1. Introduction to Groups

Theorem 1.1. Let $(G, \cdot)$ be a group, $H \subseteq G$. Then $(H, \cdot)$ is a subgroup of G if

1. $H \neq \varnothing$.
2. For all $a, b \in H$, $ab^{-1} \in H$.

Definition 1.2. Let $g \in G$ a group, then g^{-1} is the *unique* element of G such that $gg^{-1} = g^{-1}g = id$

Definition 1.3. A ***group action*** of a group G on a set A is a map, $G \times A$ to A satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G$ and $a \in A$.
2. $id_G \cdot a = a$ for all $a \in A$.

2. Subgroups

Definition 2.1. Let $A \subseteq G$, $A \neq \varnothing$. Define $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the ***centralizer*** of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A. When $A = G$ this set is denoted by $Z(G)$ and is called the ***center*** of G.

Note: $Z(G) \leq C_G(A)$ for all $A \subseteq G$.

Definition 2.2. Let $A \subseteq G$, $A \neq \varnothing$. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. We define the ***normalizer*** of A in G to be the set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

Definition 2.3. Let G be a group acting on a set S. The ***stabilizer*** G_s for some fixed $s \in S$ is the set

$$G_s = \{g \in G \mid g \cdot s = s\}.$$

Proposition 2.4. Let A be some set and G be a group. Then $C_G(A) \leq N_G(A)$.

Proof. $C_G(A)$ is the kernel of $N_G(A)$ acting on A under the conjugation map $a \mapsto gag^{-1}$. ♣

Proposition 2.5. Let G be a group and $S \subseteq G$, $s \neq \varnothing$. Then $N_G(S) \leq G$.

Proof. Let G be a group and $S \subseteq G$. We know that $N_G(S) = \{g \in G \mid gSg^{-1} = S\}$. If we take $a, b \in N_G(S)$ we have that

$$abSb^{-1}a^{-1} = aSa^{-1} = S$$

so $ab \in N_G(S)$. Similarly we have that for $a \in N_G(S)$

$$a^{-1}Sa = a^{-1}(aSa^{-1})a = S$$

so $a^{-1} \in N_G(S)$ and we have that $N_G(S) \leq G$. ♣

Theorem 2.6. There is only one cyclic group of each order.

Proposition 2.7. Let G be a group, let $x \in G$ and let $a \in \mathbb{Z}^\times$.

1. If $|x| = \infty$, then $|x^a| = \infty$.

2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{\gcd(n,a)}$.

Definition 2.8. Let $A \subseteq G$ and define

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H.$$

This is called the ***subgroup of G generated by A*** and is simply the intersection of all the subgroups containing the set A.

Zorn's Lemma. If A is a nonempty partially ordered set in which every chain has an upper bound then A has a maximal element.

3. Quotient Groups and Homomorphisms

Proposition 3.1. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.

1. $\varphi(id_G) = id_H$
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$
3. $\varphi(g^n) = \varphi(g)^n$
4. $\ker(\varphi)$ is a subgroup of G
5. $\text{im}(\varphi)$ is a subgroup of H

Proposition 3.2. Let G be a group and let N be a subgroup of G

1. The operation on the set of left cosets of N in G described by

$$uN \cdot vN = (uv)N$$

   is sell defined if and only if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.

2. If the above operation is well defined then it makes the set of left cosets of N in G into a group. In particular the identity of this group is the coset $id_G N$and the inverse of gN is $g^{-1}N$.

Definition 3.3. The element gng^{-1} is called the conjugate of $n \in N$ by g. The set gNg^{-1} is also called the conjugate of N by g. The element g is said to ***normalize*** N if $gNg^{-1} = N$. A subgroup N of G is a ***normal subgroup*** if every $g \in G$ normalizes N. We will write this as $N \trianglelefteq G$.

Theorem 3.4. Let N be a subgroup of G. The following are equivalent.

1. $N \trianglelefteq G$
2. $N_G(N) = G$
3. $gN = Ng \quad \forall g \in G$
4. The operation on left cosets of N in G described by Proposition 3.2 makes the set of left cosets into a group
5. $gNg^{-1} \subseteq N$ for all $g \in G$.

Lagrange's Theorem. If G is a finite group and H is a subgroup of G, then the order of H divides the order of G and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.

Cauchy's Theorem. If G s a finite group and p is a prime dividing $|G|$ then G has an element of order p.

Definition 3.5. (Dedekind and Hamiltonian Groups) For any group G, if all the subgroups of G are normal then G is called a *Dedekind* group. If G is non-abelian then G is called a *Hamiltonian* group.

Theorem 3.6. If G is a finite group of order $p^\alpha m$, where p is a prime and p does not divide m, then G has a subgroup of order p^α (Proof will be done with the big Sylow theorem).

Definition 3.7. Let H and K be subgroups of a group and define

$$HK = \{hk |\ h \in H,\ k \in K\}.$$

Proposition 3.8. If H and K are subgroups of a group then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Corollary 3.9. If H and K are subgroups of G then HK is a subgroup if H normalizes K (i.e. if $H \subseteq N_G(K)$).

==========

Isomorphism Theorems

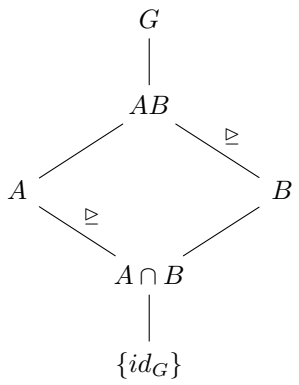
==========

Theorem 3.10. *(First Isomorphism Theorem)* If $\varphi : G \to H$ is a homomorphism of groups, then $\ker(\varphi) \trianglelefteq G$ and $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

Corollary 3.11. Let $\varphi : G \to H$ be a homomorphism of groups.

1. φ is injective if and only if $\ker(\varphi) = id_G$.
2. $|G : \ker(\varphi)| = |\mathrm{im}(\varphi)|$.

Theorem 3.12. *(The Second or Diamond Isomorphism Theorem)* Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.



Theorem 3.13. *(The Third Isomorphism Theorem)* Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K$$

Theorem 3.14. *(The Fourth Isomorphism Theorem)* Let G be a group and let N be a normal subgroup of G. The there is a bijection from the set $\mathcal{S}$ of subgroups A of G which contain N onto the set $\mathcal{T}$ of subgroups of the quotient group G/N. Specifically, there is a bijective map $\varphi : \mathcal{S} \to \mathcal{T} : A \mapsto A/N$ and we have the following:

1. $A \leq B$ if and only if $A/N \leq B/N$,
2. if $A \leq B$, then $|B : A| = |B/N : A/N|$,
3. $\langle A, B\rangle/N = \langle A/N, B/N\rangle$,

4. $(A \cap B)/N = A/N \cap B/N$, and
5. $A \trianglelefteq G$ if and only if $A/N \trianglelefteq G/N$.

==========

==========

Theorem 3.15. *(Feit-Thompson)* If G is a simple group of odd order, then $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p.

Definition 3.16. A group G is ***solvable*** if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, n-1$.

Theorem 3.17. The finite group G is solvable if and only if for every divisor n of $|G|$ such that $\gcd\left(n, \frac{|G|}{n}\right) = 1$, G has a subgroup of order n.

Definition 3.18. The *alternating group of degree n*, denoted by A_n, is the kernel of the sign homomorphism acting on S_n.

Proposition 3.19. The permutation σ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.

4. Group Actions

Definition 4.1. Let G be a group acting on a nonempty set A. For each $g \in G$ the map

$$\sigma_g : A \to A : a \mapsto g \cdot a$$

is a permutation of A. The homomorphism associated to an action of G on A

$$\varphi : G \to S_A : \varphi(g) \mapsto \sigma_g$$

is called the *permutation representation* associated to the given action.

Definition 4.2. Let G be a group acting on a set A

1. The ***kernel*** of the action is the set of elements of G that act trivially on every element of A: $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$.
2. Fro each $a \in A$ the ***stabilizer*** of a in G is the set of elements of G that fix the element a: $\{g \in G \mid g \cdot a = a\}$ and is denoted by G_a.
3. An action is ***faithful*** if its kernel is the identity.

Corollary 4.3. Let G be a group acting on a set A. Two elements of G induce the same permutation on A if and only if they are in the same coset.

Proposition 4.4. Let G be a group acting on the nonempty set A. The relation on A defined by

$$a \sim b \quad \text{if and only if} \quad a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a.

Definition 4.5. Let G be a group acting on the nonempty set A.

1. The equivalence class $\{g \cdot a \mid g \in G\}$ is called the ***orbit*** of G containing a.

2. The action of G on A is called ***transitive*** if there is only one orbit, i.e., given any two elements $a, b \in A$ there is some $g \in G$ such that $a = g \cdot b$.

Theorem 4.6. Let G be a group, let H be a subgroup of G and let G act by left multiplication on the set A of left cosets of H in G. Let π_H be the associated permutation representation afforded by this action. Then

1. G acts transitively on A
2. the stabilizer in G of the point $1H \in A$ is the subgroup H
3. the kernel of the action (i.e., the kernel of π_H) is $\cap_{x \in G}\ xHx^{-1}$, and $\ker(\pi_H)$ is the largest normal subgroup of G contained in H.

Corollary 4.7. *(Cayley's Theorem)* Every group is isomorphic to a subgroup of some symmetric group. If G is of order n, then G is isomorphic to a subgroup of S_n.

Corollary 4.8. Let G be a simple, non-abelian group and let $H \leq G$. Then G is isomorphic to a subgroup of the symmetric group on G/H, $Sym(G/H)$.

Proof. Let G be a simple, non-abelian group and let $H \leq G$. Suppose that G acts on the coset space G/H by left multiplication. Obviously, this action is transitive, so we have that there is a homomorphism

$$\varphi : G \to Sym(G/H) : g \mapsto \sigma_g$$

where

$$\sigma_g : G/H \to G/H : xH \mapsto (g \cdot x)H.$$

Now, H is a proper subgroup, so $|G/H| > 1$, and since G acts transitively, we have that φ is nontrivial. This gives us that $\ker(\varphi) \neq G$, and since G is simple we get that φ is injective. ♣

Corollary 4.9. If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal. (Note: this is used mostly with subgroups of index 2)

Definition 4.10. Two elements a and b of G are said to be ***conjugate*** in G if there is some $g \in G$ such that $b = gag^{-1}$. The orbits of G acting on itself by conjugation are called *conjugacy classes* of G.

Definition 4.11. Two subsets S and T of G are said to be ***conjugate in G*** if there is some $g \in G$ such that $T = gSg^{-1}$.

Proposition 4.12. The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$.

Theorem 4.13. *(The Class Equation)* Let G be a finite group and let $g_1, g_2, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

Theorem 4.14. *(Orbit Stabilizer Theorem)* Let G be a group acting on a set A and consider some $a \in A$. Then

$$|Orb(a)| = |G : Stab(a)|.$$

Theorem 4.15. Every normal subgroup is the union of conjugacy classes.

Definition 4.16. Let G be a group. An isomorphism from G onto itself is called an ***automorphism***. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

Proposition 4.17. Let H be a normal subgroup of G. Then G acts by conjugation on H as automorphisms of H. More specifically, the action of G on H by conjugation is defined for each $g \in G$ by

$$h \mapsto ghg^{-1} \qquad \text{for each } h \in H.$$

For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism of G into $\mathrm{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Corollary 4.18. If K is any subgroup of the group G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.

Corollary 4.19. For any subgroup H of a group G the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.

Definition 4.20. Let G be a group and let $g \in G$. Conjugation by g is called an ***inner automorphism*** of G and the subgroup of $\mathrm{Aut}(G)$ consisting of all inner automorphisms is denoted by $\mathrm{Inn}(G)$.

Note: For any group G we have that

$$\mathrm{Inn}(G) \cong G/Z(G).$$

This is really useful when proving that $\mathrm{Aut}(G)$ is nontrivial.

Definition 4.21. A subgroup H of a group G is called ***characteristic*** in G, denoted H char G, if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$ for all $\sigma \in Aut(G)$.

Proposition 4.22. *(Properties of Characteristic Subgroups)*

1. characteristic subgroups are normal
2. if H is the unique subgroup of G of a given order, then H is characteristic in G, and
3. if K char H and $H \trianglelefteq G$, then $K \trianglelefteq G$.

Proposition 4.23. The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, and abelian group of order $\varphi(n)$ (where φ is Euler's function).

==========

Sylow Theorems

==========

Definition 4.24. Let G be a group and let p be a prime.

1. A group of order p^α for some $\alpha \geq 0$ is called a ***p-group***. Subgroups of G which are p-groups are called ***p-subgroups***.
2. If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a ***Sylow p-subgroup*** of G.
3. The set of Sylow p-subgroups of G will be denoted by $Syl_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$.

Theorem 4.25. *(Sylow's Theorem)* Let G be a group of order $p^\alpha m$, where p is a prime not dividing m.

1. Sylow p-subgroups of G exist.

2. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.

