □

8.12. **Theorem.** *A_n is simple if $n \neq 4$, but A_4 is not simple.*

Proof. A_1 and A_2 are trivial, and $A_3 \cong \mathbb{Z}/\langle 3\rangle$, while A_4 has the normal subgroup

$$\left\langle \begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}, \begin{pmatrix}0 & 2\end{pmatrix}\begin{pmatrix}1 & 3\end{pmatrix}, \begin{pmatrix}0 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}\right\rangle.$$

The case when $n > 4$ is handled by the previous lemmas. □

Here's a way to prove that A_5 is simple by counting and using the following

8.13. **Lemma.** *If $N \trianglelefteqslant G$ and $x \in G$, and the index of N in G and the order of x are finite and relatively prime, then $x \in N$.*

Now, A_5 has $5!/2$ or 60 elements, namely:

- 1 identity;
- 15 products $\begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}c & d\end{pmatrix}$;
- 20 cycles of order 3;
- 24 cycles of order 5.

Suppose $N \trianglelefteqslant A_5$, so $|N|$ divides $2^2 \cdot 3 \cdot 5$:

- If $|N|$ is a multiple of 3, then $[A_5 : N]$ is prime to 3, so N contains all 3-cycles, hence all elements of A_5.
- If $|N|$ is a multiple of 5, then $[A_5 : N]$ is prime to 5, so N contains the 24 cycles of order 5, and again N must be A_5.
- If $|N|$ is a multiple of 4, then $[A_5 : N]$ is prime to 4, so N contains the 15 products $\begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}c & d\end{pmatrix}$, and $N = A_5$.
- If $|N| = 2$, then $N = \left\langle \begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}c & d\end{pmatrix} \right\rangle$, but this is not normal.

The **dihedral group** D_n is the subgroup

$$\left\langle \begin{pmatrix}0 & 1 & \dots & n-1\end{pmatrix}, \prod_{0<i<n/2} \begin{pmatrix}i & n-i\end{pmatrix} \right\rangle;$$

it can be seen as the group of symmetries of a regular n-gon.

8.14. **Theorem.** *If $n > 2$, then D_n is the unique group (up to isomorphism) with two generators a and b such that $|a| = n$ and $|b| = |ab| = 2$; the group has order $2n$.*

Proof. D_n does meet the given discription. Suppose G does. Since $abab = 1$, we have $ba = a^{-1}b$ and $ba^{-1} = ab$, whence $ba^r = a^{-r}b$ for all integers r. Hence $G = \{a^i b^j : (i,j) \in n \times 2\}$. Suppose $a^i b^j = 1$, where $(i,j) \in n \times 2$. Then $a^i = b^j$, so $a^{2i} = 1$, which means $2i \in \{0, n\}$. So if n is odd, then $(i,j) = (0,0)$. If $n = 2m$, then $aa^m aa^m = a^2 \neq 1$, so $i \neq m$, and again $(i,j) = (0,0)$. □

9. The category of groups

For any two groups G and H there is a set

$$\mathrm{Hom}(G,H)$$

comprising the homomorphisms from G to H. There is a map

$$(g,f) \mapsto g \circ f$$

from $\mathrm{Hom}(H,K) \times \mathrm{Hom}(G,H)$ to $\mathrm{Hom}(G,K)$, and there is id_H in $\mathrm{Hom}(H,H)$, such that

$$\mathsf{id}_H \circ f = f, \quad g \circ \mathsf{id}_H = g, \quad k \circ (g \circ f) = (k \circ g) \circ f$$

whenever these equations make sense. Therefore groups with their homomorphisms compose a *category.*

A category can be seen as a kind of *graph,* according to one definition of the term, namely: a **graph** $\mathfrak{G}$ is a quadruple

$$(\mathbf{G}_0, \mathbf{G}_1, t, h),$$

where $\mathbf{G}_0$ and $\mathbf{G}_1$ are classes, and t and h are functions from $\mathbf{G}_1$ to $\mathbf{G}_0$. We may refer to each element of $\mathbf{G}_0$ as a **node,** and to each element of $\mathbf{G}_1$ as an **arrow.** If a is an arrow, then $t(a)$ is its **tail,** and $h(a)$ is its **head,** and a is an **arrow from** $t(a)$ **to** $t(b)$. If f is an arrow from A to B, we may write $f\colon A \to B$ or $A \xrightarrow{f} B$. One might like to require the arrows from A to B to compose a set. We can define

$$\mathbf{G}_2 = \{(\xi,\eta) \in {\mathbf{G}_1}^2 \colon t(\xi) = h(\eta)\};$$

this is the class of paths of length 2. More generally,

$$\mathbf{G}_{n+1} = \left\{ \boldsymbol{\xi} \in {\mathbf{G}_1}^{n+1} \colon \bigwedge_{i<n} t(\xi_i) = h(\xi_{i+1}) \right\}.$$

Suppose $\mathfrak{C}$ is a graph, and

$$A \mapsto \mathsf{id}_A \colon \mathbf{C}_0 \to \mathbf{C}_1 \quad \text{and} \quad (f,g) \mapsto f \circ g \colon \mathbf{C}_2 \to \mathbf{C}_1,$$

where $t(\mathsf{id}_A) = h(\mathsf{id}_A) = A$, and $t(f \circ g) = t(g)$, and $h(f \circ g) = h(f)$, and

$$f \circ \mathsf{id}_B = f, \quad \mathsf{id}_A \circ g = g, \quad f \circ (g \circ h) = (f \circ g) \circ h$$

whenever these make sense. Then $\mathfrak{C}$ is a **category.** The arrows of a category are also called **morphisms.** The morphism $f \circ g$ is the **composite** of f and g.

A category is **concrete** if each of its objects has an underlying set, and the morphisms are maps in the way suggested by the notation.

9.1. **Example.** The class of sets, with the class of functions, is a concrete category.

Not all categories are concrete:

9.2. **Example.** If G is a group, then its elements can be considered as objects of a category in which $\mathrm{Hom}(a,b) = \{ba^{-1}\}$ and $\mathsf{id}_a = 1$ and $c \circ d = cd$.

In a category, a morphism f is an **isomorphism** if

$$g \circ f = \mathsf{id}_{t(f)} \quad \text{and} \quad f \circ g = \mathsf{id}_{h(f)}$$

for some morphism g; then g is an **inverse** of f.

9.3. **Lemma.** *In a category, inverses are unique.*

Proof. If g and h are inverses of f, then $g = g \circ \mathsf{id}_{h(f)} = g \circ (f \circ h) = (g \circ f) \circ h = \mathsf{id}_{t(f)} \circ h = h$. $\square$

If it exists, then the inverse of f is f^{-1}. It is immediate then that $(f^{-1})^{-1} = f$.

Let I be an index-set, and let i range over this. For any class $\mathbf{D}$, let $\mathbf{D}^I$ be the class of functions from I to $\mathbf{D}$. If it exists, a **product** of an element A of ${\mathbf{C}_0}^I$ is an element of $\mathbf{C}_0 \times {\mathbf{C}_1}^I$, denoted by

$$\left(\prod A, \boldsymbol{\pi}\right)$$

or $\left(\prod_{i\in I} A_i, (\pi_i \colon i \in I)\right)$, where

$$\pi_i \colon \prod A \to A_i,$$

and whenever $(B, \boldsymbol{f}) \in \mathbf{C}_0 \times {\mathbf{C}_1}^I$ and $f_i \colon B \to A_i$, then $g \colon B \to \prod A$, and

$$\pi_i \circ g = f_i$$

for each i in I, for some unique g.

$$\begin{tikzcd} \prod A \arrow[r, "\pi_i"] & A_i \\ B \arrow[u, dotted, "\exists!"] \arrow[ur, "f_i"'] & \end{tikzcd}$$

The morphisms π_i are the **canonical projections.**

9.4. **Lemma.** *Products are unique when they exist.*

(One can define commutative diagrams formally. A **diagram** is a homomorphism from a graph to a category. One then thinks of the diagram as the graph with its nodes and arrows labelled with their images in the category. The diagram is **commutative** if every path in the graph with the same tail and head is sent to the same morphism in the category.)

9.5. **Theorem.** *The category of groups has products. In fact,*

$$\prod_{i\in I} G_i = \Big\{\boldsymbol{\xi} \in \Big(\bigcup_{i\in I} G_i\Big)^I : \xi_i \in G_i\Big\} \qquad \textit{and } \pi_i\boldsymbol{g} = g_i.$$

Proof. It is clear that $\prod G$ is a group. Suppose $f_i\colon H \to G_i$. Then we can define a homomorphism h from H to $\prod G$ by

$$h(x)_i = f_i(x),$$

that is, $\pi_i(h(x)) = f_i(x)$, that is, $\pi_i \circ h = f_i$. Thus h is the unique homomorphism satisfying the last equation. $\square$

Every category $\mathfrak{C}$ has a **dual category,** $\mathfrak{C}^*$, in which the arrows are reversed, so that

$$t^*(f) = h(f), \quad h^*(f) = t(f), \quad g \circ^* f = f \circ g, \quad \mathsf{id}^*_A = \mathsf{id}_A.$$

A **co-product** or **sum** in a category is a product in the dual and may be denoted by

$$\Big(\coprod A, \boldsymbol{\iota}\Big) \quad \text{or} \quad \Big(\sum A, \boldsymbol{\iota}\Big);$$

the maps ι_i are the **canonical injections.**

$$\begin{tikzcd} \coprod A \arrow[d, dotted, "\exists!"'] & A_i \arrow[l, "\iota_i"'] \arrow[dl, "f_i"] \\ B & \end{tikzcd}$$

9.6. **Theorem.** *Sums exist in the category of* abelian *groups. In fact,*

$$\sum_{i\in I} G_i = \{\boldsymbol{\xi} \in \prod_{i\in I} G_i\colon\ |\{i \in I\colon \xi_i \neq 0\}| < \infty\} \qquad \textit{and} \qquad \iota_i(x)_j = \begin{cases} x, & \textit{if } i = j; \\ 0, & \textit{if } i \neq j. \end{cases}$$

Proof. It is clear that $\sum G$ is a group. Suppose $f_i\colon G_i \to H$. Then we can define a homomorphism h from $\sum G$ to H by

$$h(g) = \sum_{i\in I} f_i(g_i).$$

Then h is a well-defined homomorphism, and

$$h(\iota_i(g)) = f_i(g)$$

when $g \in G_i$, that is, $h \circ \iota_i = f_i$. This condition determines h as a homomorphism. $\square$

Suppose F is an object in a concrete category and A is a set. Then F is called **free** on A if there is a map i from A to F, and for any map f from A to an object, there is a unique morphism $\tilde{f}$ from F to the object such that $\tilde{f} \circ i = f$: that is, the following diagram commutes (although the nodes and arrows are from the category of sets):

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[dr] & F \arrow[d, dotted, "\exists!"] \\ & B \end{tikzcd}$$

9.7. **Theorem.** *The category of groups has free objects on all sets.*

Proof. Let A be a set, let $x \mapsto x^{-1}$ be a bijection between A and a disjoint set, let $x \mapsto x^{+1}$ be the identity on A, and let $x \mapsto -x$ be the non-trivial permutation of $\{+1, -1\}$. Let F be the set of all finite sequences whose terms are $a^{\pm 1}$, where $a \in A$, and in which a^{+1} and a^{-1} are never adjacent. Then F is a group when the product is defined by

$$(a_{m-1}^{\epsilon(m-1)} \cdots a_0^{\epsilon(0)})(b_0^{\zeta(0)} \cdots b_{n-1}^{\zeta(n-1)}) = a_{m-1}^{\epsilon(m-1)} \cdots a_j^{\epsilon(j)} b_j^{\zeta(j)} \cdots b_{n-1}^{\zeta(n-1)},$$

where j is maximal such that $a_i^{\epsilon(i)} = b_i^{-\zeta(i)}$ when $i < j$. Then F is a group (in which the identity is the empty sequence), and F is the free group on A. $\square$

Elements of the free group on A are **reduced words** on A. (A **word** on A is just a finite sequence whose terms are $a^{\pm 1}$ or 1.)

9.8. **Theorem.** *The category of abelian groups has free objects on all sets.*

Proof. The free abelian group on A is $\sum_{i \in A} \mathbb{Z}$, into which A maps by the function f given by

$$f(x)_i = \begin{cases} 1, & \text{if } i = x; \\ 0, & \text{if } i \neq x. \end{cases}$$

Indeed, if g is a map from A into an abelian group G, then we have

$$\xi \mapsto \sum_{i \in A} \xi_i \cdot g(i)$$

from $\sum_{i \in A} \mathbb{Z}$ to G, and this is the unique function $\tilde{g}$ such that $\tilde{g} \circ f = g$. $\square$

The **free product** of a family $(G_i : i \in I)$ of groups is defined in the way F is in the proof of Theorem 9.7: it is the set, denoted by

$$\prod_{i \in I}^{*} G_i,$$

of sequences of non-identity elements of the G_i, no two adjacent entries being from the same group. (So the groups are considered to be disjoint, except for their identities.) Multiplication on $\prod^{*}_{i \in I} G_i$ is defined in the obvious way: it is juxtaposition, followed by multiplication of adjacent terms from the same group, with identities deleted.

9.9. **Theorem.** *Co-products exist in the category of groups; in fact,*

$$\coprod_{i \in I} G_i = \prod_{i \in I}^{*} G_i,$$

and the ι_i are the obvious injections.

Proof. Suppose $f_i : G_i \to H$. We can define h from $\prod^{*}_{i \in I} G_i$ to H by

$$h(g_0 \cdots g_{m-1}) = f_{n(0)}(g_0) \cdots f_{n(m-1)}(g_{m-1}),$$

where $g_i \in G_{n(i)}$. Then h is unique such that $h \circ \iota_i = f_i$. $\square$

10. Products of groups

Strictly speaking, a product $\prod_{i\in I} G_i$ is the product, not of the set $\{G_i \colon i \in I\}$, but of the 'indexed set' or function $(G_i \colon i \in I)$; however, not all writers observe this. For example, if $I = 2$, then $(G_i \colon i \in I)$ might be (G, G), with product $G \times G$; but $\{G_i \colon i \in I\}$ would be $\{G\}$, and G is not $G \times G$.

Instead of $\prod_{i<n} G_i$, we may write

$$G_0 \times \cdots \times G_{n-1},$$

or $G_0 \oplus \cdots \oplus G_{n-1}$ if the groups are abelian.

In the general case, the set

$$\Bigl\{g \in \prod_{i\in I} G_i \colon\ |\{i \in I : g_i \neq 1\}| < \infty\Bigr\}$$

is the **weak direct product** of $(G_i \colon i \in I)$ and is denoted by

$$\prod_{i\in I}^{\mathrm{w}} G_i;$$

but in the abelian case this is just the **direct sum**

$$\sum_{i\in I} G_i.$$

Note that weak direct products are *not* sums in the category of groups.

10.1. **Theorem.** $\prod^{\mathrm{w}}_{i\in I} G_i \trianglelefteq \prod_{i\in I} G_i$, *and the natural image of each* G_j *in* $\prod^{\mathrm{w}}_{i\in I} G_i$ *is also normal.*

10.2. **Lemma.** *If* M *and* N *are normal subgroups of* G, *and* $M \cap N = \langle 1\rangle$, *then* $mn = nm$ *for all* m *in* M *and* n *in* N.

Proof. The group-element $mnm^{-1}n^{-1}$ can be analyzed as the element

$$(mnm^{-1})n^{-1}$$

of N and as $m(nm^{-1}n^{-1})$ in M; so it is 1, which means $mn = (m^{-1}n^{-1})^{-1} = nm$. □

10.3. **Theorem.** *If* $N_i \trianglelefteq G$ *for each* i *in* I, *and*

$$G = \Bigl\langle \bigcup_{i\in I} N_i \Bigr\rangle,$$

while

$$N_j \cap \Bigl\langle \bigcup_{i\in I\smallsetminus\{j\}} N_i \Bigr\rangle = \langle 1\rangle\,,$$

then $G \cong \prod^{\mathrm{w}}_{i\in I} N_i$.

Proof. By Lemma 10.2, there is an obvious homomorphism from $\prod^{\mathrm{w}}_{i\in I} N_i$ into G. It is surjective, since the N_i generate G. It is injective, since if $n \in N_j$ and $m \in \prod^{\mathrm{w}}_{i\in I\smallsetminus\{j\}} N_i$ and $nm = 1$, then $n = m^{-1}$, so n is also in $\bigl\langle \bigcup_{i\in I\smallsetminus\{j\}} N_i \bigr\rangle$ and is therefore 1. □

In the conclusion of the theorem, G is the **internal** weak direct product of the N_i.

11. Presentation of groups

11.1. **Theorem.** *Every group is isomorphic to a quotient F/N, where F is a free group.*

Proof. Let F be the free group on G and let N be the kernel of the induced homomorphism from F onto G. □

The normal subgroup **generated** by a subset of a group is the intersection of the normal subgroups that include the subset. If A is a set, F is a free group on A, and $B \subseteq F$, let N be the normal subgroup of F generated by B. Then the group F/N is the **group on** A with **relations** B, denoted by

$$\langle A \mid B \rangle .$$

Note that, strictly, this group is generated by the *image* of A, not by A itself; indeed, the natural map from A into $\langle A \mid B \rangle$ need not be injective.

11.2. **Theorem** (Dyck[3]). *If F is a free group on A, and B is included in the kernel of an epimorphism f from F into a group G (that is, the relations B hold in G), then f factors through $\langle A \mid B \rangle$.*

$$\begin{tikzcd} F \arrow[r, "f"] \arrow[d] & G \\ \langle A \mid B \rangle \arrow[ur, dotted] & \end{tikzcd}$$

In particular, $f = g \circ h$, where h is an epimorphism from $\langle A \mid B \rangle$ onto G.

11.3. **Example.** If F is the free group on A, then $F = \langle A \mid \varnothing \rangle$.

11.4. **Example.** $\mathbb{Z}/\langle n \rangle = \langle a \mid a^n \rangle$.

11.5. **Example.** $D_n = \langle a, b \mid a^n, b^2, (ab)^2 \rangle$.

[3]Walther von Dyck (1856–1934) gave an early (1882–3) definition of abstract groups [2, ch. 49, p. 1141].

Part 2. Analysis of groups

12. Two

An **involution** is an element of order 2 in a group.

12.1. **Lemma.** *A group of even order contains an involution.*

Proof. Let $A = \{x \in G\colon x \neq x^{-1}\}$. Then

$$|G| = |A| + 1 + |\{x \in G\colon\ |x| = 2\}|\,.$$

Now, $|A|$ is even. If also $|G|$ is even, then $\{g \in G\colon\ |g| = 2\}$ must be non-empty. □

12.2. **Theorem.** *A group of order twice an odd number contains a subgroup of index* 2 *(the subgroup is therefore normal).*

Proof. Say $|G| = 2m$; then G contains an element g of order 2. We the embedding $x \mapsto \lambda_x$ of G in $\mathrm{Sym}(G)$; we can identify G with the image of this embedding. Now, λ_g is the product of m disjoint 2-cycles, an odd permutation. Hence the even permutations in G compose a subgroup of index 2. (That is, the homomorphism $x \mapsto \mathrm{sgn}(x)$ from G to $\{\pm 1\}$ is surjective.) □

13. Finitely generated abelian groups

A general problem now is to classify all groups: to find reasonable functions on the class of groups whose values at a given group determine the group up to isomorphism.

The problem is made easier if we restrict attention to a sub-class of groups: say, first, finitely generated abelian groups.

13.1. **Lemma.** *Suppose G is an abelian group generated by the subset $A \cup B$, where the elements of A have finite order, and elements of B, infinite order. Then G is the direct sum $\langle A\rangle \oplus \langle B\rangle$.*

Proof. Since G is abelian, all elements of $\langle A\rangle$ have finite order, but all nontrivial elements of $\langle B\rangle$ have infinite order. Hence $\langle A\rangle \cap \langle B\rangle = \langle 0\rangle$, so Theorem 10.3 applies. □

13.2. **Remark.** The proof fails if G is not abelian: $\langle a, b \mid a^2, b^2\rangle$ has elements of infinite order, and $\langle c, d \mid (cd)^2\rangle$ has nontrivial elements of finite order, but is generated by elements of infinite order.

A **basis** for a free abelian group is a subset on which the group is free (in the natural way). That is, suppose F is free abelian, and $A \subseteq F$. Then A is a basis of F if and only if the induced homomorphism from $\sum_{x\in A} \langle x\rangle$ into F is an isomorphism. We may then write $F = \sum_{x\in A} \langle x\rangle$. (However, this notation makes sense even if A is not a basis of F.)

The following three lemmas are based on [3, I, § 7].