3. The number of Sylow p-subgroups in G is of the form $1 + kp$, i.e.,

$$n_p \equiv 1 \mod p.$$

Further, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, hence n_p divides m.

Lemma 4.26. Let $P \in Syl_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.

Theorem 4.27. A nontrivial p-group has a nontrivial center.

Proof. Let G be a nontrivial p-group, and P the set of order-p elements of G. We have seen that P is nonempty, and indeed that $|P|$ is congruent to $-1 \mod p$. Now consider the action of G on P by conjugation. The stabilizer under this action of any x in P is the centralizer $C(x)$ of x, which is the subgroup of G consisting of all elements that commute with x. The orbit of x then has size $[G : C(x)]$. But G is a p-group, so $[G : C(x)]$ is a power of p. Hence $[G : C(x)]$ is either 1 or a multiple of p. Since $|P|$ is not a multiple of p, it follows that at least one of the orbits is a singleton. Then $C(x) = G$, which is to say that x commutes with every element of G. We have thus found a nontrivial element x of the center of G. ♣

Corollary 4.28. Let P be a Sylow p-subgroup of G. Then the following are equivalent:

1. P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$
2. P normal in G
3. P is characteristic in G
4. All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-subgroup.

5. Direct and Semidirect Products and Abelian Groups

Proposition 5.1. Let $G_1, G_2, \ldots, G_n$ be groups and let $G = G_1 \times G_2 \times \cdots \times G_n$ be their direct product.

1. For each fixed i the set of elements of G which have the identity of G_j in the j^{th} position for all $j \neq i$ and arbitrary elements of G_i in position i is a subgroup of G isomorphic to G_i:

$$G_i \cong \{(1, 1, \ldots, 1, g_i, 1, \ldots, 1) \mid g_i \in G_i\}.$$

If we identify G_i with this subgroup, then $G_i \trianglelefteq G$ and

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

2. for each fixed i define $\pi_i : G \to G_i$ by

$$\pi_i((g_1, g_2, \ldots, g_n)) = g_i.$$

Then π_i is a surjective homomorphism with

$$\begin{aligned} \ker(\pi_i) &= \{(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, 1) \mid g_j \in G_j \text{ for all } j \neq i\} \\ &\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n. \end{aligned}$$

3. Under the identifications in part (1), if $x \in G_i$ and $y \in G_j$ then $xy = yx$.

Definition 5.2.

1. A group G is *finitely generated* if there is a finite subset A of G such that $G = \langle A \rangle$.

2. For each $r \in \mathbb{Z}$ with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the *free abelian group of rank r*.

Theorem 5.3. *(Fundamental Theorem of Finitely Generated Abelian Groups)* Let G be a finitely generated abelian group. Then

1. $$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}$$
   for some integers $r, n_1, n_2, \ldots, n_s$ satisfying the following conditions:
   (a) $r \geq 0$ and $n_j \geq 2$ for all j, and
   (b) $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$.
2. the expression in (1) is unique.

Definition 5.4. The integer r in the previous theorem is called the *free rank* or *Betti number* of G and the integers $n_1, n_2, \ldots, n_s$ are called the *invariant factors* of G. The description

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}$$

is called the *invariant factor decomposition* of G.

Corollary 5.5. If n is the product of distinct primes, then up to isomorphism the only abelian group of order n is the cyclic group of order n, $\mathbb{Z}/n\mathbb{Z} = Z_n$.

Theorem 5.6. Let G be an abelian group of order $n > 1$ and let the unique factorization of n distinct prime powers be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then

1. $G \cong A_1 \times A_2 \times \cdots \times A_k$, where $|A_i| = p_i^{\alpha_i}$
2. for each $A \in \{A_1, A_2, \ldots, A_k\}$ with $|A| = p^\alpha$,
   $$A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \cdots \times Z_{p^{\beta_t}}$$
   with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$
3. the decomposition in (1) and (2) is unique.

Definition 5.7. The integers p^{β_j} described in the preceding theorem are called the *elementary divisors* of G. The description of G given in the first two parts of the previous theorem is called the *elementary divisor decomposition* of G.

Proposition 5.8. Let $m, n \in \mathbb{Z}^+$

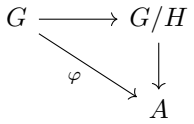
1. $Z_m \times Z_n \cong Z_{mn}$ if and only if $\gcd(m, n) = 1$.
2. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ then $Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$

Definition 5.9. Let G be a group, let $x, y \in G$ and let A, B be nonempty subsets of G.

1. Define $[x, y] = x^{-1}y^{-1}xy$, called the *commutator* of x and y.
2. Define $[A, B] = \langle [a, b] \mid a \in A,\ b \in B \rangle$, the group generated by commutator of elements from A and B.
3. Define $G' = \langle [x, y] \mid x, y \in G \rangle$, the subgroup of G generated by the commutators of elements from G, called the *commutator subgroup* of G.

Proposition 5.10. Let G be a group, let $x, y \in G$ and let $H \leq G$. Then

1. $xy = xy[x, y]$.
2. $H \trianglelefteq G$ if and only if $[H, G] \leq H$.
3. $\sigma([x, y]) = [\sigma(x), \sigma(y)]$ for any $\sigma \in \mathrm{Aut}(G)$, G' char G, and G/G' is abelian.
4. G/G' is the largest abelian quotient of G in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$ and $H \trianglelefteq G$, then G/H is abelian.
5. If $\varphi : G \to A$ is any homomorphism of G into an abelian group A, then φ factors through G' i.e. $G' \leq \ker(\varphi)$ and the following diagram commutes



Proposition 5.11. Let H and K be subgroup of the group G. The number of distinct ways of writing each element of the set HK in the form hk, for some $h \in H$ and $k \in K$ is $|H \cap K|$. In particular, if $H \cap K = 1$, the each element of HK can be written uniquely as a product hk, for some $h \in H$ and $k \in K$.

Theorem 5.12. *(Product Recognition)* Suppose G is a group with subgroups H and K such that

1. H and K are normal in G, and
2. $H \cap K = 1$.

Then $HK \cong H \times K$.

Definition 5.13. If G is a group and H and K are normal subgroups of G with $H \cap K = 1$ then we call HK the *internal direct product* of H and K. We shall call $H \times K$ the *external direct product* of H and K (Note: This difference purely determines the notation of the elements of the group as these two are isomorphic by the recognition theorem).

Theorem 5.14. Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. Let $\cdot$ denote the (left) action of K on H determined by φ. Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define the following multiplication on G:

$$(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1 k_2).$$

1. This multiplication makes G into a group of order $|H||K|$.
2. The sets $\{(h, 1) \mid h \in H\}$ and $\{(1, k) \mid k \in K\}$ are subgroups of G and the maps $h \mapsto (h, 1)$ for $h \in H$ and $k \mapsto (1, k)$ for $k \in K$ are isomorphisms of these subgroups with the groups H and K respectively:

$$H \cong \{(h, 1) \mid h \in H\} \quad \text{and} \quad K \cong \{(1, k) \mid k \in K\}.$$

3. $\widehat{H} = \{(h, 1) \mid h \in H\} \trianglelefteq G$
4. $\widehat{H} \cap \widehat{K} = 1$
5. for all $h \in \widehat{H}$ and $k \in \widehat{K}$, $khk^{-1} = k \cdot h = \varphi(k)(h)$.

Definition 5.15. Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. The group described in Theorem 5.14 is called the *semidirect product* of H and K with respect to φ and will be denoted $H \rtimes_\varphi K$ (or simply $H \rtimes K$).

Proposition 5.16. Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then the following are equivalent:

1. the identity (set) map between $H \rtimes K$ and $H \times K$ is a group homomorphism
2. φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$
3. $K \trianglelefteq H \rtimes K$.

Theorem 5.17. Suppose G is a group with subgroups H and K such that

1. H and K are normal in G, and
2. $H \cap K = 1$.

Let $\varphi : K \to \mathrm{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Then $HK \cong H \times K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then G is the semidirect product of H and K.

Definition 5.18. Let H be a subgroup of G. A subgroup K is called a ***compliment*** for H in G if $G = HK$ and $H \cap K = 1$.

6. Futher Topics in Group Theory

Definition 6.1. A ***maximal subgroup*** of a group G is a proper subgroup M of G such that there are no subgroups H of G such that $M < H < G$.

Theorem 6.2. Let p be a prime and let P be a group of order p^a, $a \geq 1$. Then

1. The center of P is nontrivial.
2. If H is a nontrivial normal subgroup of P then H intersects the center non-trivially. In particular, every subgroup of order p is contained in the center.
3. If H is a normal subgroup of P then H contains a subgroup of order p^b that is normal in P for each divisor p^b of $|H|$. In particular, P has a normal subgroup of order p^b for every $b \in \{1, 2, \ldots, a\}$.
4. Let $H < P$ then $H < N_P(H)$.
5. Every maximal subgroup of P is of index p and is normal in P.

Definition 6.3.

1. For any (finite or infinite) group G define the following subgroups inductively

$$Z_0(G) = 1, \qquad Z_1(G) = Z(G)$$

and $Z_{i+1}(G)$ is the subgroup of G containing $Z_i(G)$ such that

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

(i.e. $Z_{i+1}(G)$ is the complete preimage in G of the center of $G/Z_i(G)$ under the natural projection). The chain of subgroups

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$$

is called the ***upper central series of*** G.

2. A group G is called ***nilpotent*** if $Z_c(G) = G$ for some $c \in \mathbb{Z}$. The smallest such c is called the *nilpotence class of* G.

Proposition 6.4. Let p be a prime and let P be a group of order p^a. Then P is nilpotent of nilpotence class at most $a - 1$ for $a \geq 2$.

Proof. For each $i \geq 0$, $P/Z_i(P)$ is a p-group, so if

$$|P/Z_i(P)| > 1 \text{ then } Z(P/Z_i(P) \neq 1$$

by Theorem 6.1 (1). Thus if $Z_i(P) \neq P$ then we have that $|Z_{i+1}(P) \geq p|Z_i(P)|$and so $|Z_{i+1}(P) \geq p^{i+1}$. In particular $|Z_a(P)| \geq p^a$, so $P = Z_a(P)$. The only way P could be of nilpotence class exactly equal to a would be if $|Z_i(P)| = p^i$ for all i. In this case, however, Z_{a-2} would have index p^2 in P, so $P/Z_{a-2}(P)$ would be abelian by Corollary 4.9. But then $P/Z_{a-1}(P)$ would equal its center and so $Z_{a-1}(P)$ would equal P $\lightning$. This proves that the class of P is $\leq a-1$. ♣

Theorem 6.5. Let G be a finite group, let $p_1, p_2, \ldots, p_s$ be the distinct primes dividing the order, and let $P_i \in Syl_{p_i}(G)$, $1 \leq i \leq s$. Then the following are equivalent:

1. G is nilpotent
2. if $H < G$ then $H < N_G(H)$
3. $P_i \trianglelefteq G$ for $1 \leq i \leq s$, i.e., every Sylow subgroup is normal in G
4. $G \cong P_1 \times P_2 \times \cdots \times P_s$.

Corollary 6.6. A finite abelian group is the direct product of its Sylow subgroups (all abelian groups are nilpotent of rank 1).

Proposition 6.7. If G is a finite group such that for all positive integers n dividing its order, G contains at most n elements x satisfying $x^n = 1$, then G is cyclic.

Proposition 6.8. *(Frattini's Argument)* Let G be a group, let H be a normal subgroup of G, and let $P \in Syl_p(H)$. Then $G = HN_G(P)$ and $|G : H|$ divides $|N_G(P)|$.

Proposition 6.9. A finite group is nilpotent if and only if every maximal subgroup is normal.

Definition 6.10. For any (finite or infinite) group G define the following subgroups inductively:

$$G^0 = G, \qquad G^1 = [G, G], \quad \text{and} \quad G^{i+1} = [G, G^i].$$

The chain of groups

$$G^0 \geq G^1 \geq G^2 \geq \cdots$$

is called the ***lower central series of*** G.

Theorem 6.11. A group G is nilpotent if and only if $G^n = 1$ for some $n \geq 0$. More precisely, G is nilpotent of class c if and only if c is the smallest nonnegative integer such that $G^c = 1$. If G is nilpotent of class c then

$$G^{c-1} \leq Z_i(G) \quad \text{for all } i \in \{0, 1, \ldots, c\}.$$

Definition 6.12. For any group G define the following sequence of subgroups inductively:

$$G^{(0)} = G, \qquad G^{(1)} = [G, G], \quad \text{and} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad \text{for all } i \geq 1.$$

This series of subgroups is called the *derived* or *commutator* series of G.

Theorem 6.13. A group G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 0$.