13.3. **Lemma.** *If G and F are abelian groups, F being free, and if ϕ is an epimorphism from G onto F, then $G = H \oplus \ker\phi$ for some subgroup H of G that is isomorphic to F under ϕ.*

Proof. Let A be a basis of F, and let B be a subset of G mapped bijectively onto A by ϕ. Then let H be $\langle B\rangle$. □

13.4. **Lemma.** *A subgroup of a free abelian group on a finite set is free.*

Proof. The claim is true for free groups on singletons. Suppose it is true for free groups on sets of size n. Let F be free on $\{x_0, \dots, x_n\}$, and say $G \leqslant F$. Let ϕ be the restriction to G of the epimorphism $\sum_{i=0}^{n} c_i x_i \mapsto c_n$ from F to $\mathbb{Z}$. By the previous lemma, $G = H \oplus \ker \phi$, where H is infinite-cyclic; by inductive hypothesis, $\ker \phi$ is free. $\square$

13.5. **Lemma.** *An abelian group generated by finitely many elements, all of infinite order, is free.*

Proof. Let A be a finite set of generators of the abelian group G, all elements of A having infinite order. Let $\{x_i \colon i < n\}$ be a maximal subset of A such that

$$\sum_{i<n} c_i x_i = 0 \implies \bigwedge_{i<n} c_i = 0$$

for all c_i in $\mathbb{Z}$. Hence, for every u in A, there are integers c_i and d in $\mathbb{Z}$ such that

$$\sum_{i<n} c_i x_i + du = 0$$

and $u \neq 0$. Let F be $\langle x_i \colon i < n \rangle$; then F is free. Since A is finite, we have $dG \leqslant F$ for some integer d. By the previous lemma, dG must be free; but this is isomorphic to G. $\square$

13.6. **Lemma.** *Any finitely generated abelian group is the direct sum of a free group and a finite group.*

Proof. Any generating set of an abelian group G can be written $A \cup B$, where the elements of A have finite order, and the elements of B, infinite. Then $G = \langle A \rangle \oplus \langle B \rangle$. If A and B are finite, then $\langle B \rangle$ is free by the previous lemma, and $\langle A \rangle$ is finite. $\square$

Now we want to analyze finite abelian groups.

13.7. **Lemma.** *If G is finite abelian, and p is a prime dividing $|G|$, then G has an element of order p.*

Proof. Suppose the claim holds when $|G| < |H|$, and p divides $|H|$. Let x be a non-trivial element of H. If p divides $|x|$, then $(|x|/p)x$ has order p. Suppose p does not divide $|x|$. Then p divides $|G/\langle x \rangle|$. By inductive hypothesis, $G/\langle x \rangle$ has an element $u + \langle x \rangle$ of order p. Then $pu \in \langle x \rangle$, so p divides $|u|$, whence $(|u|/p)u$ has order p. $\square$

13.8. **Lemma.** *If G is abelian and $|G| = n_0 n_1$, where $\gcd(n_0, n_1) = 1$, then $G = H_0 \oplus H_1$ for some subgroups H_i such that $|H_i| = n_i$.*

Proof. Let $H_i = \{x \in G \colon n_i x = 0\}$; this is a subgroup of G since G is abelian. There are integers a_i such that

$$a_0 n_0 + a_1 n_1 = 1.$$

Hence we have

$$x \in H_0 \cap H_1 \implies n_0 x = 0 = n_1 x \implies x = (a_0 n_0 + a_1 n_1)x = 0$$

for all x in G; also

$$x = (a_0 n_0 + a_1 n_1)x = a_0 n_0 x + a_1 n_1 x \in H_1 + H_0.$$

Therefore $G = H_0 \oplus H_1$. Finally, suppose if possible that p divides both $|H_i|$ and n_{1-i}. Then H_i has an element x of order p, but x is also in H_{1-i}, so $x = 0$, which is absurd. Hence $|H_i|$ divides n_i, so it *is* n_i. $\square$

By induction, we now have

13.9. **Theorem.** *If G is abelian and $|G| = \prod_{i<n} p_i^{a(i)}$, where $(p_i : i < n)$ is a tuple of distinct primes, then*

$$G = \sum_{i<n} H_i,$$

where $|H_i| = p_i^{a(i)}$.

13.10. **Theorem.** *If G is abelian and $|G| = p^n$, then G is a direct sum of cyclic groups.*

Proof. By induction on $|G|$, we shall show that if g is an element of G of maximal order, then

$$G = \langle g \rangle \oplus H$$

for some subgroup H of G. There are two cases:

Suppose first that $\langle g \rangle$ contains all elements of G of order p. The order of g is p^e for some e. Let ϕ be the endomorphism $x \mapsto px$ of G. Then $\ker \phi^e = G$, by maximality of $|g|$. But also, $\ker \phi \leqslant \langle g \rangle$, and therefore $\ker \phi$ is $\langle p^{e-1} g \rangle$, which has order p, which means $|\ker \phi^e| = p^e$. Therefore $G = \langle g \rangle$.

Now suppose on the contrary that G has an element h of order p that is not in $\langle g \rangle$. The order of any u in G is at least as great as the order of $u + \langle h \rangle$ in $G/\langle h \rangle$. The order of $g + \langle h \rangle$ *is* $|g|$—and is therefore maximal—since if $mg \in \langle h \rangle$, then mg is in $\langle h \rangle \cap \langle g \rangle$, that is, $\langle 0 \rangle$. By inductive hypothesis then,

$$G/\langle h \rangle = \langle g + \langle h \rangle \rangle \oplus H/\langle h \rangle$$

for some subgroup H of G. Then $G = \langle g \rangle + H$, and in fact the sum is direct, since

$$z \in \langle g \rangle \cap H \implies z + \langle h \rangle \in \langle g + \langle h \rangle \rangle \cap H/\langle h \rangle = \langle h \rangle,$$

so if $z \in \langle g \rangle \cap H$, then $z \in \langle g \rangle \cap \langle h \rangle = \langle 0 \rangle$. □

13.11. **Theorem.** *A cyclic group of prime-power order has no proper non-trivial direct summand.*

Proof. All elements of $\sum_{i<n} \mathbb{Z}/\langle p^{a(i)} \rangle$ have order dividing p^b, where b is the maximum of the $a(i)$. □

So now the number of non-isomorphic abelian groups of a given finite order depends on the prime factorization of that order. In particular, the number of order p^n is the number of ways to write n as a sum:

13.12. **Example.** $400 = 2^4 \cdot 5^2$, and $4 = 1 + 3 = 2 + 2 = 1 + 1 + 2 = 1 + 1 + 1 + 1$, while $2 = 1 + 1$, so there are $5 \cdot 2$ or 10 non-isomorphic abelian groups of order 400.

13.13. **Theorem.** *If $\gcd(m, n) = 1$, then $\mathbb{Z}/\langle m \rangle \oplus \mathbb{Z}/\langle n \rangle = \mathbb{Z}/\langle mn \rangle$.*

Proof. If $g + \langle mn \rangle$ is in the kernel of $x + \langle mn \rangle \mapsto (x + \langle m \rangle, x + \langle n \rangle)$, then both m and n divide g, so mn divides g. So the map is injective; by counting, it is surjective. □

13.14. **Theorem.** *Any finite abelian group can be written*

$$\sum_{i<n} \mathbb{Z}/\langle m_i \rangle,$$

where m_i divides m_{i+1}.

14. Actions of groups

See Appendix A for an alternative development.

An **action** of a group G on a set A is a homomorphism from G to $\mathrm{Sym}(A)$; equivalently, it is a map

$$(x, \xi) \mapsto x\xi$$

from $G \times A$ to A such that $1a = a$ and $(gh)a = g(ha)$. (Strictly, we have defined a **left action.**)

14.1. **Example.** $\mathrm{Sym}(A)$ acts on A in the obvious way.

14.2. **Example.** Left-multiplication, $x \mapsto \lambda_x$ from G to $\mathrm{Sym}(G)$, is an action.

If G is a group, then the subgroup of $\mathrm{Sym}(G)$ comprising the automorphisms of G can be denoted by

$$\mathrm{Aut}(G).$$

If $g \in G$, then **conjugation** by g is the automorphism

$$x \mapsto gxg^{-1}.$$

Then G acts on itself by conjugation.

If G acts on A, and $a \in A$, then:

- the subset $\{x \colon xa = a\}$ of G is the **stabilizer** of a, denoted by G_a;
- the subset $\{xa \colon x \in G\}$ of A is the **orbit** of a, denoted by Ga;
- the subset $\{x \colon G_x = G\}$ of A can be denoted by A_0.

14.3. **Lemma.** *Suppose G acts on A, and $a \in A$. Then:*

(1) $G_a \leqslant G$;
(2) $[G : G_a] = |Ga|$;
(3) *the orbits partition A;*
(4) *if there are finitely many orbits, then*

$$|A| = |A_0| + \sum_{i<n} [G : G_{g(i)}]$$

*(the **class equation**) for some $g(i)$ in G whose orbits are non-trivial.*

If G is understood to act on itself by conjugation, and $g \in G$, then:

- G_0 is $\mathrm{C}(G)$, the **center** of G;
- G_g is $\mathrm{C}_G(g)$, the **centralizer** of g.

So the elements of the center of the group commute with all elements of the group; in particular, the center is abelian and is a normal subgroup. The centralizer of g is the largest subgroup H of G such that g is in the center of H.

A p-**group** is a group whose order is a power of p.

14.4. **Lemma.** *If A is acted on by a p-group, then $|A| \equiv |A_0| \pmod{p}$.*

Proof. In the previous lemma, $[G : G_{g(i)}]$ is a multiple of p in each case. □

15. Finite groups

15.1. **Theorem.** *Every non-trivial p-group has non-trivial center.*

Proof. By the last lemma, we have

$$|G| \equiv |\mathrm{C}(G)| \pmod{p},$$

so p divides $|\mathrm{C}(G)|$. Since $\mathrm{C}(G)$ contains one element, it contains at least p of them. □

15.2. **Theorem.** *All groups of order p^2 are abelian.*

Proof. Let G have order p^2. Then either $\mathrm{C}(G)$ is all of G, or else $|\mathrm{C}(G)| = p$, by the previous theorem. In any case, there is a in G such that

$$G = \langle \{a\} \cup \mathrm{C}(G) \rangle .$$

Then every element of G has the form $a^n h$ for some n in $\mathbb{Z}$ and h in $\mathrm{C}(G)$. But

$$(a^m h)(a^n h') = a^m a^n h h' = a^n a^m h' h = (a^n h')(a^m h),$$

so G is abelian. □

15.3. **Theorem** (Cauchy)**.** *If p divides $|G|$, then $|g| = p$ for some g in G.*

Proof (J. H. McKay [4]). Let $A = \{x \in G^p \colon x_0 \cdots x_{p-1} = 1\}$. If $a \in A$ and $k < p$, then

$$(a_0 \cdots a_{k-1})^{-1} = a_k \cdots a_{p-1},$$

hence we have an action

$$(\xi, x) \mapsto x_\xi \cdots x_{p-1} x_0 \cdots x_{\xi-1}$$

of $\mathbb{Z}/\langle p \rangle$ on A, and $A_0 = \{x \in A \colon x_0 = \cdots = x_{p-1}\}$. Now, the map

$$x \mapsto (x_0, \dots, x_{p-2}, (x_0 \cdots x_{p-2})^{-1})$$

from G^{p-1} to A is a bijection, so $|A|$ is a multiple of p; hence $|A_0|$ is a multiple of p, by Lemma 14.4. Since A_0 contains $(1, \dots, 1)$, it contains some $(a, \dots, a)$, where $|a| = p$. □

15.4. **Lemma.** *A group is a p-group if and only if the order of every element is a power of p.*

Proof. If ℓ is a prime dividing $|g|$, then ℓ divides $|G|$. Conversely, if ℓ divides $|G|$, then G has an element of order ℓ. □

Hence the definition of p-group can be generalized, so that an infinite group is a p-group if the order of its every element is a power of p.

A p-**subgroup** is a subgroup that is a p-group. A **Sylow** p-subgroup is a maximal p-subgroup.

If $H \leqslant G$, then the set $\{x \in G \colon xHx^{-1} = H\}$ is the **normalizer** of H in G, denoted by

$$\mathrm{N}_G(H);$$

it is the largest subgroup of G of which H is a normal subgroup.

15.5. **Lemma.** *If H is a p-subgroup of G, then*

$$[G : H] \equiv [\mathrm{N}_G(H) : H] \pmod{p}.$$

Proof. Let H act on the set G/H of cosets by left multiplication. Then

$$(G/H)_0 = \mathrm{N}_G(H)/H,$$

since the following are equivalent:

(1) $gH \in (G/H)_0$;
(2) $hgH = gH$ for all h in H;
(3) $g^{-1}hg \in H$ for all h in H;
(4) $g^{-1}Hg = H$;
(5) $g^{-1} \in \mathrm{N}_G(H)$;
(6) $g \in \mathrm{N}_G(H)$.

Now use Lemma 14.4. □

15.6. **Theorem** (Sylow I). *Of a finite group, every p-subgroup is included in a Sylow group, whose index is not a multiple of p.*

Proof. Suppose G has a p-subgroup H whose index is a multiple of p. By the lemma, p divides $[\mathrm{N}_G(H) : H]$. By Cauchy's Theorem, since $\mathrm{N}_G(H)/H$ is a group, it has a subgroup K/H of order p. So K is a p-subgroup of G that includes H. Repetition yields the claim. □

15.7. **Theorem** (Sylow II). *All Sylow p-subgroups are conjugate.*

Proof. Say H and P are p-subgroups of G, where P is maximal. Now, H acts on the set G/P by left multiplication. Then the following are equivalent:

(1) $xP \in (G/P)_0$;
(2) $hxP = xP$ for all h in H;
(3) $x^{-1}Hx \subseteq P$;
(4) $H \subseteq xPx^{-1}$.

Since $[G : P]$ is not a multiple of p, the claim follows by Lemma 14.4. □

15.8. **Theorem** (Sylow III). *The number of Sylow p-subgroups of a finite group is congruent to* 1 modulo *p and divides the order of the group.*

Proof. Let A be the set of Sylow p-subgroups of a finite group G. Then G acts on A by conjugation. Let $H \in A$. Then the orbit of H is precisely A, and the stabilizer of H is $\mathrm{N}_G(H)$. Hence

$$[G : \mathrm{N}_G(H)] = |A|,$$

so $|A|$ divides $|G|$.

Now consider H as acting on A by conjugation. Then

$$|A| \equiv |A_0| \pmod{p}.$$

The following are equivalent:

(1) $P \in A_0$;
(2) $H \leqslant \mathrm{N}_G(P)$;
(3) H is a Sylow subgroup of $\mathrm{N}_G(P)$.

But $P \trianglelefteq \mathrm{N}_G(P)$, so P is the unique Sylow p-subgroup of $\mathrm{N}_G(P)$. Therefore

$$|A| \equiv 1 \pmod{p},$$

since $A_0 = \{H\}$. □

15.9. **Lemma.** *Suppose p and q are distinct primes such that $q \not\equiv 1 \pmod{p}$, and $|G| = pq$. Then G has a unique Sylow p-subgroup, which is therefore normal.*

Proof. Let A be the set of Sylow p-subgroups of G. Then $|A| \equiv 1 \pmod{p}$, so $|A|$ is not q or pq; but $|A|$ divides pq; so $|A| = 1$. □

15.10. **Theorem.** *Suppose p and q are primes such that $q \not\equiv 1 \pmod{p}$ and $p < q$, and $|G| = pq$. Then G is cyclic.*

Proof. By the Lemma, G has normal subgroups of orders q and p; their intersection must be trivial, so their product is G. □

15.11. **Lemma.** $(\mathbb{Z}/\langle p\rangle)^\times \cong \mathbb{Z}/\langle p-1\rangle$.

Proof. $(\mathbb{Z}/\langle p\rangle)^\times$ is isomorphic to

$$\sum_{i<n} \mathbb{Z}/\langle m_i\rangle \oplus \mathbb{Z}/\langle k\rangle,$$

where m_i divides m_{i+1}, and $m_{n-1} \mid k$. Hence every element of $(\mathbb{Z}/\langle p\rangle)^\times$ is a solution of

$$X^k = 1.$$

But this polynomial can have at most k solutions in $\mathbb{Z}/\langle p\rangle$, since this is a *field*. Hence $p-1 \leqslant k$, so $p-1 = k$, and $n = 0$. □

Suppose N and H are groups, and $x \mapsto \sigma_x$ is an action of H on N. For all n and n' in N, and g and g' in H, we have

$$\begin{aligned}
\lambda_n \circ \sigma_g \circ \lambda_{n'} \circ \sigma_{g'} &= \lambda_n \circ \sigma_g \circ \lambda_{n'} \circ \sigma_{g^{-1}} \circ \sigma_g \circ \sigma_{g'} \\
&= \lambda_n \circ \lambda_{\sigma_g(n')} \circ \sigma_g \circ \sigma_{g'} \\
&= \lambda_{n\cdot\sigma_g(n')} \circ \sigma_{g\cdot g'}.
\end{aligned}$$

Hence there is a group-structure on $N \times H$ with multiplication given by

$$(n, g) \cdot (n', g') = (n \cdot \sigma_g(n'), g \cdot g').$$

(This is so, even if $x \mapsto \sigma_x$ is not injective.) The group itself is the **semi-direct product** of N and H with respect to σ, and it can be denoted by

$$N \rtimes_\sigma H.$$

The images of N and H in this group have trivial intersection, and the image of N is a normal subgroup.

A special case arises when N and H are already subgroups of some group G. If $H \trianglelefteqslant \mathrm{N}_G(N)$, then $N \trianglelefteqslant \langle N \cup H\rangle$, so the latter group has the universe NH. If also $N \cap H = \langle 1\rangle$, then NH has the structure of an **internal semi-direct product,** which can be denoted by

$$N \rtimes H;$$

it is isomorphic to $N \rtimes_\sigma H$, where

$$\sigma_g(n) = gng^{-1}.$$

15.12. **Example.** Every automorphism of $\mathbb{Z}/\langle n\rangle$ is $x \mapsto a \cdot x$ for some a that is prime to n. Let t be the order of this automorphism. Then there is an action $x \mapsto \sigma_x$ of $\mathbb{Z}/\langle t\rangle$ on $\mathbb{Z}/\langle n\rangle$, where σ_1 is $x \mapsto a \cdot x$. We can therefore construct

$$\mathbb{Z}/\langle n\rangle \rtimes_\sigma \mathbb{Z}/\langle t\rangle,$$

where the multiplication is given by

$$(x, y)(x', y') = (x + a^y \cdot x', y + y').$$

15.13. **Lemma.** *For every prime p, for every prime divisor q of $p-1$, there is a unique non-abelian semi-direct product $\mathbb{Z}/\langle p\rangle \rtimes \mathbb{Z}/\langle q\rangle$.*

Proof. As $(\mathbb{Z}/\langle p\rangle)^\times$ is cyclic, it has a unique subgroup G of order q. As q is prime, every non-trivial element of G is a generator. If $a \in G \smallsetminus \{1\}$, let $x \mapsto \sigma_x$ be the action of $\mathbb{Z}/\langle q\rangle$ on $\mathbb{Z}/\langle p\rangle$ that takes 1 to $x \mapsto a \cdot x$. Then we can form

$$\mathbb{Z}/\langle p\rangle \rtimes_\sigma \mathbb{Z}/\langle q\rangle.$$

If $\mathbb{Z}/\langle p\rangle \rtimes_\tau \mathbb{Z}/\langle q\rangle$ is some other non-abelian semi-direct product, then τ_1 is $x \mapsto b \cdot x$ for some b in $G \smallsetminus \{1\}$. But then $b^n = a$ for some n, so there is an isomorphism from $\mathbb{Z}/\langle p\rangle \rtimes_\sigma \mathbb{Z}/\langle q\rangle$ to $\mathbb{Z}/\langle p\rangle \rtimes_\tau \mathbb{Z}/\langle q\rangle$ that takes (x, y) to (x, ny). □

15.14. **Theorem.** *Suppose p and q are prime, with $p \equiv 1 \pmod{q}$, and $|G| = pq$. Then either G is cyclic, or G is the non-abelian semi-direct product $\mathbb{Z}/\langle p\rangle \rtimes \mathbb{Z}/\langle q\rangle$.*

Proof. Since $q \not\equiv 1 \mod p$, the group G has a unique Sylow p-subgroup N, which is a normal subgroup of order p. But G also has a subgroup H of order q. Then G is the internal semi-direct product $N \rtimes H$. □

16. Nilpotent groups

The **commutator** of two elements a and b of G is the element

$$aba^{-1}b^{-1},$$

denoted by $[a, b]$. Then

$$\mathrm{C}(G) = \{g \in G \colon \forall x\ [g, x] = 1\}.$$

We can generalize this definition, letting

$$\mathrm{C}_0(G) = \langle 1\rangle,$$
$$\mathrm{C}_{n+1}(G) = \{g \in G \colon \forall x\ [g, x] \in \mathrm{C}_n(G)\}.$$

Then $\mathrm{C}(G) = \mathrm{C}_1(G)$, and

$$\mathrm{C}_n(G) = \{g \in G \colon \forall x_1\ \dots \forall x_n\ [\dots[g, x_1], \dots x_n] = 1\}.$$

16.1. **Lemma.** $\mathrm{C}_n(G) \trianglelefteq G$ *and* $\mathrm{C}_n(G) \leqslant \mathrm{C}_{n+1}(G)$ *and*

$$\mathrm{C}_{n+1}(G)/\mathrm{C}_n(G) = \mathrm{C}(G/\mathrm{C}_n(G)).$$

Proof. We have $\mathrm{C}_0(G) \trianglelefteq G$. Suppose $\mathrm{C}_k(G) \trianglelefteq G$. Then the following are equivalent:

(1) $g \in \mathrm{C}_{k+1}(G)$;
(2) $\forall x\ [g, x] \in \mathrm{C}_k(G)$;
(3) $\forall x\ gxg^{-1}x^{-1} \in \mathrm{C}_k(G)$;
(4) $\forall x\ \mathrm{C}_k(G)gx = \mathrm{C}_k(G)xg$;
(5) $\mathrm{C}_k(G)g \in \mathrm{C}(G/\mathrm{C}_k(G))$.