Proof. Assume that G is solvable and so possesses a series

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$$

such that each factor H_{i+1}, H_i is abelian. We prove by induction that $G^{(i)} \leq H_{s-i}$. This is true for $i = 0$, so assume that $G^{(i)} \leq H_{s-i}$. Then

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [H_{s-i}, H_{s-i}].$$

Since G is solvable, we know that H_{s-i}/H_{s-i-1} is abelian. Moreover, $[H_{s-i}, H_{s-i}]$ is the commutator subgroup of H_{s-1}, so $H_{s-i}/[H_{s-i}, H_{s-i}]$ is the largest abelian quotient of H_{s-i} which gives us that $[H_{s-i}, H_{s-i}] \leq H_{s-i-1}$. Thus $G^{(i+1)}[H_{s-i}, H_{s-i}] \leq H_{s-i-1}$. Since $H_0 = 1$, we have that $G^{(s)} = 1$.

Conversely, if $G^{(n)} = 1$ for some $n \geq 0$ then if we take $H_i = G^{(n-i)}$ we have H_i is the largest abelian quotient of H_{i+1}. Thus the commutator series satisfies the condition for solvability. ♣

Proposition 6.14. Let G and K be groups, let H be a subgroup of G, and let $\varphi : G \to K$ be a surjective homomorphism.

1. $H^{(i)} \leq G^{(i)}$ for all $i \geq 0$. In particular, if G is solvable, then so is H.
2. $\varphi(G^{(i)}) = K^{(i)}$. In particular, homomorphic images and quotient groups of solvable groups are solvable.
3. If $N \trianglelefteq G$ and both N and G/N are solvable then so is G.

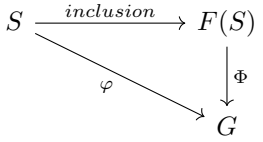
Theorem 6.15. Let G be a finite group.

1. (Burnside) If $|G| = p^a q^b$ for some primes p and q, then G is solvable.
2. (Phillip Hall) If for every prime p dividing $|G|$ we factor the order of G as $|G| = p^a m$ where $\gcd(p, m) = 1$, and G has a subgroup of order m, then G is solvable.
3. (Feit-Thompson) If $|G|$is odd then G is solvable.
4. (Thompson) If for every pair of elements $x, y \in G$, $\langle x, y \rangle$ is a solvable group, then G is solvable.

- Free Groups -

The basic idea behind a free group $F(S)$ generated by a set S is that there are no relations satisfied by any of the elements of S (in this sense S can be considered "free" of relations). Now, if we let S be an arbitrary set then a ***word*** in S is a finite sequence of elements of S. We can then define $F(S)$ to simply be the set of all words in S. We shall use this idea to carry out a formal construction of $F(S)$ for an arbitrary S below.

One of the important properties that reflects the fact that there are no relations that must be satisfied by members of S is that any *map* from the set S to a group G can be ***uniquely extended*** to a homomorphism from the group $F(S)$ to G. This is called the ***universal property*** of the free group and is what characterizes the group $F(S)$.



Now, the difficulty in the construction of $F(S)$ is the proof that the word concatenation operation is both well defined and associative. If we say that S is given as a set of literals, then we can define a set S^{-1} such that there is a bijection from the set S to the set S^{-1} as given by sending $s \in S$ to its corresponding $s^{-1} \in S^{-1}$. If we then take some singleton set that is not contained in either S or S^{-1} and call it $\{1\}$. If we then join these sets we can take any $x \in S \cup S^{-1} \cup \{1\}$ and declare that $x^1 = x$. This allows us to think of words of S as finite products of members of S and their inverses. A word $s = (s_1, s_2, s_3, \ldots)$ is then said to be *reduced* if

1. $s_{i+1} \neq s_i^{-1}$ for all i with $s_i \neq 1$
2. if $s_k = 1$ for some k, then $s_i = 1$ for all $i \geq k$

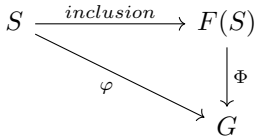
The reduced word $(1, 1, 1, \ldots)$ is called the *empty word* and is denoted by 1. If we let $F(S)$ be the set of reduced words on S then we can embed S into $F(S)$ by

$$s \mapsto (s, 1, 1, 1, \ldots).$$

Under this set injection we identify S with its image and henceforth consider S as a subset of $F(S)$. We can then introduce a binary operation on the set $F(S)$ to the tune of word concatenation followed by reduction (this is pretty self-explanatory), and with the introduction of this operation we get our first theorem of this section.

Theorem 6.16. $F(S)$ is a group under the binary operation given above.

Theorem 6.17. Let G be a group, S a set and $\varphi : S \to G$ a set map. Then there is a unique group homomorphism $\Phi : F(S) \to G$ such that the following diagram commutes:



Proof. If such a map were to exist, then Φ must satisfy $\Phi(s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_n^{\varepsilon_n}) = \varphi(s_1)^{\varepsilon_1} \varphi(s_2)^{\varepsilon_2} \cdots \varphi(s_n)^{\varepsilon_n}$ if it is so be a homomorphism (which gives us uniqueness), and the fact that this actually is a homomorphism follows almost directly. ♣

Definition 6.18. The group $F(S)$ is called the *free group* on the set S. A group F is a *free group* if there is some set S such that $F = F(S)$ – in this case we call S the set of *free generators* of F. The cardinality of S is called the *rank* of the free group.

Definition 6.19. Let S be a subset of a group G such that $G = \langle S \rangle$.

CHAPTER 16

Semidirect products are split short exact sequences

Chit-chat 16.1. Last time we talked about short exact sequences

$$G \to H \to K.$$

To make things easier to read, from now on we'll write

$$L \to H \to R.$$

The L is for left, the R is for right. Since $L \to H$ is injective, from now on we'll identify L with its image in H for simplicity of notation.

Note there is no way to think of R as a subgroup of H a priori. For instance, in the example

$$\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

the second copy of $\mathbb{Z}/2\mathbb{Z}$ doesn't naturally "embed" back into $\mathbb{Z}/4\mathbb{Z}$.

Proposition 16.2. The above short exact sequence doesn't split.

PROOF. $\mathbb{Z}/2\mathbb{Z}$ only has elements of order 1 and 2, so no homomorphism $j : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ can have an image containing elements of order ≥ 3. [1]

But let's observe that both [1] and [3] are elements of order 4 inside $\mathbb{Z}/4\mathbb{Z}$:

$$\langle [1] \rangle = \{[1], [2], [3], [0]\}, \qquad \langle [3] \rangle = \{[3], [6] = [2], [5] = [1], [0]\}.$$

Hence any homomorphism $j : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ must have image contained in $\{[0], [2]\} \subset \mathbb{Z}/4\mathbb{Z}$. But this is the kernel of the map from $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ above; so no j could factor the identity map of $R = \mathbb{Z}/2\mathbb{Z}$. □

Here's a more dramatic example:

Example 16.3. The short exact sequence

$$\mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

does not split for any $n \neq -1, 0, 1$. [2]

[1] After all, if $g^n = 1$, we must have that $j(g)^n = 1$ as well.

[2] Any homomorphism from $\mathbb{Z}/n\mathbb{Z}$ must send an element of order n to some element of finite order. But $\mathbb{Z}$ has no element of finite order except 0, so there is no injection from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}$.

Chit-chat 16.4. Since this is our first time trying to understand short exact sequences, let's try to analyze the case where we *are* allowed to think of R as a subgroup of H. If both L and R are inside H, maybe you'll buy the philosophy more that H is "built up" from L and R. So we come to the definition we ended with last time:

Definition 16.5. A short exact sequence *splits* if there is a group homomorphism $j : R \to H$ such that the composition $R \xrightarrow{j} H \to R$ is equal to id_R. We will call a choice of $j : R \to H$ a *splitting*.

Chit-chat 16.6. So if the short exact sequence is given by homomorphisms $\phi : L \to H, \psi : H \to R$, the definitions says that $\psi \circ j = \mathrm{id}_R$. In particular, j is an *injection*.

Chit-chat 16.7. In the above example, clearly there is no way to think about $\mathbb{Z}/n\mathbb{Z}$ as a subgroup of $\mathbb{Z}$.

Chit-chat 16.8. So we have a new idea. We'd like to be able to recognize semidirect products in nature, and we'd like to be able to produce examples! Let's analyze.

As before, let's identify R with $j(R)$ when we have a split short exact sequence. Well, every element of R defines an action on H itself by conjugation: $h \mapsto rhr^{-1}$. But since L is normal, $rLr^{-1} = L$, so this defines an action on L, via $C_r : l \mapsto rlr^{-1}$.

Moreover, this is a group isomorphism from L to itself. As you showed in your homework, this defines a group homomorphism $R \to \mathrm{Aut}(L)$ given by $r \mapsto C_r$. So any splitting gives rise to a homomorphism $R \to \mathrm{Aut}(L)$. [3]

Question 16.9. Fix two groups R and L. The natural question is: Does any homomorphism $R \to \mathrm{Aut}(L)$ give rise to a split exact sequence?

Chit-chat 16.10. Another observation is that, given a splitting, both R and L become subgroups of H. Moreover, their intersection consists only of 1_H—after all, if a non-identity element $l \in L \cap R$, then the map $R \to H \to R$ could not be injective (l would be in the image of R, hence in the kernel of $H \to L$). Finally, since the orbits of the L action span H itself, we see that $H = \bigcup_{r \in R} Lr$. That is, $H = LR$.[4]

[3] Here, $\mathrm{Aut}(L)$ refers to the group of *group automorphisms*; not of set automorphisms.

[4] See below.

Definition 16.11. Let L, R be subgroups of H. We let

$$LR = \{g \text{ such that } g = lr \text{ for some } l \in L, r \in R\}.$$

Question 16.12. Fix $L, R \subset H$. If $L \cap R = \{1\}$, $L \subset H$ is normal, and $LR = H$, is H a semidirect product of L and R?

What good questions we ask, when the answers are yes!

Theorem 16.13. Fix a normal subgroup $L \subset H$, and let $R \cong H/L$. The following are equivalent:

(1) A homomorphism $j : R \to H$ splitting a short exact sequence $L \to H \to R$.
(2) An isomorphism $R \to R'$ to a subgroup $R' \subset H$ such that $R' \cap L = \{1\}$ and the set map $L \times R' \to H$ is a surjection.
(3) A group homomorphism $\phi : R \to \mathrm{Aut}(L)$.

Proof. Another time. □

Chit-chat 16.14. Of these, my favorite interpretation is the last. It's because it has no reference to the group H—once you construct a group homomorphism $\phi : R \to \mathrm{Aut}(L)$, one can construct a short exact sequence $L \to H \to R$.

What is the group operation on H in terms of R and L?

Proposition 16.15. Fix a homomorphism

$$\phi : R \to \mathrm{Aut}(L), \qquad r \mapsto \phi_r.$$

Then

(1) the following defines a group structure on the set $L \times R$:

$$(l_1, r_1) \cdot (l_2, r_2) := (l_1 \cdot \phi_{r_1}(l_2), r_1 r_2).$$

Moreover,
(2) The set $\{(l, 1)\}$ is a normal subgroup isomorphic to L,
(3) The set $\{(1, r)\}$ is a subgroup isomorphic to R.

Definition 16.16. Given $\phi : R \to \mathrm{Aut}(L)$, we will write

$$L \rtimes_\phi R$$

to be the group defined in the above proposition. We call it the *semidirect product* of L by R. When ϕ is implicit, we will drop the subscript and simply write

$$L \rtimes R.$$

PROOF. Clearly, $(1,1)$ is the identity element, since $\phi_1 = \mathrm{id}_L$. Likewise, the inverse to (l,r) is the element $(\phi_r^{-1}(l^{-1}), r^{-1})$:

$$\begin{aligned}(\phi_r^{-1}(l^{-1}), r^{-1}) \cdot (l,r) &= (\phi_r^{-1}(l^{-1}) \cdot \phi_{r^{-1}}(l), r^{-1}r) \\ &= (\phi_r^{-1}(l^{-1}) \cdot \phi_r^{-1}(l), r^{-1}r) \\ &= (\phi_r^{-1}(l^{-1}l), r^{-1}r) \\ &= (1,1).\end{aligned}$$

and

$$\begin{aligned}(l,r) \cdot (\phi_r^{-1}(l^{-1}), r^{-1}) &= (l\phi_r(\phi_r^{-1}(l^{-1})), rr^{-1}) \\ &= (ll^{-1}, rr^{-1}) \\ &= (1,1).\end{aligned}$$

I'll leave it to you to check associativity. □

Chit-chat 16.17. Next time, we'll study the symmetries of the regular n-gon. This group can be written as a semi-direct product.

1. Some practice

Exercise 16.18. If L and R are finite groups, and if one has a short exact sequence $1 \to L \to H \to R \to 1$, verify that $|H| = |L| \cdot |R|$.

Exercise 16.19. If L is an abelian group, show that the "inversion" map $a \mapsto a^{-1}$ is a group automorphism. Show that this defines a group homomorphism $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(L)$.

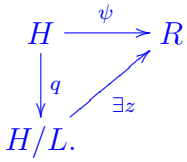
Exercise 16.20. Convince yourself that all the non-splitting short exact sequences from this lecture really don't split.

2. Proof that $H = LR$

By request, here is a more detailed proof that $H = LR$ when the SES splits.

Lemma 16.21. Let $L \to H \xrightarrow{\psi} R$ be a short exact sequence. Let $q : H \to H/L$ be the quotient homomorphism sending $h \mapsto Lh$. Then there exists an isomorphism $z : H/L \to R$ such that $z \circ q = \psi$. (That is, there exists a z so

that the diagram



is commutative.)

Once we have the lemma, we have

Corollary 16.22. If $j : R \to H$ is a splitting of the $L \to H \to R$, then

$$H = \bigcup_{r \in R} Lj(r).$$

Proof of corollary. By definition of splitting, we have that $\psi \circ j = \mathrm{id}_R$. On the other hand, we know that $\psi = z \circ q$ by the Lemma, so we have

$$z \circ q \circ j = \mathrm{id}_R .$$

Since z is a group isomorphism, its inverse is a homomorphism, and we have an equality of homomorphisms

$$q \circ j = z^{-1}.$$

Now we interpret the map $q \circ j$. The homomorphism q sends $h \mapsto Lh$. So the composite $q \circ j$ sends r to the coset $Lj(r) \in H/L$. Well, z^{-1} is a bijection onto H/L, so for any coset $Lh \in H/L$, we have a unique $r \in R$ for which $Lh = Lj(r)$. Since

$$\bigcup_{H/L} Lh = H,$$

this proves that

$$\bigcup_{r \in R} Lj(r) = H.$$

In the notes above, we identified elements $r \in R$ with their image in H using j, so we wrote this as

$$\bigcup_{r \in R} Lr = H.$$

□

SPLITTING OF SHORT EXACT SEQUENCES FOR GROUPS

KEITH CONRAD

1. Introduction

A sequence of groups and group homomorphisms

$$H \xrightarrow{\alpha} G \xrightarrow{\beta} K$$

is called *exact* at G if $\operatorname{im}\alpha = \ker\beta$. This means two things: the image of α is killed by β ($\beta(\alpha(h)) = 1$ for all $h \in H$), so $\operatorname{im}\alpha \subset \ker\beta$, and also *only* the image of α is killed by β (if $\beta(g) = 1$ then $g = \alpha(h)$ for some h), so $\ker\beta \subset \operatorname{im}\alpha$. For example, to say $1 \longrightarrow G \xrightarrow{f} K$ is exact at G means f is injective, and to say $H \xrightarrow{f} G \longrightarrow 1$ is exact at G means f is surjective. There is no need to label the homomorphisms coming out of 1 or going to 1 since there is only one possible choice. If the group operations are written additively, we may use 0 in place of 1 for the trivial group.

A *short exact sequence* of groups is a sequence of groups and group homomorphisms

$$1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1 \tag{1.1}$$

which is exact at H, G, and K. That means α is injective, β is surjective, and $\operatorname{im}\alpha = \ker\beta$.

A more general exact sequence can have lots of terms:

$$G_1 \xrightarrow{\alpha_1} G_2 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_{n-1}} G_n, \tag{1.2}$$

and it must be exact at each G_i for $1 < i < n$. Exact sequences can also be of infinite length in one or both directions. We will only deal with short exact sequences here.

Exact sequences first arose in algebraic topology, and the later development of homological algebra (the type of algebra underlying algebraic topology) spread exact sequences into the rest of mathematics.

Example 1.1. The determinant on $\mathrm{GL}_2(\mathbf{R})$ gives rise to a short exact sequence

$$1 \longrightarrow \mathrm{SL}_2(\mathbf{R}) \longrightarrow \mathrm{GL}_2(\mathbf{R}) \xrightarrow{\det} \mathbf{R}^\times \longrightarrow 1.$$

Example 1.2. When $N \lhd G$ we have a short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1, \tag{1.3}$$

where the map from N to G is inclusion, and the map from G to G/N is reduction mod N.

This example is the prototype for all short exact sequences, as we'll see below.

Example 1.3. For two groups H and K, the direct product $H \times K$ fits into the short exact sequence

$$1 \longrightarrow H \longrightarrow H \times K \longrightarrow K \longrightarrow 1,$$

where the map out of H is embedding to the first factor ($h \mapsto (h, 1)$) and the map out of $H \times K$ is projection to the second factor ($(h, k) \mapsto k$).

Example 1.4. For two groups H and K, together with an action of K on H by automorphisms (a homomorphism $\varphi\colon K \to \mathrm{Aut}(H)$), the semidirect product $H \rtimes_\varphi K$ fits into the short exact sequence

$$1 \longrightarrow H \longrightarrow H \rtimes_\varphi K \longrightarrow K \longrightarrow 1,$$

where the maps are the same as in the previous example: $h \mapsto (h, 1)$ and $(h, k) \mapsto k$.

Every short exact sequence (1.1) is a disguised form of (1.3). Indeed, even though in (1.1) the group H may not literally be a subgroup of G and the group K may not literally be a quotient group of G, α restricts to an isomorphism of H with the subgroup $\alpha(H)(= \ker\beta)$ of G and β induces an isomorphism $\overline{\beta}$ of the quotient group $G/\alpha(H) = G/\ker\beta$ with K. Therefore we can place the general short exact sequence (1.1) and a short exact sequence of the type (1.3) in a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \overline{\beta}} & & \\ 1 & \longrightarrow & \alpha(H) & \longrightarrow & G & \longrightarrow & G/\ker\beta & \longrightarrow & 1 \end{array} \tag{1.4}$$

where the bottom short exact sequence is a special case of (1.3). The vertical maps are all isomorphisms, and in this sense (1.1) looks like (1.3): they are linked to each other through compatible isomorphisms of groups in the same positions in the two short exact sequences. (The compatibility of the isomorphisms simply means the diagram (1.4) commutes.)

In Section 2 we will look at some more examples of short exact sequences. Then in Section 3, which is the most important part, we will see how direct products and semidirect products of groups can be characterized in terms of short exact sequences with extra structure. Section 4 discusses the idea of two short exact sequences being alike in broad terms.

2. Examples

When $N \lhd G$, knowing N and G/N does not usually tell us what G is. That is, nonisomorphic groups can have isomorphic normal subgroups with isomorphic quotient groups. For example, $D_4 \ncong Q_8$ but $\langle r^2\rangle \cong \{\pm 1\}(\cong \mathbf{Z}/2\mathbf{Z})$ and $D_4/\langle r^2\rangle \cong Q_8/\{\pm 1\}(\cong (\mathbf{Z}/2\mathbf{Z})^2)$. In terms of short exact sequences, the two short exact sequences

$$1 \longrightarrow \langle r^2\rangle \longrightarrow D_4 \longrightarrow D_4/\langle r^2\rangle \longrightarrow 1$$

and

$$1 \longrightarrow \{\pm 1\} \longrightarrow Q_8 \longrightarrow Q_8/\{\pm 1\} \longrightarrow 1 \tag{2.1}$$

have isomorphic first groups and isomorphic third groups, but nonisomorphic middle groups. Here is a third example like these, with an abelian group in the middle:

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow \mathbf{Z}/2\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^2 \longrightarrow (\mathbf{Z}/2\mathbf{Z})^2 \longrightarrow 0.$$

This is the short exact sequence for a direct product, as in Example 1.3.

Here are two examples of short exact sequences with first group $\mathbf{Z}/4\mathbf{Z}$ and third group $\mathbf{Z}/2\mathbf{Z}$, but nonisomorphic groups in the middle:

$$0 \longrightarrow \mathbf{Z}/4\mathbf{Z} \longrightarrow \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0$$

$$0 \longrightarrow \mathbf{Z}/4\mathbf{Z} \longrightarrow \mathbf{Z}/8\mathbf{Z} \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0,$$

where the map $\mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/8\mathbf{Z}$ in the second short exact sequence is doubling ($x \bmod 4 \mapsto 2x \bmod 8$). The other maps are all the obvious ones.

Here are two short exact sequences with first and third groups equal to μ_m ($m > 1$) but nonisomorphic groups in the middle:

$$1 \longrightarrow \mu_m \longrightarrow \mu_m \times \mu_m \longrightarrow \mu_m \longrightarrow 1$$

and

$$1 \longrightarrow \mu_m \xrightarrow{\iota} \mu_{m^2} \xrightarrow{z \mapsto z^m} \mu_m \longrightarrow 1.$$

The first short exact sequence is the usual one for a direct product. In the second short exact sequence, ι is the inclusion. The middle groups $\mu_m \times \mu_m$ and μ_{m^2} are not isomorphic since $\mu_m \times \mu_m$ is not cyclic (no element of order m^2).

3. Direct and Semidirect Products

For two groups H and K, an important "lifting" problem is the determination of all groups G having a normal subgroup isomorphic to H and corresponding quotient group isomorphic to K. Such G are the groups that fit into a short exact sequence $1 \longrightarrow H \longrightarrow G \longrightarrow K \longrightarrow 1$. There is always at least one such G, namely $H \times K$. More generally, a semidirect product $H \rtimes_\varphi K$ always sits in a short exact sequence having kernel H and image K (Example 1.4). Not all short exact sequences arise from semidirect products.

Example 3.1. In the short exact sequence (2.1), Q_8 is not isomorphic to a semidirect product of $\{\pm 1\}$ and $Q_8/\{\pm 1\} \cong (\mathbf{Z}/2\mathbf{Z})^2$ since such a semidirect product has more than 1 element of order 2 while Q_8 has only one element of order 2.

Since semidirect products are "known," short exact sequences made with them are considered "trivial" (even though semidirect products may seem like a nontrivial way to create groups). It is important to recognize if a short exact sequence $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$ is essentially that for a direct product $H \times K$ or semidirect product $H \rtimes_\varphi K$. The next two theorems give such criteria in terms of a left inverse for α and a right inverse for β.

Theorem 3.2. *Let $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$ be a short exact sequence of groups. The following are equivalent:*

1. *There is a homomorphism $\alpha' \colon G \to H$ such that $\alpha'(\alpha(h)) = h$ for all $h \in H$.*
2. *There is an isomorphism $\theta \colon G \to H \times K$ such that the diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \times K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

commutes, where the bottom row is the short exact sequence for a direct product.

The commutative diagram in (2) says that θ identifies α with the embedding $H \to H \times K$ and β with the projection $H \times K \to K$. So the point of (2) is not simply that G is isomorphic to $H \times K$, but it is in a way that turns α and β into the standard maps from H to $H \times K$ and from $H \times K$ to K.

The key point of (1) is that α' is a homomorphism. Merely from α being injective, there is a *function* $\alpha' \colon G \to H$ such that $\alpha'(\alpha(h)) = h$ for all h, for instance the function

$$\alpha'(g) = \begin{cases} 1, & \text{if } g \notin \alpha(H), \\ h, & \text{if } g = \alpha(h). \end{cases}$$

But this α' is almost surely not a homomorphism.

Proof. (1) $\Rightarrow$ (2): Define $\theta\colon G \to H \times K$ by

$$\theta(g) = (\alpha'(g), \beta(g)).$$

This is a homomorphism since α' and β are homomorphisms. To see θ is injective, suppose $\theta(g) = (1,1)$, so $\alpha'(g) = 1$ and $\beta(g) = 1$. From exactness at G, the condition $\beta(g) = 1$ implies $g = \alpha(h)$ for some $h \in H$. Then $1 = \alpha'(g) = \alpha'(\alpha(h)) = h$, so $g = \alpha(h) = \alpha(1) = 1$.

To show θ is surjective, let $(h,k) \in H \times K$. Since β is onto, $k = \beta(g)$ for some $g \in G$. Since $\ker\beta = \operatorname{im}\alpha$, the general inverse image of k under β is $g\alpha(x)$ for $x \in H$. We want to find $x \in H$ such that $\alpha'(g\alpha(x)) = h$, so then $\theta(g\alpha(x)) = (h,k)$. Since α' is a homomorphism, the condition $\alpha'(g\alpha(x)) = h$ is equivalent to $\alpha'(g)x = h$, so *define* $x = \alpha'(g)^{-1}h$. Then

$$\theta(g\alpha(x)) = (\alpha'(g\alpha(x)), \beta(g\alpha(x))) = (h,k),$$

so θ is an isomorphism from G to $H \times K$.

Next, we want to check the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \times K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

commutes. In the first square

$$\begin{array}{ccc} H & \xrightarrow{\alpha} & G \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \theta} \\ H & \longrightarrow & H \times K \end{array}$$

taking $h \in H$ along the top and right has the effect $h \mapsto \alpha(h) \mapsto (\alpha'(\alpha(h)), \beta(\alpha(h))) = (h,1)$, which is also the result of taking h along the left and bottom. In the second square

$$\begin{array}{ccc} G & \xrightarrow{\beta} & K \\ \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}} \\ H \times K & \longrightarrow & K \end{array}$$

taking $g \in G$ along the top and right has the effect $g \mapsto \beta(g) \mapsto \beta(g)$, and going along the left and bottom leads to $g \mapsto (\alpha'(g), \beta(g)) \mapsto \beta(g)$. So the diagram commutes.