Thus $\mathrm{C}_k(G) \leqslant \mathrm{C}_{k+1}(G)$, and $\mathrm{C}_{k+1}(G)/\mathrm{C}_k(G) = \mathrm{C}(G/\mathrm{C}_k(G))$; in particular,

$$\mathrm{C}_{k+1}(G)/\mathrm{C}_k(G) \trianglelefteq G/\mathrm{C}_k(G),$$

so $\mathrm{C}_{k+1}(G) \trianglelefteq G$. □

So we have the **ascending central series** of G:

$$\langle 1\rangle \trianglelefteq \mathrm{C}(G) \trianglelefteq \mathrm{C}_2(G) \trianglelefteq \mathrm{C}_3(G) \trianglelefteq \cdots.$$

A group is called **nilpotent** if this series reaches the group itself. So an abelian group is nilpotent, since its center is itself.

16.2. **Theorem.** *Finite p-groups are nilpotent.*

Proof. Suppose G is a p-group. If H is a proper normal subgroup of G, then G/H is a non-trivial p-group, so it has a non-trivial center. Therefore the ascending central series of G is strictly increasing, until it reaches G itself. □

16.3. **Theorem.** *A finite direct product of nilpotent groups is nilpotent.*

Proof. The definition shows

$$\mathrm{C}_n\Bigl(\prod_{i\in I} G_i\Bigr) = \prod_{i\in I} \mathrm{C}_n(G_i).$$

If I is finite, and each $\mathrm{C}_n(G_i)$ reaches G_i for some n, then so must $\mathrm{C}_n(G)$. □

16.4. **Lemma.** $\mathrm{C}_n(G) \leqslant H \leqslant \mathrm{C}_{n+1}(G) \implies \mathrm{C}_{n+1}(G) \leqslant \mathrm{N}_G(H)$.

Proof. Say $a \in \mathrm{C}_{n+1}(G)$. If $h \in H$, then $[a,h] \in \mathrm{C}_n(G)$, so $aha^{-1} \in \mathrm{C}_n(G)h \subseteq H$. Therefore $aHa^{-1} \subseteq H$, so $a \in \mathrm{N}_G(H)$. □

16.5. **Lemma.** *If G is nilpotent, and $H \leqslant G$, but $H \neq G$, then $H \neq \mathrm{N}_G(H)$.*

Proof. Let n be maximal such that $\mathrm{C}_n(G) \leqslant H$. Then $\mathrm{C}_{n+1}(G) \smallsetminus H$ is non-empty, but contains members of $\mathrm{N}_G(H)$. □

16.6. **Theorem.** *A finite group is nilpotent if and only if it is the direct product of its Sylow subgroups.*

Proof. Suppose G is a finite nilpotent group, and P is a Sylow p-subgroup. We shall show that $P \trianglelefteqslant G$. To do this, it is enough to show $\mathrm{N}_G(P) = G$. To do *this*, it is enough to show $\mathrm{N}_G(\mathrm{N}_G(P)) \leqslant \mathrm{N}_G(P)$. To do *this*, note that, as $P \trianglelefteqslant \mathrm{N}_G(P)$, so P is the unique Sylow p-subgroup of $\mathrm{N}_G(P)$. Hence, in particular, for any x in G, if $xPx^{-1} \leqslant \mathrm{N}_G(P)$, then $xPx^{-1} = P$, so $x \in \mathrm{N}_G(P)$. But every x in $\mathrm{N}_G(\mathrm{N}_G(P))$ satisfies the hypothesis.

Let I comprise the prime divisors of $|G|$. For each p in I, the group G has a unique Sylow p-subgroup, P_p. Then the homomorphism

$$(x_p \colon p \in I) \mapsto \prod_{p\in I} x_p$$

from $\prod_{p\in I} P_p$ to G is a well-defined isomorphism. □

17. Soluble groups

The **commutator subgroup** of a group G is the subgroup

$$\bigl\langle [x,y] \colon (x,y) \in G^2 \bigr\rangle,$$

which is denoted by G'.

17.1. **Theorem.** *G' is the smallest of the normal subgroups N of G such that G/N is abelian.*

Proof. If $f \in \mathrm{Aut}(G)$, then $f(G') \leqslant G'$. In particular, $xG'x^{-1} \leqslant G'$ for all x in G; so $G' \trianglelefteqslant G$. Suppose $N \trianglelefteqslant G$; then the following are equivalent:

(1) G/N is abelian;
(2) $N = [xN, yN] = [x,y]N$ for all $(x,y) \in G^2$;
(3) $G' \leqslant N$.

This completes the proof. □

We now define the **derived subgroups** $G^{(n)}$ of G by

$$
\begin{aligned}
G^{(0)} &= G,\\
G^{(n+1)} &= (G^{(n)})'.
\end{aligned}
$$

We have a descending sequence

$$G \trianglerighteq G' \trianglerighteq G^{(2)} \trianglerighteq \cdots.$$

The group G is called **soluble** if this sequence reaches $\langle 1\rangle$.

17.2. **Theorem.** *Nilpotent groups are soluble.*

Proof. Each $\mathrm{C}_{k+1}(G)/\mathrm{C}_k(G)$ is a center (of some group, namely $G/\mathrm{C}_k(G)$), so it is abelian, and therefore

$$\mathrm{C}_{k+1}(G)' \leqslant \mathrm{C}_k(G).$$

Suppose G is nilpotent, that is, $G^{(0)} \leqslant G \leqslant \mathrm{C}_n(G)$ for some n. If also

$$G^{(k)} \leqslant \mathrm{C}_{n-k}(G)$$

for some k in n, then

$$G^{(k+1)} = (G^{(k)})' \leqslant \mathrm{C}_{n-k}(G)' \leqslant \mathrm{C}_{n-(k+1)}(G).$$

By induction then, $G^{(n)} \leqslant \mathrm{C}_0(G) = \langle 1\rangle$. □

The proof can be seen as the construction of the following commutative diagram, in which the arrows are inclusions:

$$
\begin{tikzcd}
G \arrow[d] & G' \arrow[l] \arrow[d] & G^{(2)} \arrow[l] \arrow[d] & G^{(3)} \arrow[l] \arrow[d] & {} \arrow[l, dotted] \\
G \arrow[d] & \mathrm{C}_n(G)' \arrow[l] \arrow[d] & \mathrm{C}_{n-1}(G)' \arrow[l] \arrow[d] & \mathrm{C}_{n-2}(G)' \arrow[l] \arrow[d] & {} \arrow[l, dotted] \\
\mathrm{C}_n(G) & \mathrm{C}_{n-1}(G) \arrow[l] & \mathrm{C}_{n-2}(G) \arrow[l] & \mathrm{C}_{n-3}(G) \arrow[l] & {} \arrow[l, dotted]
\end{tikzcd}
$$

17.3. **Lemma.** *Solubility is preserved in subgroups and quotients. If $N \trianglelefteq G$, and N and G/N are soluble, then G is soluble.*

Proof. Suppose f is a homomorphism from G to H. Then $f(G^{(n)}) \leqslant H^{(n)}$, with equality is f is surjective. In particular then:

- If H is soluble, and f is an inclusion, then G is soluble.
- If G is soluble, and f is the quotient-map onto G/N, then this is soluble.

If $(G/N)^{(n)} = \langle 1\rangle$, then $G^{(n)} \leqslant N$; if also $N^{(m)} = \langle 1\rangle$, then $G^{(n+m)} = \langle 1\rangle$. □

17.4. **Theorem.** *Groups with non-abelian simple subgroups are not soluble. In particular,* $\mathrm{Sym}(5)$ *is not soluble if* $n \geqslant 5$.

18. Normal series

A **normal series** for a group G is a decreasing chain

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots .$$

(If one wants to distinguish, one may call this a *subnormal series*, normal if each G_i is normal in G.) The **factors** of the normal series are the quotients G_i/G_{i+1}. If $G_n = \langle 1 \rangle$ for some n, then the series is called

- a **composition series,** if the factors are simple;
- a **soluble series,** if the factors are abelian.

18.1. **Example.** If G is nilpotent, then the series

$$\langle 1 \rangle \trianglelefteq \mathrm{C}(G) \trianglelefteq \mathrm{C}_2(G) \trianglelefteq \cdots \trianglelefteq G$$

is a soluble series. If G is soluble, then the series

$$G \trianglerighteq G' \trianglerighteq G^{(2)} \trianglerighteq \cdots \trianglerighteq \langle 1 \rangle$$

is a soluble series.

18.2. **Theorem.** *Every finite group has a composition series.*

Proof. A finite group G has a maximal proper normal subgroup N (which need not be unique); then G/N is simple. □

(Every group has maximal proper normal subgroups, by Zorn's Lemma.)

18.3. **Theorem.** *Groups with soluble series are soluble.*

Proof. If the series

$$G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = \langle 1 \rangle$$

is soluble, then $G^{(i)} \leqslant G_i$ in each case. □

As a normal series, a composition series is maximal in that no distinct term can be inserted, that is, an inserted term introduces no new non-trivial factors.

In a soluble series for a finite group, terms can be added so that the non-trivial factors are cyclic of prime order.

Any normal series is **equivalent** with the series that results when all repeated terms are deleted (so that all trivial factors are removed). Then two normal series

$$G_i(0) \trianglerighteq G_i(1) \trianglerighteq G_i(2) \trianglerighteq \cdots \trianglerighteq G_i(n)$$

(where $i < 2$) with no trivial factors are **equivalent** if there is σ in $\mathrm{Sym}(n)$ such that

$$G_0(i)/G_0(i+1) \cong G_1(\sigma(i))/G_1(\sigma(i+1))$$

for each i in n.