(2) $\Rightarrow$ (1): Suppose there is an isomorphism $\theta\colon G \to H \times K$ such that

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \times K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

commutes. For $g \in G$, $\theta(g) \in H \times K$ has second coordinate $\beta(g)$ from commutativity of the second square. Let $\alpha'(g)$ denote the first coordinate:

$$\theta(g) = (\alpha'(g), \beta(g)).$$

Then $\alpha'\colon G \to H$ is a function and θ is a homomorphism, so α' is a homomorphism. The commutativity of the first square implies $\theta(\alpha(h)) = (h, 1)$, so $(\alpha'(\alpha(h)), \beta(\alpha(h))) = (h, 1)$, so $\alpha'(\alpha(h)) = h$ for all $h \in H$. □

The proof shows that the homomorphisms α' in (1) and the isomorphisms θ in (2) are in bijection by the formula $\theta(g) = (\alpha'(g), \beta(g))$ for all $g \in G$.

Theorem 3.3. *Let $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$ be a short exact sequence. The following are equivalent:*

(1) *There is a homomorphism $\beta'\colon K \to G$ such that $\beta(\beta'(k)) = k$ for all $k \in K$.*
(2) *There is a homomorphism $\varphi\colon K \to \mathrm{Aut}(H)$ and an isomorphism $\theta\colon G \to H \rtimes_\varphi K$ such that the diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \Big\downarrow{\scriptstyle \mathrm{id}} & & \Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \rtimes_\varphi K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

commutes, where the bottom short exact sequence is the usual one for a semidirect product.

As with Theorem 3.2, the key part of (1) is that β' is a homomorphism. From surjectivity of β, there is a function $\beta'\colon K \to G$ such that $\beta(\beta'(k)) = k$ for all $k \in K$, for instance set $\beta'(k)$ for each k to be a solution[1] to $\beta(g) = k$. But usually this β' is not a *homomorphism*.

Proof. (1) $\Rightarrow$ (2): From the homomorphism β' we have to create an action φ of K on H by automorphisms and an isomorphism of G with $H \rtimes_\varphi K$. Using β', we can make K act on H using conjugation in G: for $k \in K$ and $h \in H$, $\beta'(k)\alpha(h)\beta'(k^{-1}) \in \ker\beta$ since

$$\beta(\beta'(k)\alpha(h)\beta'(k^{-1})) = \beta(\beta'(k))\beta(\alpha(h))\beta(\beta'(k^{-1})) = k \cdot 1 \cdot k^{-1} = 1.$$

Since $\ker\beta = \mathrm{im}\,\alpha$, we can write $\beta'(k)\alpha(h)\beta'(k^{-1}) = \alpha(h')$ for an $h' \in H$, and h' is unique since α is injective. This h' is determined by h and k. We write h' as $\varphi_k(h)$, so $\varphi_k(h)$ denotes the unique element of H such that

$$\beta'(k)\alpha(h)\beta'(k)^{-1} = \alpha(\varphi_k(h)), \tag{3.1}$$

where $\beta'(k^{-1}) = \beta'(k)^{-1}$ since β' is a homomorphism. Since $\varphi_k(h) \in H$, we get a function $\varphi_k\colon H \to H$. We will show $\varphi_k \in \mathrm{Aut}(H)$ and $k \mapsto \varphi_k$ is a homomorphism $K \to \mathrm{Aut}(H)$.

First, setting $k = 1$ in (3.1), $\alpha(h) = \alpha(\varphi_1(h))$, so $\varphi_1(h) = h$ for all $h \in H$. Thus $\varphi_1 = \mathrm{id}_H$. Next we check $\varphi_k\colon H \to H$ is a homomorphism for each $k \in K$. For h_1 and h_2 in H, $\varphi_k(h_1h_2)$ is characterized by the equation $\beta'(k)\alpha(h_1h_2)\beta'(k)^{-1} = \alpha(\varphi_k(h_1h_2))$. The left side is

$$\begin{aligned} \beta'(k)\alpha(h_1)\alpha(h_2)\beta'(k)^{-1} &= \beta'(k)\alpha(h_1)\beta'(k)^{-1}\beta'(k)\alpha(h_2)\beta'(k)^{-1} \\ &= \alpha(\varphi_k(h_1))\alpha(\varphi_k(h_2)) \\ &= \alpha(\varphi_k(h_1)\varphi_k(h_2)), \end{aligned}$$

so by injectivity of α we have $\varphi_k(h_1)\varphi_k(h_2) = \varphi_k(h_1h_2)$.

Next we show $\varphi_{k_1} \circ \varphi_{k_2} = \varphi_{k_1k_2}$. For $h \in H$, $\varphi_{k_1k_2}(h)$ is characterized by the equation

$$\beta'(k_1k_2)\alpha(h)\beta'(k_1k_2)^{-1} = \alpha(\varphi_{k_1k_2}(h)),$$

[1]Here we use the Axiom of Choice.

and the left side is

$$\begin{aligned}\beta'(k_1)\beta'(k_2)\alpha(h)\beta'(k_2)^{-1}\beta'(k_1)^{-1} &= \beta'(k_1)\alpha(\varphi_{k_2}(h))\beta'(k_1)^{-1} \quad \text{by (3.1)}\\ &= \alpha(\varphi_{k_1}(\varphi_{k_2}(h))),\end{aligned}$$

so $\varphi_{k_1}(\varphi_{k_2}(h)) = \varphi_{k_1k_2}(h)$, so $\varphi_{k_1} \circ \varphi_{k_2} = \varphi_{k_1k_2}$. In particular, $\varphi_k \circ \varphi_{k^{-1}} = \varphi_1$ and $\varphi_{k^{-1}} \circ \varphi_k = \varphi_1$, so $\varphi_k \in \mathrm{Aut}(H)$ and $k \mapsto \varphi_k$ is a homomorphism $K \to \mathrm{Aut}(H)$. We have proved that (3.1) provides an action of K on H by automorphisms, so we have the semidirect product $H \rtimes_\varphi K$.

To get an isomorphism $G \to H \rtimes_\varphi K$, it is easier to go in the other direction. Let $\gamma\colon H \rtimes_\varphi K \to G$ by

$$\gamma(h,k) = \alpha(h)\beta'(k).$$

To check γ is a homomorphism,

$$\begin{aligned}\gamma((h_1,k_1)(h_2,k_2)) &= \gamma(h_1\varphi_{k_1}(h_2), k_1k_2)\\ &= \alpha(h_1\varphi_{k_1}(h_2))\beta'(k_1k_2)\\ &= \alpha(h_1)\alpha(\varphi_{k_1}(h_2))\beta'(k_1)\beta'(k_2)\\ &= \alpha(h_1)(\beta'(k_1)\alpha(h_2)\beta'(k_1)^{-1})\beta'(k_1)\beta'(k_2) \quad \text{by (3.1)}\\ &= \alpha(h_1)\beta'(k_1)\alpha(h_2)\beta'(k_2)\\ &= \gamma(h_1,k_1)\gamma(h_2,k_2).\end{aligned}$$

To show γ is injective, if $\gamma(h,k) = 1$ then $\alpha(h)\beta'(k) = 1$. Applying β to both sides, $\beta(\alpha(h))\beta(\beta'(k)) = \beta(1) = 1$, so $k = 1$. Then $\alpha(h) \cdot 1 = 1$, so $h = 1$ since α is injective.

To show γ is surjective, pick $g \in G$. We want to find $h \in H$ and $k \in K$ such that $\alpha(h)\beta'(k) = g$. Applying β to both sides, $\beta(\alpha(h))\beta(\beta'(k)) = \beta(g)$, so $k = \beta(g)$. So we *define* $k := \beta(g)$ and then ask if there is $h \in H$ such that $\alpha(h) = g\beta'(k^{-1}) = g\beta'(\beta(g)^{-1})$. Since $\mathrm{im}\,\alpha = \ker\beta$, whether or not there is such an h is equivalent to checking $g\beta'(\beta(g)^{-1})) \in \ker\beta$:

$$\begin{aligned}\beta(g\beta'(\beta(g)^{-1})) &= \beta(g)\beta(\beta'(\beta(g)^{-1}))\\ &= \beta(g)\beta(g)^{-1}\\ &= 1.\end{aligned}$$

Thus $\gamma\colon H \rtimes_\varphi K \to G$ is an isomorphism. Let $\theta = \gamma^{-1}$ be the inverse isomorphism.

Finally, to show the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1\\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \rtimes_\varphi K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

commutes, it is equivalent to show the "flipped" diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1\\ & & \uparrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle \gamma} & & \uparrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \longrightarrow & H \rtimes_\varphi K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

commutes. For $h \in H$, going around the first square along the left and top has the effect $h \mapsto h \mapsto \alpha(h)$, and going around the other way has the effect $h \mapsto (h,1) \mapsto \gamma(h,1) =$

$\alpha(h)\beta'(1) = \alpha(h)$. In the second square, for $(h,k) \in H \rtimes_\varphi K$ going around the left and top has the effect $(h,k) \mapsto \beta(\gamma(h,k)) = \beta(\alpha(h))\beta(\beta'(k)) = k$, while going around the other way has the effect $(h,k) \mapsto k \mapsto k$.

(2) $\Rightarrow$ (1): In the proof that (1) $\Rightarrow$ (2), $\gamma(h,k) = \alpha(h)\beta'(k)$, so $\gamma(1,k) = \beta'(k)$. This *suggests* that when we have an isomorphism $\theta\colon G \to H \rtimes_\varphi K$ that we define $\beta'\colon K \to G$ by $\beta'(k) = \theta^{-1}(1,k)$. This is a homomorphism since $k \mapsto (1,k)$ is a homomorphism and θ^{-1} is a homomorphism. The composite $\beta(\beta'(k)) = \beta(\theta^{-1}(1,k))$ equals k from commutativity of the diagram

$$\begin{array}{ccc} G & \xrightarrow{\beta} & K \\ {\scriptstyle\theta^{-1}}\uparrow & & \uparrow{\scriptstyle\mathrm{id}} \\ H \rtimes_\varphi K & \longrightarrow & K. \end{array}$$

□

Definition 3.4. A short exact sequence $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$ is said to *split* if it fits the conditions of Theorem 3.3.

A split short exact sequence is one that essentially corresponds to the standard short exact sequence for a semidirect product. One nonsplit short exact sequence is (2.1).

Since a semidirect product is usually not a direct product, the first conditions in Theorems 3.2 and 3.3 are not equivalent: for a short exact sequence of groups $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$, if there is a homomorphism $\beta'\colon K \to G$ such that $\beta(\beta'(k)) = k$ for all k there need not be a homomorphism $\alpha'\colon G \to H$ such that $\alpha'(\alpha(h)) = h$ for all h. However, when G is abelian, (3.1) simplifies to $\alpha(h) = \alpha(\varphi_k(h))$ for all k and h, so $h = \varphi_k(h)$. Thus K acts trivially on H, so $H \rtimes_\varphi K = H \times K$. Therefore Theorems 3.2 and 3.3 provide three equivalent conditions on $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$ when G is *abelian*:

(1) There is a homomorphism $\alpha'\colon G \to H$ such that $\alpha'(\alpha(h)) = h$ for all $h \in H$.
(2) There is a homomorphism $\beta'\colon K \to G$ such that $\beta(\beta'(k)) = k$ for all $k \in K$.
(3) There is an isomorphism $\theta\colon G \to H \times K$ such that the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & {\scriptstyle\mathrm{id}}\downarrow & & {\scriptstyle\theta}\downarrow & & {\scriptstyle\mathrm{id}}\downarrow & & \\ 1 & \longrightarrow & H & \longrightarrow & H \times K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

commutes, where the bottom row is the short exact sequence for a direct product.

4. Equivalent Short Exact Sequences

We said in the introduction that every short exact sequence (1.1) is basically like a short exact sequence of type (1.3), and made the idea precise in terms of a commutative diagram (1.4) having both short exact sequences (1.1) and (1.3) appearing in it as the rows, and the columns being isomorphisms. This idea of two short exact sequences being basically alike can be applied more generally. Say $1 \longrightarrow H_1 \xrightarrow{\alpha_1} G_1 \xrightarrow{\beta_1} K_1 \longrightarrow 1$ and

$1 \longrightarrow H_2 \xrightarrow{\alpha_2} G_2 \xrightarrow{\beta_2} K_2 \longrightarrow 1$ are *equivalent* if they fit into a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H_1 & \xrightarrow{\alpha_1} & G_1 & \xrightarrow{\beta_1} & K_1 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H_2 & \xrightarrow{\alpha_2} & G_2 & \xrightarrow{\beta_2} & K_2 & \longrightarrow & 1 \end{array} \tag{4.1}$$

where the vertical maps are isomorphisms. In this terminology, (1.4) shows every short exact sequence is equivalent to a short exact sequence of type (1.3). When two short exact sequences are equivalent, the first groups both sit inside the second groups in the same way, and the third groups are homomorphic images of the second groups in the same way.

Here is a concrete example of equivalent short exact sequences:

$$1 \longrightarrow A_3 \longrightarrow S_3 \xrightarrow{\text{sgn}} \{\pm 1\} \longrightarrow 1 \tag{4.2}$$

and

$$0 \longrightarrow \mathbf{Z}/3\mathbf{Z} \longrightarrow \mathrm{Aff}(\mathbf{Z}/3\mathbf{Z}) \xrightarrow{\det} (\mathbf{Z}/3\mathbf{Z})^\times \longrightarrow 1, \tag{4.3}$$

where the first map in (4.2) is inclusion and the first map in (4.3) is $b \mapsto \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$. These are equivalent because there is a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A_3 & \longrightarrow & S_3 & \xrightarrow{\text{sgn}} & \{\pm 1\} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbf{Z}/3\mathbf{Z} & \longrightarrow & \mathrm{Aff}(\mathbf{Z}/3\mathbf{Z}) & \xrightarrow{\det} & (\mathbf{Z}/3\mathbf{Z})^\times & \longrightarrow & 1 \end{array}$$

where (4.2) and (4.3) are the rows and the vertical maps are all isomorphisms.

Theorem 3.2 gives us a condition for detecting when a short exact sequence $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$ is equivalent to the usual short exact sequence for $H \times K$ with the first and third vertical maps being the identities on H and K. Similarly, Theorem 3.3 tells us when $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$ is equivalent to the usual short exact sequence for some semidirect product $H \rtimes_\varphi K$ with the first and third vertical maps being the identities on H and K.

The notion of equivalent short exact sequences is an equivalence relation: any short exact sequence $1 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} K \longrightarrow 1$ is equivalent to itself from the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \\ & & \text{id}\downarrow & & \text{id}\downarrow & & \text{id}\downarrow & & \\ 1 & \longrightarrow & H & \xrightarrow{\alpha} & G & \xrightarrow{\beta} & K & \longrightarrow & 1 \end{array} \tag{4.4}$$

and using inverse isomorphisms in the vertical rows of (4.1) gives a commutative diagram where the two rows are interchanged, so the notion of equivalent short exact sequences is symmetric. For transitivity, we can combine two commutative diagrams

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H_1 & \xrightarrow{\alpha_1} & G_1 & \xrightarrow{\beta_1} & K_1 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H_2 & \xrightarrow{\alpha_2} & G_2 & \xrightarrow{\beta_2} & K_2 & \longrightarrow & 1 \end{array}$$

and

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H_2 & \xrightarrow{\alpha_2} & G_2 & \xrightarrow{\beta_2} & K_2 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H_3 & \xrightarrow{\alpha_3} & G_3 & \xrightarrow{\beta_3} & K_3 & \longrightarrow & 1 \end{array}$$

into the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H_1 & \xrightarrow{\alpha_1} & G_1 & \xrightarrow{\beta_1} & K_1 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H_2 & \xrightarrow{\alpha_2} & G_2 & \xrightarrow{\beta_2} & K_2 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H_3 & \xrightarrow{\alpha_3} & G_3 & \xrightarrow{\beta_3} & K_3 & \longrightarrow & 1 \end{array}$$

and then use the composite of the pairs of vertical isomorphisms to eliminate the middle row and get the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H_1 & \xrightarrow{\alpha_1} & G_1 & \xrightarrow{\beta_1} & K_1 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H_3 & \xrightarrow{\alpha_3} & G_3 & \xrightarrow{\beta_3} & K_3 & \longrightarrow & 1 \end{array}$$

with isomorphisms as the vertical maps.

Here is the analogue of homomorphisms for short exact sequences. A *morphism* from $1 \longrightarrow H_1 \xrightarrow{\alpha_1} G_1 \xrightarrow{\beta_1} K_1 \longrightarrow 1$ to $1 \longrightarrow H_2 \xrightarrow{\alpha_2} G_2 \xrightarrow{\beta_2} K_2 \longrightarrow 1$ is a commutative diagram (4.1) where the vertical maps are homomorphisms rather than isomorphisms. An example of a morphism of short exact sequences is (for $m > 1$)

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{SL}_2(\mathbf{Z}) & \longrightarrow & \mathrm{GL}_2(\mathbf{Z}) & \xrightarrow{\det} & \{\pm 1\} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{SL}_2(\mathbf{Z}/m\mathbf{Z}) & \longrightarrow & \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z}) & \xrightarrow{\det} & (\mathbf{Z}/m\mathbf{Z})^\times & \longrightarrow & 1, \end{array}$$

where the vertical maps are the natural mod m reduction maps. The identity morphism for a short exact sequence is (4.4). Our argument that equivalence of short exact sequences is transitive also shows how to compose two morphisms to get a third: compose vertical homomorphisms in the same positions in the two diagrams. What we called equivalence of two short exact sequences is the concept of isomorphism: a morphism of short exact sequences that admits an inverse morphism (one whose composite with the original morphism on both sides gives the identity morphism for the two short exact sequences).

CHAPTER 7

Extensions and Cohomology

A group G having a normal subgroup K can be "factored" into K and G/K. The study of extensions involves the inverse question: Given $K \lhd G$ and G/K, to what extent can one recapture G?

The Extension Problem

Definition. If K and Q are groups, then an ***extension*** of K by Q is a group G having a normal subgroup $K_1 \cong K$ with $G/K_1 \cong Q$.

As a mnemonic device, K denotes kernel and Q denotes quotient. We think of G as a "product" of K and Q.

EXAMPLE 7.1. Both $\mathbb{Z}_6$ and S_3 are extensions of $\mathbb{Z}_3$ by $\mathbb{Z}_2$. However, $\mathbb{Z}_6$ is an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_3$, but S_3 is not such an extension (for S_3 has no normal subgroup of order 2).

EXAMPLE 7.2. For any groups K and Q, the direct product $K \times Q$ is an extension of K by Q as well as an extension of Q by K.

The extension problem (formulated by O. Hölder) is to find all extensions of a given group K by a given group Q. We can better understand the Jordan–Hölder theorem in light of this problem. Let a group G have a composition series

$$G = K_0 \geq K_1 \geq \cdots \geq K_{n-1} \geq K_n = 1$$

and corresponding factor groups

$$K_0/K_1 = Q_1, \ldots, K_{n-2}/K_{n-1} = Q_{n-1}, K_{n-1}/K_n = Q_n.$$

Since $K_n = 1$, we have $K_{n-1} = Q_n$, but something more interesting happens at the next stage; $K_{n-2}/K_{n-1} = Q_{n-1}$, so that K_{n-2} is an extension of K_{n-1} by Q_{n-1}. If we could solve the extension problem, then we could recapture K_{n-2} from K_{n-1} and Q_{n-1}; that is, from Q_n and Q_{n-1}. Once we have K_{n-2}, we can attack K_{n-3} in a similar manner, for $K_{n-3}/K_{n-2} = Q_{n-2}$. Thus, a solution of the extension problem would allow us to recapture K_{n-3} from Q_n, Q_{n-1}, and Q_{n-2}. Climbing up the composition series to $K_0 = G$, we could recapture G from $Q_n, \ldots, Q_1$. The group G is thus a "product" of the Q_i, and the Jordan–Hölder theorem says that the simple groups Q_i in this "factorization" of G are uniquely determined by G. We could thus survey all finite groups if we knew all finite simple groups and if we could solve the extension problem. In particular, we could survey all finite solvable groups if we could solve the extension problem.

A solution of the extension problem consists of determining from K and Q all the groups G for which $G/K \cong Q$. But what does "determining" a group mean? We gave two answers to this question at the end of Chapter 1 when we considered "knowing" a group. One answer is that a multiplication table for a group G can be constructed; a second answer is that the isomorphism class of G can be characterized. In 1926, O. Schreier determined all extensions in the first sense (see Theorem 7.34). On the other hand, no solution is known in the second sense. For example, given K and Q, Schreier's solution does not allow us to compute the number of nonisomorphic extensions of K by Q (though it does give an upper bound).

Exercises

7.1. If K and Q are finite, then every extension G of K by Q has order $|K||Q|$. If G has a normal series with factor groups $Q_n, \ldots, Q_1$, then $|G| = \prod |Q_i|$.

7.2. (i) Show that A_4 is an extension of $\mathbf{V}$ by $\mathbb{Z}_3$.
(ii) Find all the extensions of $\mathbb{Z}_3$ by $\mathbf{V}$.

7.3. If p is prime, every nonabelian group of order p^3 is an extension of $\mathbb{Z}_p$ by $\mathbb{Z}_p \times \mathbb{Z}_p$. (*Hint.* Exercise 4.7.)

7.4. Give an example of an extension of K by Q that does not contain a subgroup isomorphic to Q.

7.5. If $(a, b) = 1$ and K and Q are abelian groups of orders a and b, respectively, then there is only one (to isomorphism) abelian extension of K by Q.

7.6. Which of the following properties, when enjoyed by both K and Q, is also enjoyed by every extension of K by Q? (i) finite; (ii) p-group; (iii) abelian; (iv) cyclic; (v) solvable; (vi) nilpotent; (vii) ACC; (viii) DCC; (ix) ***periodic*** (every element has finite order); (x) ***torsion-free*** (every element other than 1 has infinite order).

Automorphism Groups

The coming construction is essential for the discussion of the extension problem; it is also of intrinsic interest.

Definition. The ***automorphism group*** of a group G, denoted by $\mathrm{Aut}(G)$, is the set of all the automorphisms of G under the operation of composition.

It is easy to check that $\mathrm{Aut}(G)$ is a group; indeed, it is a subgroup of the symmetric group S_G.

Definition. An automorphism φ of G is ***inner*** if it is conjugation by some element of G; otherwise, it is ***outer***. Denote the set of all inner automorphisms of G by $\mathrm{Inn}(G)$.

Theorem 7.1.

(i) **(*N/C* Lemma).** *If* $H \leq G$, *then* $C_G(H) \lhd N_G(H)$ *and* $N_G(H)/C_G(H)$ *can be imbedded in* $\mathrm{Aut}(H)$.
(ii) $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ *and* $G/Z(G) \cong \mathrm{Inn}(G)$.

Proof. (i) If $a \in G$, let γ_a denote conjugation by a. Define $\varphi\colon N_G(H) \to \mathrm{Aut}(H)$ by $a \mapsto \gamma_a|H$ (note that $\gamma_a|H \in \mathrm{Aut}(H)$ because $a \in N_G(H)$); φ is easily seen to be a homomorphism. The following statements are equivalent: $a \in \ker \varphi$; $\gamma_a|H$ is the identity on H; $aha^{-1} = h$ for all $h \in H$; $a \in C_G(H)$. By the first isomorphism theorem, $C_G(H) \lhd N_G(H)$ and $N_G(H)/C_G(H) \cong \mathrm{im}\ \varphi \leq \mathrm{Aut}(H)$.

(ii) If $H = G$, then $N_G(G) = G$, $C_G(G) = Z(G)$, and $\mathrm{im}\ \varphi = \mathrm{Inn}(G)$. Therefore, $G/Z(G) \cong \mathrm{Inn}(G)$ is a special case of the isomorphism just established.

To see that $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$, take $\gamma_a \in \mathrm{Inn}(G)$ and $\varphi \in \mathrm{Aut}(G)$. Then $\varphi\gamma_a\varphi^{-1} = \gamma_{\varphi a} \in \mathrm{Inn}(G)$, as the reader can check. ■

Definition. The group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the ***outer automorphism group*** of G.

EXAMPLE 7.3. $\mathrm{Aut}(\mathbf{V}) \cong S_3 \cong \mathrm{Aut}(S_3)$.

The 4-group $\mathbf{V}$ consists of 3 involutions and 1, and so every $\varphi \in \mathrm{Aut}(\mathbf{V})$ permutes the 3 involutions: if $X = \mathbf{V} - \{1\}$, then the map $\varphi \mapsto \varphi|X$ is a homomorphism $\mathrm{Aut}(\mathbf{V}) \to S_X \cong S_3$. The reader can painlessly check that this map is an isomorphism.

The symmetric group S_3 consists of 3 involutions, 2 elements of order 3, and the identity, and every $\varphi \in \mathrm{Aut}(S_3)$ must permute the involutions: if $Y = \{(1\ 2), (1\ 3), (2\ 3)\}$, then the map $\varphi \mapsto \varphi|Y$ is a homomorphism $\mathrm{Aut}(S_3) \to S_Y \cong S_3$; this map is easily seen to be an isomorphism.

We conclude that nonisomorphic groups can have isomorphic automorphism groups.

EXAMPLE 7.4. If G is an elementary abelian group of order p^n, then $\mathrm{Aut}(G) \cong \mathrm{GL}(n, p)$.

This follows from Exercise 2.78: G is a vector space over $\mathbb{Z}_p$ and every automorphism is a nonsingular linear transformation.

EXAMPLE 7.5. $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

Let $G = \langle x \rangle$ be infinite cyclic. If $\varphi \in \mathrm{Aut}(G)$, then $\varphi(x)$ must be a generator of G. Since the only generators of G are x and x^{-1}, there are only two automorphisms of G, and so $\mathrm{Aut}(\mathbb{Z}) \cong \mathrm{Aut}(G) \cong \mathbb{Z}_2$. Thus, an infinite group can have a finite automorphism group.