18.4. **Lemma** (Zassenhaus or Butterfly)**.** *Suppose $N_i \trianglelefteq H_i \leqslant G$ for each i in 2. Let $H = H_0 \cap H_1$. Then:*

(1) *$N_i(H_i \cap N_{1-i}) \trianglelefteq N_i H$ for each i;*
(2) *the two groups $N_i H / N_i(H_i \cap N_{1-i})$ are isomorphic.*

$$\begin{tikzcd}
 & H_0 & & H_1 & \\
 & N_0H \arrow[u] & & N_1H \arrow[u] & \\
 & & H \arrow[ul] \arrow[ur] & & \\
 & N_0(H_0 \cap N_1) \arrow[uu] & & N_1(H_1 \cap N_0) \arrow[uu] & \\
N_0 \arrow[ur] & & K \arrow[ul] \arrow[ur] \arrow[uu] & & N_1 \arrow[ul] \\
 & H_1 \cap N_0 \arrow[ul] \arrow[ur] & & H_0 \cap N_1 \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Proof. We have $H_i \cap N_{1-i} \trianglelefteqslant H$. Let
$$K = (H_0 \cap N_1)(H_1 \cap N_0);$$
then $K \trianglelefteqslant H$. It is now enough to exhibit an epimorphism from N_iH onto H/K with kernel $N_i(H_i \cap N_{1-i})$. If $n, n' \in N_i$ and $h, h' \in H$ and $nh' = n'h$, then
$$h'h^{-1} = n^{-1}n' \in N_i \cap H \leqslant K,$$
so that $Nh = Nh'$. Hence there is a well-defined homomorphism f from N_iH into H/K that, when $(n, h) \in N_i \times H$, takes nh to Kh. That f is surjective is clear. Moreover, the following are equivalent:

(1) $nh \in \ker f$;
(2) $h \in K$;
(3) $h = n_0n_1 = n_1n_0$ for some n_i in $H_{1-i} \cap N_i$;

Also, (3) implies $nh \in N_i(H_i \cap N_{1-i})$. Conversely, suppose this last statement holds. Then also $h \in N_i(H_i \cap N_{1-i})$, so $h = n'h'$ for some n' in N_i and h' in $H_i \cap N_{1-i}$. Then $n' = h(h')^{-1} \in H_{1-i}$, so $n' \in H_{1-i} \cap N_i$, and therefore $h \in K$. □

18.5. **Theorem** (Schreier)**.** *Any two normal series have equivalent refinements.*

Proof. Suppose that
$$G = G_i(0) \trianglerighteqslant G_i(1) \trianglerighteqslant \cdots \trianglerighteqslant G_i(n_i) = \langle 1 \rangle,$$
where $i < 2$, are normal series for G. In particular,
$$G_i(j+1) \trianglelefteqslant G_i(j) \leqslant G.$$
Define
$$G_i(j,k) = G_i(j+1)(G_i(j) \cap G_{1-i}(k)),$$
where $(j,k) \in n_i \times n_{1-i}$. Then
$$G_i(j) = G_i(j,0) \trianglerighteqslant G_i(j,1) \trianglerighteqslant \cdots \trianglerighteqslant G_i(j, n_{1-i}-1) \trianglerighteqslant G_i(j, n_{1-i}) = G_i(j+1),$$
giving us normal series that are refinements of the original ones; but also
$$G_0(j,k)/G_0(j,k+1) \cong G_1(k,j)/G_1(k,j+1),$$

completing the proof. □

18.6. **Theorem** (Jordan–Hölder). *Any two composition series of a group are equivalent.*

Part 3. Rings

19. Rings

A **ring** is a structure $(\mathfrak{R}, \cdot)$ such that:

- $\mathfrak{R}$ is an abelian group;
- $(R, \cdot)$ is a semi-group;
- $\forall x\ \forall y\ \forall z\ (x \cdot (y + z) = xy + xz\ \&\ (x + y) \cdot z = xz + yz)$.

That is, a ring is an abelian group with a **multiplication,** that is, an associative operation that distributes over addition. An **identity** in the ring is a multiplicative identity: an element 1 such that $(R, \cdot, 1)$ is a monoid. A ring is **commutative** if the multiplication is commutative.

19.1. **Example.** $\mathbb{Z}/\langle n\rangle$ is a commutative ring (with identity) for all n in $\mathbb{Z}$.

19.2. **Example.** The set $M_n(\mathbb{Z})$ of $n \times n$ matrices with entries from $\mathbb{Z}$ is a ring with identity, non-commutative if $n > 1$.

19.3. **Example.** The set of continuous functions on $\mathbb{R}$ with compact support is a commutative ring without identity.

A **ring-homomorphism** has the obvious definition: a group-homomorphism preserving multiplication. A homomorphism of rings-with-identity preserves the identity.

For an abelian G, let $\mathrm{End}(G)$ be the set of **endomorphisms** of G, that is, homomorphisms from G to itself.

19.4. **Lemma.** *If G is an abelian group, then $\mathrm{End}(G)$ is an abelian group with addition given by*

$$(f + g)(x) = f(x) + g(x),$$

and $(\mathrm{End}(G), \circ, \mathsf{id}_G)$ is a ring with identity. The map taking an integer n to the map $x \mapsto nx$ from G to itself is a homomorphism from the ring-with-identity $\mathbb{Z}$ to $(\mathrm{End}(G), \circ, \mathsf{id}_G)$.

The symbols 0 and 1 can stand for integers or ring-elements, but there is no ambiguity. For ring-elements x we have $1 \cdot x = x = 1x$ by definition. Also:

19.5. **Lemma.** *If x is a ring-element, then $0 \cdot x = 0$. If y is also a ring-element, and $n \in \mathbb{Z}$, then $nx \cdot y = n(x \cdot y) = x \cdot ny$.*

If a is a ring-element, then we can let λ_a be the map $x \mapsto a \cdot x$ from the ring to itself.

19.6. **Lemma.** *Let $(\mathfrak{R}, \cdot)$ be a ring. Then the map $x \mapsto \lambda_x$ is a homomorphism from $(\mathfrak{R}, \cdot)$ into $(\mathrm{End}(\mathfrak{R}), \circ)$; it preserves the identity, if the ring has one.*

The **characteristic** of a ring R is the non-negative integer n such that $\mathbb{Z}/\langle n\rangle$ is the kernel of the homomorphism from $\mathbb{Z}$ to $\mathrm{End}(R)$. This kernel is the kernel of $n \mapsto n1$, if R has an identity.

19.7. **Example.** If $0 \leqslant n$, then $\mathbb{Z}/\langle n\rangle$ has characteristic n.

19.8. **Theorem.** *Any ring embeds in a ring with identity; the latter ring can have the characteristic of the former, or characteristic 0.*

Proof. Suppose R is a ring of characteristic n. Let A be $\mathbb{Z}$ or $\mathbb{Z}/\langle n\rangle$, and give $A \oplus R$ the multiplication defined by

$$(m, x)(n, y) = (mn, my + nx + xy);$$

then $(1, 0)$ is an identity, and $x \mapsto (0, x)$ is an embedding. $\square$

Henceforth let us understand 'ring' to mean 'ring with identity'.

Let R be a commutative ring (with identity). A **unit** of R is an element a such that $ax = 1$ for some x in R. The set of units of R is denoted by

$$R^{\times};$$

this is a group under multiplication. A **zero-divisor** of R is a element b distinct from 0 such that $bx = 0$ for some x in R. So zero-divisors are not units. (The unique element of the trivial ring is a unit, but not a zero-divisor.) The ring R is a **field** if $R \smallsetminus \{0\} \subseteq R^{\times}$. So fields have no zero-divisors. The ring R is merely an **integral domain** if it has no zero-divisors.

19.9. **Example.** $\mathbb{Z}$ is an integral domain, but not a field; $\mathbb{Q}$ is a field.

19.10. **Example.** If $m > 1$ and $n > 1$, then $m + \langle mn\rangle$ and $n + \langle mn\rangle$ are zero-divisors in $\mathbb{Z}/\langle mn\rangle$. If p is prime, then $\mathbb{Z}/\langle p\rangle$ is a field, denoted by $\mathbb{F}_p$. Also, $\mathbb{Z}/\langle 1\rangle$ is the trivial ring, which by our definition is a field, $\mathbb{F}_1$ (although some writers would require $0 \neq 1$ in an integral domain).

One can discuss these notions in non-commutative rings:

19.11. **Example.** The real vector-space with basis $\{1, i\}$ becomes the complex field $\mathbb{C}$ when we define $i^2 + 1 = 0$. The field-structure has the non-trivial automorphism $z \mapsto \overline{z}$, where $\overline{a + bi} = a - bi$. The complex vector-space with basis $\{1, j\}$ becomes a non-commutative ring, the ring $\mathbb{H}$ of **quaternions,** when $j^2 + 1 = 0$ and $j \cdot z = \overline{z}j$ if $z \in \mathbb{C}$. We have

$$(z + wj)(\overline{z} - wj) = z\overline{z} + w\overline{w} \in \mathbb{R},$$

so all non-zero elements of $\mathbb{H}$ can be called units, and $\mathbb{H}$ is a **division-ring.**

20. Ideals

If A is a sub-ring of R, then we can form the abelian group R/A. We could try to define a multiplication on this by

$$(x + A)(y + A) = xy + A.$$

However, if $x - x' \in A$, and $y - y' \in A$, we need not have $xy - x'y' \in A$.

A **left ideal** of R is a sub-ring I such that

$$RI \subseteq I,$$

that is, $rx \in I$ whenever $r \in R$ and $x \in I$. Likewise, **right** and **two-sided** ideal.

20.1. **Theorem.** *If I is a two-sided ideal of R, then R/I is a well-defined ring. The kernel of a ring-homomorphism is a two-sided ideal.*

20.2. **Example.** The set of matrices

$$\begin{bmatrix} * & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ * & 0 & \dots & 0 \end{bmatrix}$$

is a left ideal of $M_n(\mathbb{Z})$, but not a right ideal unless $n = 1$.

20.3. **Example.** Rx is a left ideal; RxR is a two-sided ideal.

Suppose $(A_i : i \in I)$ is a tuple of left ideals of a ring R. Let the abelian sub-group of R generated by $\bigcup_{i\in I} A_i$ be denoted by

$$\sum_{i\in I} A_i;$$

this is the **sum** of the ideals A_i. Suppose in particular $I = n$. Let the abelian sub-group of R generated by

$$\{a_0 \cdots a_{n-1} : a_i \in A_i\}$$

be denoted by

$$A_0 \cdots A_{n-1};$$

this is the **product** of the ideals A_i.

20.4. **Lemma.** *Sums and finite products of left ideals are left ideals; sums and products of two-sided ideals are two-sided ideals. Addition and multiplication of ideals are associative; addition is commutative; multiplication distributes over addition.*

20.5. **Lemma.** *If A and B are left ideals of a ring, then so is $A \cap B$, and $AB \subseteq A \cap B$.*

20.6. **Lemma.** *If $f : R \to S$, a homomorphism of rings, and I is a two-sided ideal of R included in $\ker f$, then there is a unique homomorphism $\tilde{f}$ from R/I to S such that $f = \tilde{f} \circ \pi$.*

Hence the isomorphism theorems, as for groups.

21. Commutative rings

Henceforth, let all rings be commutative, so all ideals are two-sided. Also, let all rings have identities. An subset A of a ring R determines an ideal

$$(A),$$

namely the smallest ideal including A.

21.1. **Lemma.** *(A) is the set of finite R-linear combinations $\sum_{a\in A} r_a a$, where $r_a \in R$ (and $r_a = 0$ for all but finitely many a).*

If $A = \{a\}$, then (A) is the **principal ideal** (a). A **principal ideal domain** or PID is an integral domain whose every ideal is principal.