EXAMPLE 7.6. $\mathrm{Aut}(G) = 1$ if and only if $|G| \leq 2$.

It is clear that $|G| \leq 2$ implies $\mathrm{Aut}(G) = 1$. Conversely, assume that $\mathrm{Aut}(G) = 1$. If $a \in G$, then $\gamma_a = 1$ if and only if $a \in Z(G)$; it follows that G is abelian. The function $a \mapsto a^{-1}$ is now an automorphism of G, so that G has exponent 2; that is, G is a vector space over $\mathbb{Z}_2$. If $|G| > 2$, then $\dim G \geq 2$ and there exists a nonsingular linear transformation $\varphi: G \to G$ other than 1.

Recall that if R is a ring, then $U(R)$ denotes its group of units:

$$U(R) = \{r \in R: \text{there is } s \in R \text{ with } sr = 1 = rs\}.$$

Lemma 7.2. *If G is a cyclic group of order n, then* $\mathrm{Aut}(G) \cong U(\mathbb{Z}_n)$.

Proof. Let $G = \langle a \rangle$. If $\varphi \in \mathrm{Aut}(G)$, then $\varphi(a) = a^k$ for some k; moreover, a^k must be a generator of G, so that $(k, n) = 1$, by Exercise 2.20, and $[k] \in U(\mathbb{Z}_n)$. It is routine to show that $\Theta: \mathrm{Aut}(G) \to U(\mathbb{Z}_n)$, defined by $\Theta(\varphi) = [k]$, is an isomorphism. ■

Theorem 7.3.

(i) $\mathrm{Aut}(\mathbb{Z}_2) = 1$; $\mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$; *if* $m \geq 3$, *then* $\mathrm{Aut}(\mathbb{Z}_{2^m}) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$.
(ii) *If p is an odd prime, then* $\mathrm{Aut}(\mathbb{Z}_{p^m}) \cong \mathbb{Z}_l$, *where* $l = (p-1)p^{m-1}$.
(iii) *If* $n = p_1^{e_1} \dots p_t^{e_t}$, *where the p_i are distinct primes and the $e_i > 0$, then* $\mathrm{Aut}(\mathbb{Z}_n) \cong \prod_i \mathrm{Aut}(\mathbb{Z}_{q_i})$, *where* $q_i = p_i^{e_i}$.

Proof. (i) $U(\mathbb{Z}_2) = 1$ and $U(\mathbb{Z}_4) = \{[1], [-1]\} \cong \mathbb{Z}_2$. If $m \geq 3$, then the result is Theorem 5.44.

(ii) This is Theorem 6.7.

(iii) If a ring $R = R_1 \times \cdots \times R_t$ is a direct product of rings (addition and multiplication are coordinatewise), then it is easy to see that $U(R)$ is the direct

product of groups $U(R_1) \times \cdots \times U(R_t)$; moreover, the primary decomposition of the cyclic group $\mathbb{Z}_n = \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_t}$ is also a decomposition of $\mathbb{Z}_n$ as a direct product of rings. ■

Theorem 7.1 suggests the following class of groups:

Definition. A group G is ***complete*** if it is centerless and every automorphism of G is inner.

It follows from Theorem 7.1(ii) that $\mathrm{Aut}(G) \cong G$ for every complete group. We are now going to see that almost every symmetric group is complete.

Lemma 7.4. *An automorphism φ of S_n preserves transpositions ($\varphi(\tau)$ is a transposition whenever τ is) if and only if φ is inner.*

Proof. If φ is inner, then it preserves the cycle structure of every permutation, by Theorem 3.5.

We prove, by induction on $t \geq 2$, that there exist conjugations $\gamma_2, \ldots, \gamma_t$ such that $\gamma_t^{-1} \ldots \gamma_2^{-1}\varphi$ fixes $(1\ 2), \ldots, (1\ t)$. If $\pi \in S_n$, we will denote $\varphi(\pi)$ by π^φ in this proof. By hypothesis, $(1\ 2)^\varphi = (i\ j)$ for some i, j; define γ_2 to be conjugation by $(1\ i)(2\ j)$ (if $i = 1$ or $j = 2$, then interpret $(1\ i)$ or $(2\ j)$ as the identity). By Lemma 3.4, the quick way of computing conjugates in S_n, we see that $(1\ 2)^\varphi = (1\ 2)^{\gamma_2}$, and so $\gamma_2^{-1}\varphi$ fixes $(1\ 2)$.

Let $\gamma_2, \ldots, \gamma_t$ be given by the inductive hypothesis, so that $\psi = \gamma_t^{-1} \ldots \gamma_2^{-1}\varphi$ fixes $(1\ 2), \ldots, (1\ t)$. Since ψ preserves transpositions, $(1\ t+1)^\psi = (l\ k)$. Now $(1\ 2)$ and $(l\ k)$ cannot be disjoint, lest $[(1\ 2)(1\ t+1)]^\psi = (1\ 2)^\psi(1\ t+1)^\psi = (1\ 2)(l\ k)$ have order 2, while $(1\ 2)(1\ t+1)$ has order 3. Thus, $(1\ t+1)^\psi = (1\ k)$ or $(1\ t+1)^\psi = (2\ k)$. If $k \leq t$, then $(1\ t+1)^\psi \in \langle (1\ 2), \ldots, (1\ t) \rangle$, and hence it is fixed by ψ; this contradicts ψ being injective, for either $(1\ t+1)^\psi = (1\ k) = (1\ k)^\psi$ or $(1\ t+1)^\psi = (2\ k) = (2\ k)^\psi$. Hence, $k \geq t+1$. Define γ_{t+1} to be conjugation by $(k\ t+1)$. Now γ_{t+1} fixes $(1\ 2), \ldots, (1\ t)$ and $(1\ t+1)^{\gamma_{t+1}} = (1\ t+1)^\psi$, so that $\gamma_{t+1}^{-1} \cdots \gamma_2^{-1}\varphi$ fixes $(1\ 2), \ldots, (1\ t+1)$ and the induction is complete. It follows that $\gamma_n^{-1} \cdots \gamma_2^{-1}\varphi$ fixes $(1\ 2), \ldots, (1\ n)$. But these transpositions generate S_n, by Exercise 2.9(i), and so $\gamma_n^{-1} \ldots \gamma_2^{-1}\varphi$ is the identity. Therefore, $\varphi = \gamma_2 \cdots \gamma_n \in \mathrm{Inn}(S_n)$. ■

Theorem 7.5. *If $n \neq 2$ or $n \neq 6$, then S_n is complete.*

Remark. $S_2 \cong \mathbb{Z}_2$ is not complete because it has a center; we shall see in Theorem 7.9 that S_6 is not complete.

Proof. Let T_k denote the conjugacy class in S_n consisting of all products of k disjoint transpositions. By Exercise 1.16, a permutation in S_n is an involution if and only if it lies in some T_k. It follows that if $\theta \in \mathrm{Aut}(S_n)$, then $\theta(T_1) = T_k$

for some k. We shall show that if $n \neq 6$, then $|T_k| \neq |T_1|$ for $k \neq 1$. Assuming this, then $\theta(T_1) = T_1$, and Lemma 7.4 completes the proof.

Now $|T_1| = n(n-1)/2$. To count T_k, observe first that there are

$$\tfrac{1}{2}n(n-1) \times \tfrac{1}{2}(n-2)(n-3) \times \cdots \times \tfrac{1}{2}(n-2k+2)(n-2k+1)$$

k-tuples of disjoint transpositions. Since disjoint transpositions commute and there are $k!$ orderings obtained from any k-tuple, we have

$$|T_k| = n(n-1)(n-2)\cdots(n-2k+1)/k!2^k.$$

The question whether $|T_1| = |T_k|$ leads to the question whether there is some $k > 1$ such that

$$(*) \qquad (n-2)(n-3)\cdots(n-2k+1) = k!2^{k-1}.$$

Since the right side of $(*)$ is positive, we must have $n \geq 2k$. Therefore, for fixed n,

$$\text{left side} \geq (2k-2)(2k-3)\cdots(2k-2k+1) = (2k-2)!.$$

An easy induction shows that if $k \geq 4$, then $(2k-2)! > k!2^{k-1}$, and so $(*)$ can hold only if $k = 2$ or $k = 3$. When $k = 2$, the right side is 4, and it easy to see that equality never holds; we may assume, therefore, that $k = 3$. Since $n \geq 2k$, we must have $n \geq 6$. If $n > 6$, then the left side of $(*) \geq 5 \times 4 \times 3 \times 2 = 120$, while the right side is 24. We have shown that if $n \neq 6$, then $|T_1| \neq |T_k|$ for all $k > 1$, as desired. ■

Corollary 7.6. *If θ is an outer automorphism of S_6, and if $\tau \in S_6$ is a transposition, then $\theta(\tau)$ is a product of three disjoint transpositions.*

Proof. If $n = 6$, then we saw in the proof of the theorem that $(*)$ does not hold if $k \neq 3$. (When $k = 3$, both sides of $(*)$ equal 24.) ■

Corollary 7.7. *If $n \neq 2$ or $n \neq 6$, then* $\mathrm{Aut}(S_n) \cong S_n$.

Proof. If G is complete, then $\mathrm{Aut}(G) \cong G$. ■

We now show that S_6 is a genuine exception. Recall that a subgroup $K \leq S_X$ is *transitive* if, for every pair $x, y \in X$, there exists $\sigma \in K$ with $\sigma(x) = y$. In Theorem 3.14, we saw that if $H \leq G$, then the family X of all left cosets of H is a G-set (where ρ_a: $gH \mapsto agH$ for each $a \in G$); indeed, X is a transitive G-set: given gH and $g'H$, then $\rho_a(gH) = g'H$, where $a = g'g^{-1}$.

Lemma 7.8. *There exists a transitive subgroup $K \leq S_6$ of order* 120 *which contains no transpositions.*

Proof. If σ is a 5-cycle, then $P = \langle\sigma\rangle$ is a Sylow 5-subgroup of S_5. The Sylow theorem says that if r is the number of conjugates of P, then $r \equiv 1 \bmod 5$ and r is a divisor of 120; it follows easily that $r = 6$. The representation of S_5 on

X, the set of all left cosets of $N = N_{S_5}(P)$, is a homomorphism $\rho: S_5 \to S_X \cong S_6$. Now X is a transitive S_5-set, by Exercise 4.11, and so $|\ker \rho| \leq |S_5|/r = |S_5|/6 = 20$, by Exercise 3.44(iii). Since the only normal subgroups of S_5 are S_5, A_5, and 1, it follows that $\ker \rho = 1$ and ρ is an injection. Therefore, $\operatorname{im} \rho \cong S_5$ is a transitive subgroup of S_X of order 120.

For notational convenience, let us write $K \leq S_6$ instead of $\operatorname{im} \rho \leq S_X$. Now K contains an element α of order 5 which must be a 5-cycle; say, $\alpha = (1\ 2\ 3\ 4\ 5)$. If K contains a transposition $(i\ j)$, then transitivity of K provides $\beta \in K$ with $\beta(j) = 6$, and so $\beta(i\ j)\beta^{-1} = (\beta i\ \beta j) = (l\ 6)$ for some $l \neq 6$ (of course, $l = \beta i$). Conjugating $(l\ 6) \in K$ by the powers of α shows that K contains (16), (2 6), (3 6), (4 6), and (5 6). But these transpositions generate S_6, by Exercise 2.9(i), and this contradicts K ($\cong S_5$) being a proper subgroup of S_6. ■

The "obvious" copy of S_5 in S_6 consists of all the permutations fixing 6; plainly, it is not transitive, and it does contain transpositions.

Theorem 7.9 (Hölder, 1895). *There exists an outer automorphism of* S_6.

Proof. Let K be a transitive subgroup of S_6 of order 120, and let Y be the family of its left cosets: $Y = \{\alpha_1 K, \ldots, \alpha_6 K\}$. If $\theta: S_6 \to S_Y$ is the representation of S_6 on the left cosets of K, then $\ker \theta \leq K$ is a normal subgroup of S_6. But A_6 is the only proper normal subgroup of S_6, so that $\ker \theta = 1$ and θ is an injection. Since S_6 is finite, θ must be a bijection, and so $\theta \in \operatorname{Aut}(S_6)$, for $S_Y \cong S_6$. Were θ inner, then it would preserve the cycle structure of every permutation in S_6. In particular, $\theta_{(12)}$, defined by $\theta_{(12)}: \alpha_i K \mapsto (1\ 2)\alpha_i K$ for all i, is a transposition, and hence θ fixes $\alpha_i K$ for four different i. But if $\theta_{(12)}$ fixes even one left coset, say $\alpha_i K = (1\ 2)\alpha_i K$, then $\alpha_i^{-1}(1\ 2)\alpha_i$ is a transposition in K. This contradiction shows that θ is an outer automorphism. ■

Theorem 7.10. $\operatorname{Aut}(S_6)/\operatorname{Inn}(S_6) \cong \mathbb{Z}_2$, and so $|\operatorname{Aut}(S_6)| = 1440$.