21.2. **Example.** $\mathbb{Z}$ is a PID.

21.3. **Example.** In the polynomial ring $\mathbb{R}[X, Y]$, the ideal (X, Y) is not principal.

An ideal is proper if and only if it does not contain a unit. A *proper* ideal I is **prime** if

$$ab \in I \implies a \in I \vee b \in I.$$

So a ring is an integral domain if and only if (0) is a prime ideal.

21.4. **Theorem.** *A proper ideal I of a ring R is prime if and only if R/I is an integral domain.*

Proof. That I is prime means

$$ab \in I \implies a \in I \vee b \in I.$$

That R/I is integral means

$$(a+I)(b+I) = I \implies a + I = I \vee b + I = I.$$

These characterizations are equivalent. □

An ideal is called **maximal** if it is maximal as a proper ideal. A ring is a field if and only if (0) is a maximal ideal.

21.5. **Theorem.** *A proper ideal I of a ring R is maximal if and only if R/I is a field.*

Proof. That R/I is a field means that, if $a \in R \smallsetminus I$, then

$$ab \in 1 + I$$

for some b. That I is maximal means that, if $a \in R \smallsetminus I$, then

$$I + (a) = R,$$

equivalently,

$$1 \in I + (a),$$

that is, $ba \in 1 + I$ for some b. □

21.6. **Corollary.** *Maximal ideals are prime.*

The converse?

21.7. **Example.** The prime ideals of $\mathbb{Z}$ are the ideals (0) and (p), where p is prime; the latter are maximal.

A ring is **Boolean** if it satisfies

$$\forall x\ x \cdot x = x.$$

21.8. **Example.** A power-set is a Boolean ring if multiplication is intersection and addition is symmetric difference.

21.9. **Theorem.** *In Boolean rings, all prime ideals are maximal.*

Proof. In a Boolean ring, we have

$$x + x = (x+x)^2 = x^2 + 2x + x^2 = x + 2x + x,$$

so $2x = 0$. Hence

$$x(1+x) = x + x = 0.$$

Therefore there are no Boolean integral domains besides $\mathbb{F}_2$, which is a field. □

In $\mathbb{Z}$, the ideal (a, b) is the principal ideal generated by $\gcd(a, b)$. So a and b are co-prime if $(a, b) = \mathbb{Z}$.

21.10. **Theorem** (Chinese remainder)**.** *Suppose R has ideals I_i $(i < n)$ such that $I_i + I_j = R$ in each case. Then*

$$R/\bigcap_{i<n} I_i = \sum_{i<n} R/I_i.$$

Proof. We have to show that the map

$$x \mapsto (x + I_i : i < n)$$

from R to $\sum_{i<n} R/I_i$ is surjective. Say $x_i \in I_i$. If $n = 2$, then $a_0 + a_1 = 1$ for some a_i in I_i. But then

$$a_0 x_1 + a_1 x_0 + I_i = a_0(x_1 - x_0)a_{1-i}x_i + I = x_i + I$$

since $a_{1-i} = 1 - a_i$. □

22. Factorization

(Recall that all rings are now commutative with identity.) In a ring R, an element a is a **divisor** of b, or a **divides** b,

$$a \mid b,$$

if $ax = b$ for some x in R. Two elements that divide each other are **associates.**

22.1. **Lemma.** *In any ring:*

- $a \mid b \iff (b) \subseteq (a)$*;*
- a *and* b *are associates if and only if* $(a) = (b)$*.*

Suppose $a = bx$*.*

- *If* x *is a unit, then* a *and* b *are associates.*
- *If* b *is a zero-divisor or* 0*, then so is* a*.*
- *If* a *is a unit, then so is* b*.*

22.2. **Example.** In $\mathbb{Z}/6\mathbb{Z}$, the elements 1 and 5 are units; the other non-zero elements are zero-divisors. Of these, 2 and 4 are associates, since $2 \cdot 2 = 4$ and $4 \cdot 2 \equiv 2 \pmod 6$; but 3 is not an associate of these.

A ring-element is **irreducible** if it is not a unit, and its only factors are associates and units. So the element is irreducible just in case the ideal it generates is maximal amongst the proper principal ideals.

22.3. **Example.** In $\mathbb{R}[X, Y]$, the element X is irreducible, although (X) is not a maximal ideal.

A (non-zero) ring-element is **prime** if the ideal it generates is prime. So p is prime just in case

$$p \mid ab \implies p \mid a \vee p \mid b.$$

22.4. **Example.** The primes of $\mathbb{Z}$ are the integers $\pm p$, where p is a prime natural number. The primes of $\mathbb{Z}$ are just the irreducibles of $\mathbb{Z}$.

22.5. **Example.** In $\mathbb{Z}/6\mathbb{Z}$, the element 2 is prime but not irreducible.

22.6. **Example.** Let $\mathbb{Z}[\sqrt{-5}]$ be the smallest sub-ring of $\mathbb{C}$ containing the integers and $\sqrt{-5}$; so it consists of sums

$$a + b\sqrt{-5},$$

where a and b are integers. We have

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

The elements 2, 3 and $1 \pm \sqrt{-5}$ are irreducible. For example, suppose $2 = \alpha\beta$, where $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$. Then $4 = |\alpha|^2 |\beta|^2$. We are now in $\mathbb{Z}$, so $(|\alpha|^2, |\beta|^2) \in \{(1, 4), (2, 2), (4, 1)\}$, which is impossible if a, b, c and d are integers. Evidently, for example, 2 does not divide $1 \pm \sqrt{-5}$; so 2 is not prime.

22.7. **Theorem.** *In an integral domain, if a and b are non-zero associates, and $a = bx$, then x is a unit.*

Proof. We have also $b = ay = bxy$, $b(1 - xy) = 0$, $1 = xy$ since $b \neq 0$ and we are in an integral domain. □

22.8. **Corollary.** *In an integral domain, prime elements are irreducible.*

Proof. If p is prime, and $p = ab$, then p is an associate of a or b, so the other is a unit. □

A **unique factorization domain** is an integral domain whose every element is 'uniquely' a product of irreducibles. In such a domain, by the uniqueness, irreducibles are prime. Moreover, two elements have a **greatest common divisor;** for any two elements can be written

$$u \prod_{i<n} \pi_i^{a(i)} \quad \text{and} \quad v \prod_{i<n} \pi_i^{b(i)},$$

where u and v are units and the π_i are irreducibles; the g.c.d. is then

$$\prod_{i<n} \pi_i^{\min(a(i),b(i))},$$

which is determined up to a unit factor.

22.9. **Lemma.** *In a* UFD*, an element d is a g.c.d. of a and b if and only if d divides both a and b, and every divisor of a and b divides d.*

Proof. Elements d meeting the latter condition are associates. □

The condition in the lemma *defines* a g.c.d., when it exists.

22.10. **Lemma.** *G.c.d.s exist in* PID*s; in fact the equation*

$$aX + bY = \gcd(a, b)$$

can be solved.

Proof. The ideal generated by the $ax + by$ must be $(\gcd(a, b))$. □

22.11. **Theorem.** *In a* PID*, irreducibles are prime.*

Proof. Suppose the irreducible π divides ab but not a. Then the *g.c.d.* of π and a is 1; hence $\pi x + ay = 1$ for some x and y. Then $b = \pi xb + aby$, and π divides each summand, so $\pi \mid b$. □

22.12. **Corollary.** *In a* PID*, prime factorizations are unique.*

A ring is **Noetherian** if every ascending chain of ideals eventually stops.

22.13. **Theorem.** PID*s are Noetherian.*

Proof. If $I_0 \subseteq I_1 \subseteq \cdots$, then $\bigcup_{i\in\omega} I_i$ is an ideal (a); if $a \in I_n$, then the chain stops at I_n. □

22.14. **Lemma.** *In a* PID*, every element is a product of irreducibles.*

Proof. A tree of factorizations has no infinite branches. □

22.15. **Theorem.** PID*s are* UFD*s.*

A **Euclidean domain** is an integral domain equipped with a map ϕ into $\{-1\} \cup \omega$ such that $\phi^{-1}(-\infty) = \{0\}$ and, for all x and y, if $y \neq 0$, then:

- $\phi(x) \leqslant \phi(xy)$;
- there exist q and r such that $x = qy + r$ and $\phi(r) < \phi(y)$.

22.16. **Example.** On $\mathbb{Z}$, let $\phi(x) = |x| - 1$.

22.17. **Example.** On a field, let $\phi(x) = 0$ if $x \neq 0$.

22.18. **Example.** On a polynomial-ring $K[X]$ over a field K, let $\phi = \deg$.

22.19. **Example.** The **Gaussian integers** compose the domain $\mathbb{Z}[i]$ comprising the complex numbers $a + bi$ such that $a, b \in \mathbb{Z}$. This domain is Euclidean when we define $\phi(a + bi) = a^2 + b^2 - 1$.

22.20. **Theorem.** *Euclidean domains are* PID*s.*

Proof. An ideal of a Euclidean domain is generated by any non-zero element x such that $\phi(x)$ is minimal. □

23. Localization

A subset of a ring is **multiplicative** if it is closed under multiplication.

23.1. **Example.** The complement of a prime ideal is multiplicative.

23.2. **Theorem.** *If S is a multiplicative subset of a ring R, then on $R \times S$ there is an equivalence-relation $\sim$ given by*

$$(a, b) \sim (c, d) \iff (ad - bc) \cdot e = 0 \text{ for some } e \text{ in } S.$$

The equivalence-class of (a, b) being denoted by

$$\frac{a}{b},$$

the quotient $R \times S/{\sim}$ is a ring in which the operations are given by

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}, \qquad \frac{a}{b} \pm \frac{c}{d} = \frac{a \cdot d \pm b \cdot c}{b \cdot d}.$$

The ring $R \times S/{\sim}$ of the theorem is denoted by

$$S^{-1}R.$$

In the most important case, S is the complement of a prime ideal $\mathfrak{p}$, in which case $S^{-1}R$ is denoted by

$$R_{\mathfrak{p}}$$

and called the **localization** of R at $\mathfrak{p}$. In particular, if R is an integral domain, so that (0) is prime, then the localization of R at (0) is the **quotient-field** of R.

23.3. **Theorem.** *If R is a ring with multiplicative subset S, and $a \in S$, then the map*

$$x \mapsto \frac{ax}{a}$$

from R to $S^{-1}R$ is a ring-homomorphism. Suppose R is an integral domain and $0 \notin S$. Then the homomorphism is an embedding. Every embedding of R in a field factors through its embedding in its quotient-field.

A **local ring** is a ring with a unique maximal ideal.

23.4. **Lemma.** *An ideal $\mathfrak{m}$ of a ring R is a unique maximal ideal of R if and only if $R^{\times} = R \smallsetminus \mathfrak{m}$.*

23.5. **Theorem.** *The localization of a ring at a prime ideal is a local ring.*

Proof. The ideal generated by the image of $\mathfrak{p}$ in $R_{\mathfrak{p}}$ consists of those a/b such that $a \in \mathfrak{p}$. In this case, if $c/d = a/b$, then $cb = da \in \mathfrak{p}$, so $c \in \mathfrak{p}$ since $\mathfrak{p}$ is prime. Hence the following are equivalent:

(1) $x/y \notin R_{\mathfrak{p}}\mathfrak{p}$;
(2) $x \notin \mathfrak{p}$;
(3) x/y has an inverse, namely y/x.

By the previous lemma, we are done. □

24. Factorization of polynomials

Let $\mathcal{L}$ be the signature of rings, that is, $\{+, -, \cdot, 0, 1\}$, and let x_i be a variable if $i \in \omega$. Let R be a ring. The *terms* of $\mathcal{L}(R)$ compose the smallest set such that:

- 0, 1 and other elements of R are terms;
- variables are terms;
- if t and u are terms, then so are $-t$ and $(t + u)$ and $(t \cdot u)$.

If the variables used in a term t are in the set $\{x_i \colon i < n\}$, and if $\boldsymbol{a} \in A^n$ for some ring A that includes R, then there is a term $t(\boldsymbol{a})$ got by replacing each x_i with a_i. Define terms t and u to be equivalent, $t \sim u$, if $t(\boldsymbol{a}) = u(\boldsymbol{a})$ for all $\boldsymbol{a}$ from all rings extending R. A **polynomial** over R is an equivalence-class of terms of $\mathcal{L}(R)$. The polynomials containing only variables from $\{x_i \colon i < n\}$ compose the ring

$$R[x_0, \dots, x_{n-1}].$$

24.1. **Theorem.** *$R[x_0, \dots, x_{n-1}]$ is the unique ring-extension A of R such that, for all rings S, and all homomorphisms ϕ from R to S, and all $\boldsymbol{a}$ in S^n, there is a unique homomorphism $\tilde{\phi}$ from A to S such that $\tilde{\phi}|_R = \phi$ and $\tilde{\phi}(x^i) = a^i$ in each case.*

An arbitrary element of $R[x]$ can be written

$$\sum_{i \leqslant n} a_i x^i;$$

the **degree** of this is n, if $a_n \neq 0$; then a_n is the **leading coefficient** of the polynomial.

We have claimed that $K[x]$ is a Euclidean domain when equipped with deg. More generally:

24.2. **Lemma.** *If f and g are polynomials over R, then:*

- $\deg(f + g) \leqslant \max(\deg f, \deg g)$;
- $\deg(f \cdot g) \leqslant \deg f + \deg g$, *with equality if the product of the leading coefficients is not* 0.

In particular, if R is an integral domain, then so is $R[x]$.

Proof. The leading coefficient of a product is the product of the leading coefficients. □

24.3. **Lemma** (Division Algorithm)**.** *If f and g are polynomials in x over R, and the leading coefficient of g is 1, then*

$$f = qg + r$$

for some unique q and r in $R[x]$ such that $\deg r < \deg g$.

Proof. If $\deg g \leqslant \deg f$, and a is the leading coefficient of f, then
$$f = ax^{\deg f - \deg g} \cdot g + (f - ax^{\deg f - \deg g} \cdot g),$$
the second term having degree less than f. Continue as necessary. □

24.4. **Theorem** (Remainder)**.** *If $c \in R$, then any f in $R[x]$ can be written uniquely as $q(x) \cdot (x - c) + f(c)$.*

Proof. $f = q(x) \cdot (x - c) = d$ for some d in R; letting x be c yields the claim. □

24.5. **Corollary.** *A ring-element c is a zero of a polynomial f if and only if $(x - c) \mid f$. If f is over an integral domain, then the number of its distinct zeros is at most* $\deg f$.

24.6. **Theorem.** *If K is a field, then $K[x]$ is a Euclidean domain whose units are precisely the elements of K.*

A **derivation** of a ring R is an endomorphism δ of the underlying abelian group satisfying the Leibniz rule
$$\delta(a \cdot b) = \delta a \cdot b + \delta b \cdot a.$$
The pair (R, δ) is then a **differential ring.**

24.7. **Lemma.** *If δ is a derivation, then $\delta(x^n) = nx^{n-1}\delta x$ for all ring-elements x and n in ω.*

24.8. **Theorem.** *On a polynomial ring $R[x]$ over an integral domain, there is a unique derivation $f \mapsto f'$ such that $x' = 1$, and $c' = 0$ for all c in R.*

Proof. If δ is a derivation, then $\delta(x \cdot (y + z)) = \delta(xy + xz)$. So a derivation on $R[x]$ exists and is determined by its values on R and at x. □

24.9. **Lemma.** *Say R is an integral domain, $f \in R[x]$ and $f(c) = 0$. Then c is a multiple zero of f if and only if $f'(c) = 0$.*

Proof. Write f as $(x - c)^m \cdot g$, where $g(c) \neq 0$. Then $m \geqslant 1$, so
$$f' = m(x - c)^{m-1} \cdot g + (x - c)^m \cdot g'.$$
If $m > 1$, then $f'(c) = 0$. If $f'(c) = 0$, then $m \cdot 0^{m-1} \cdot g(c) = 0$, so $m > 1$. □

24.10. **Theorem.** *Say K is a field and $f \in K[x]$. If $\gcd(f, f') = 1$, then f has no multiple zeros.*

Proof. $1 = g \cdot f + h \cdot f'$ for some polynomials g and h, then f and f' can have no common zero. □

24.11. **Corollary.** *Suppose K is a field and $f \in K[x]$ is irreducible. Then $f' = 0$ if and only if every root of f is multiple.*

Proof. Since f is irreducible, we have $\gcd(f, f') \neq 1$ if and only if $f' = 0$. □

Appendix A. Group-actions

The following is partially inspired by a recent expository article [5] by Serre.

If $(X_i\colon i \in I)$ is a family of sets, and $R \subseteq \prod_{i\in I} X_i$, then for any pair (i,j) from I, we have
$$x \mapsto \pi_j(R \cap \pi_i^{-1}(x))\colon X_i \to \mathcal{P}(X_j),$$
which induces a map from $\mathcal{P}(X_i)$ to $\mathcal{P}(X_j)$. We are interested in the case when $I = 2$. In particular, suppose
$$(g,x) \mapsto gx$$
is an action of the group G on the set X, and let
$$\Omega = \{(g,x) \in G \times X\colon gx = x\}.$$
As above, this induces
$$x \mapsto G_x\colon X \to \mathcal{P}(G),$$
$$g \mapsto X^g\colon G \to \mathcal{P}(X).$$
In fact, $G_x \leqslant G$. As a special case, we have the action
$$(g,h) \mapsto h^g$$
of G on itself, where
$$h^g = ghg^{-1}.$$
Then
$$h \in G_{gx} \iff (h,gx) \in \Omega \iff hgx = gx \iff g^{-1}hgx = x \iff (h^{g^{-1}},x) \in \Omega \iff h^{g^{-1}} \in G_x,$$
and consequently
$$G_{gx} = (G_x)^g,$$
that is, we have a commutative diagram
$$\begin{array}{ccc} G \times X & \longrightarrow & G \times S \\ \Big\downarrow & & \Big\downarrow \\ X & \longrightarrow & S \end{array},$$
where S is the set of subgroups of G. Likewise, since
$$x \in X^{h^g} \iff (h^g,x) \in \Omega \iff (h,g^{-1}x) \in \Omega \iff g^{-1}x \in X^h,$$
we have
$$X^{h^g} = gX^h,$$
whence the commutative diagram
$$\begin{array}{ccc} G \times G & \longrightarrow & G \times \mathcal{P}(X) \\ \Big\downarrow & & \Big\downarrow \\ G & \longrightarrow & \mathcal{P}(X) \end{array}.$$
Define
$$Gx = \{gx\colon g \in G\},$$
the **orbit** of x under the action of G. Then $gx = hx \iff gG_x = hG_x$, whence
$$|Gx| = [G : G_x].$$

The sets Gx partition G. We may define

$$X/G = \{Gx \colon x \in X\}.$$

For any function ϕ from G to $\mathbb{R}$ and subset A of G, we define

$$\int_S \phi = \sum_{g \in S} \frac{\phi(g)}{|G|}, \quad \int \phi = \int_G \phi.$$

Assume now that G and X are finite. Let χ be the function

$$g \mapsto |X^g|$$

from G to ω.

A.1. **Lemma** (Burnside). *$|X/G| = \int \chi$.*

Proof. Compute:

$$\sum_{g \in G} \chi(g) = |\Omega| = \sum_{x \in X} |G_x| = \sum_{C \in X/G} \sum_{x \in C} |G_x|.$$

But if $x \in C \in X/G$, then $C = [G : G_x]$. Hence the last quantity is

$$\sum_{c \in X/G} \sum_{x \in C} \frac{|G|}{|C|},$$

which is $|X/G| \cdot |G|$. □

Define

$$G_0 = \{g \in G \colon X^g = \varnothing\}.$$

A.2. **Theorem** (Jordan). *If $|X/G| = 1$ and $|X| \geqslant 2$, then*

$$G_0 \neq \varnothing.$$

Proof. By the Burnside Lemma, the average size of X^g is 1. Since $X^1 = X$, and $|X| \geqslant 2$, we must have $|X|^g < 1$ for some g in G. □

A stronger result is the following:

A.3. **Theorem** (Cameron–Cohen). *If $|X/G| = 1$ and $|X| \geqslant 2$, then*

$$|G_0| \cdot |X| \geqslant |G|.$$

Proof. The action of G on X induces an action on $X \times X$, and $|(X \times X)^g| = \chi(g)^2$. Now, $(X \times X)/G$ contains the diagonal $G(1,1)$ and at least one other element, so

$$\int \chi^2 \geqslant 2$$

by Burnside's Lemma. Let $n = |X|$, so that

$$1 \leqslant \chi(g) \leqslant n$$

for all g in $G \smallsetminus G_0$. Then

$$\frac{|G_0| \cdot |X|}{|G|} = n \int_{G_0} 1 = \int_{G_0} (\chi - 1)(\chi - n) \geqslant \int_G (\chi - 1)(\chi - n) = \int_G (\chi^2 - 1),$$

which is at least 1. □

Serre's article gives applications to topology and number-theory.

References

[1] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[2] Morris Kline. *Mathematical thought from ancient to modern times*. Oxford University Press, New York, 1972.

[3] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[4] James H. McKay. Another proof of Cauchy's group theorem. *Amer. Math. Monthly*, 66:119, 1959.

[5] Jean-Pierre Serre. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)*, 40(4):429–440 (electronic), 2003.

[6] Lawrence Washington. A graduate course in algebra. Transcription by David Pierce, 1990.

Index