Proof. Let T_1 be the class of all transpositions in S_6, and let T_3 be the class of all products of 3 disjoint transpositions. If θ and ψ are outer automorphisms of S_6, then both interchange T_1 and T_3, by Corollary 7.6, and so $\theta^{-1}\psi(T_1) = T_1$. Therefore, $\theta^{-1}\psi \in \operatorname{Inn}(S_6)$, by Lemma 7.4, and $\operatorname{Aut}(S_6)/\operatorname{Inn}(S_6)$ has order 2. ■

This last theorem shows that there is essentially only one outer automorphism θ of S_6; given an outer automorphism θ, then every other such has the form $\gamma\theta$ for some inner automorphism γ. It follows that S_6 has exactly 720 outer automorphisms, for they comprise the other coset of $\operatorname{Inn}(S_6)$ in $\operatorname{Aut}(S_6)$.

Definition. A ***syntheme***[1] is a product of 3 disjoint transpositions. A ***pentad*** is a family of 5 synthemes, no two of which have a common transposition.

If two synthemes have a common transposition, say, $(a\ b)(c\ d)(e\ f)$ and $(a\ b)(c\ e)(d\ f)$, then they commute. It is easy to see that the converse holds: two commuting synthemes share a transposition.

Lemma 7.11. *S_6 contains exactly 6 pentads. They are*:

(12)(34)(56), (13)(25)(46), (14)(26)(35), (15)(24)(36), (16)(23)(45);

(12)(34)(56), (13)(26)(45), (14)(25)(36), (15)(23)(46), (16)(24)(35);

(12)(35)(46), (13)(24)(56), (14)(25)(36), (15)(26)(34), (16)(23)(45);

(12)(35)(46), (13)(26)(45), (14)(23)(56), (15)(24)(36), (16)(25)(34);

(12)(36)(45), (13)(24)(56), (14)(26)(35), (15)(23)(46), (16)(25)(34);

(12)(36)(45), (13)(25)(46), (14)(23)(56), (15)(26)(34), (16)(24)(35).

Proof. There are exactly 15 synthemes, and each lies in at most two pentads. There are thus at most 6 pentads, for $2 \times 15 = 30 = 6 \times 5$; there are exactly 6 pentads, for they are displayed above. ■

Theorem 7.12. *If $\{\sigma_2, \ldots, \sigma_6\}$ is a pentad in some ordering, then there is a unique outer automorphism θ of S_6 with θ: $(1\ i) \mapsto \sigma_i$ for $i = 2, 3, 4, 5, 6$. Moreover, every outer automorphism of S_6 has this form.*

Proof. Let $X = \{(1\ 2), (1\ 3), (1\ 4), (1\ 5), (1\ 6)\}$. If θ is an outer automorphism of S_6, then Corollary 7.6 shows that each $\theta((1\ i))$ is a syntheme. Since $(1\ i)$ and $(1\ j)$ do not commute for $i \neq j$, it follows that $\theta((1\ i))$ and $\theta((1\ j))$ do not commute; hence, $\theta(X)$ is a pentad. Let us count the number of possible functions from X to pentads arising from outer automorphisms. Given an outer automorphism θ, there are 6 choices of pentad for $\theta(X)$; given such a pentad P, there are $5! = 120$ bijections $X \to P$. Hence, there are at most 720 bijections from X to pentads which can possibly arise as restrictions of outer automorphisms. But there are exactly 720 outer automorphisms, by Theorem 7.10, and no two of them can restrict to the same bijection because X generates S_6. The statements of the theorem follow. ■

Since every element in S_6 is a product of transpositions, the information in the theorem allows one to evaluate $\theta(\beta)$ for every $\beta \in S_6$.

Corollary 7.13. *There is an outer automorphism of S_6 which has order 2.*

[1] A *syntheme* is a partition of a set X into subsets P_i with $|P_i| = |P_j|$ for all i, j (this term is due to J.J. Sylvester).

Proof. Define[2] $\psi \in \mathrm{Aut}(S_6)$ by

$$(1\ 2) \mapsto (1\ 5)(2\ 3)(4\ 6),$$
$$(1\ 3) \mapsto (1\ 4)(2\ 6)(3\ 5),$$
$$(1\ 4) \mapsto (1\ 3)(2\ 4)(5\ 6),$$
$$(1\ 5) \mapsto (1\ 2)(3\ 6)(4\ 5),$$
$$(1\ 6) \mapsto (1\ 6)(2\ 5)(3\ 4).$$

A routine but long calcuation shows that $\psi^2 = 1$. ■

Here is another source of (possibly infinite) complete groups.

Theorem 7.14. *If G is a nonabelian simple group, then* $\mathrm{Aut}(G)$ *is complete.*

Proof. Let $I = \mathrm{Inn}(G) \lhd \mathrm{Aut}(G) = A$. Now $Z(G) = 1$, because G is simple and nonabelian, and so Theorem 7.1 gives $I \cong G$. Now $Z(A) \leq C_A(I) = \{\varphi \in A: \varphi\gamma_g = \gamma_g\varphi \text{ for all } g \in G\}$. We claim that $C_A(I) = 1$; it will then follow that A is centerless. If $\varphi\gamma_g = \gamma_g\varphi$ for all $g \in G$, then $\gamma_g = \varphi\gamma_g\varphi^{-1} = \gamma_{\varphi(g)}$. Therefore, $\varphi(g)g^{-1} \in Z(G) = 1$ for all $g \in G$, and so $\varphi = 1$.

It remains to show that every $\sigma \in \mathrm{Aut}(A)$ is inner. Now $\sigma(I) \lhd A$, because $I \lhd A$, and so $I \cap \sigma(I) \lhd \sigma(I)$. But $\sigma(I) \cong I \cong G$ is simple, so that either $I \cap \sigma(I) = 1$ or $I \cap \sigma(I) = \sigma(I)$. Since both I and $\sigma(I)$ are normal, $[I, \sigma(I)] \leq I \cap \sigma(I)$. In the first case, we have $[I, \sigma(I)] = 1$; that is, $\sigma(I) \leq C_A(I) = 1$, and this contradicts $\sigma(I) \cong I$. Hence, $I \cap \sigma(I) = \sigma(I)$, and so $\sigma(I) \leq I$. This inclusion holds for every $\sigma \in \mathrm{Aut}(A)$; in particular, $\sigma^{-1}(I) \leq I$, and so $\sigma(I) = I$ for every $\sigma \in \mathrm{Aut}(A)$. If $g \in G$, then $\gamma_g \in I$; there is thus $\alpha(g) \in G$ with

$$\sigma(\gamma_g) = \gamma_{\alpha(g)}.$$

The reader may check easily that the function $\alpha: G \to G$ is a bijection. We now show that α is an automorphism of G; that is, $\alpha \in A$. If $g, h \in G$, then $\sigma(\gamma_g\gamma_h) = \sigma(\gamma_{gh}) = \gamma_{\alpha(gh)}$. On the other hand, $\sigma(\gamma_g\gamma_h) = \sigma(\gamma_g)\sigma(\gamma_h) = \gamma_{\alpha(g)}\gamma_{\alpha(h)} = \gamma_{\alpha(g)\alpha(h)}$; hence $\alpha(gh) = \alpha(g)\alpha(h)$.

We claim that $\sigma = \Gamma_\alpha$, conjugation by α. To this end, define $\tau = \sigma \circ \Gamma_\alpha^{-1}$. Observe, for all $h \in G$, that

$$\begin{aligned}\tau(\gamma_h) &= \sigma\Gamma_\alpha^{-1}(\gamma_h) = \sigma(\alpha^{-1}\gamma_h\alpha)\\ &= \sigma(\gamma_{\alpha^{-1}(h)})\\ &= \gamma_{\alpha\alpha^{-1}(h)} = \gamma_h.\end{aligned}$$

[2] In Lam, T.Y., and Leep, D.B., Combinatorial structure on the automorphism group of S_6, *Expo. Math.* (1993), it is shown that the order of any outer automorphism φ of S_6 is either 2, 4, 8, or 10, and they show how to determine the order of φ when it is given, as in Theorem 7.12, in terms of its values on $(1\ i)$, for $2 \leq i \leq 6$.

Thus, τ fixes everything in I. If $\beta \in A$, then for every $g \in G$,

$$\begin{aligned} \beta\gamma_g\beta^{-1} &= \tau(\beta\gamma_g\beta^{-1}) \qquad \text{(because } \beta\gamma_g\beta^{-1} \in I \text{ and } \tau \text{ fixes } I\text{)} \\ &= \tau(\beta)\gamma_g\tau(\beta)^{-1} \quad \text{(because } \tau \text{ fixes } I\text{).} \end{aligned}$$

Hence $\tau(\beta)\beta^{-1} \in C_A(I) = 1$, and $\tau(\beta) = \beta$. Therefore, $\tau = 1$, $\sigma = \Gamma_\alpha$, and A is complete. ■

It follows, for every nonabelian simple group G, that $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathrm{Aut}(G))$. There is a beautiful theorem of Wielandt (1939) with a similar conclusion. We know, by Theorem 7.1, that every centerless group G can be imbedded in $\mathrm{Aut}(G)$. Moreover, $\mathrm{Aut}(G)$ is also centerless, and so it can be imbedded in its automorphism group $\mathrm{Aut}(\mathrm{Aut}(G))$. This process may thus be iterated to give the ***automorphism tower*** of G:

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

Wielandt proved, for every finite centerless group G, that this tower is constant from some point on. Since the last term of an automorphism tower is a complete group, it follows that every finite centerless group can be imbedded in a complete group. Of course, there is an easier proof of a much stronger fact: Cayley's theorem imbeds a finite group in some S_n with $n > 6$, and Theorem 7.5 applies to show that S_n is complete.

The automorphism tower of an infinite centerless group need not stop after a finite number of steps, but a transfinite automorphism tower (indexed by ordinals) can be defined (taking unions at limit ordinals). S. Thomas (1985) proved, for every centerless group, that this automorphism tower eventually stops. As in the finite case, the last term of an automorphism tower is complete, and so every centerless group can be imbedded in a complete group. It is shown, in Exercise 11.56, that every group can be imbedded in a centerless group, and so it follows that every group can be imbedded in a complete group.

Theorem 7.15. *If $K \lhd G$ and K is complete, then K is a direct factor of G; that is, there is a normal subgroup Q of G with $G = K \times Q$.*

Proof. Define $Q = C_G(K) = \{g \in G: gk = kg \text{ for all } k \in K\}$. Now $K \cap Q \leq Z(K) = 1$, and so $K \cap Q = 1$. To see that $G = KQ$, take $g \in G$. Now $\gamma_g(K) = K$, because $K \lhd G$, and so $\gamma_g|K \in \mathrm{Aut}(K) = \mathrm{Inn}(K)$. There is thus $k \in K$ with $gxg^{-1} = kxk^{-1}$ for all $x \in K$. Hence $k^{-1}g \in \bigcap_{x \in K} C_G(x) = C_G(K) = Q$, and so $g = k(k^{-1}g) \in KQ$. Finally, $Q \lhd G$, for $gQg^{-1} = k(k^{-1}g)Q(k^{-1}g)^{-1}k^{-1} = kQk^{-1}$ (because $k^{-1}g \in Q$), and $kQk^{-1} = Q$ (because every element of Q commutes with k). Therefore, $G = K \times Q$. ■

The converse of Theorem 7.15 is true, and we introduce a construction in order to prove it. Recall that if $a \in K$, then $L_a\colon K \to K$ denotes left translation

by a; that is, $L_a(x) = ax$ for all $a \in K$. As in the Cayley theorem (Theorem 3.12), K is isomorphic to $K^l = \{L_a: a \in K\}$, which is a subgroup of S_K. Similarly, if $R_a: K \to K$ denotes right translation by a, that is, $R_a: x \mapsto xa^{-1}$, then $K^r = \{R_a: a \in K\}$ is also a subgroup of S_K isomorphic to K.

Definition. The ***holomorph*** of a group K, denoted by $\mathrm{Hol}(K)$, is the subgroup of S_K generated by K^l and $\mathrm{Aut}(K)$.

Notice, for all $a \in K$, that $R_a = L_{a^{-1}}\gamma_a$, so that $K^r \leq \mathrm{Hol}(K)$; indeed, it is easy to see that $\mathrm{Hol}(K) = \langle K^r, \mathrm{Aut}(K)\rangle$.

Lemma 7.16. *Let K be a group.*

(i) $K^l \lhd \mathrm{Hol}(K)$, $K^l \mathrm{Aut}(K) = \mathrm{Hol}(K)$, *and* $K^l \cap \mathrm{Aut}(K) = 1$.
(ii) $\mathrm{Hol}(K)/K^l \cong \mathrm{Aut}(K)$.
(iii) $C_{\mathrm{Hol}(K)}(K^l) = K^r$.

Proof. (i) It is easy to see that $\varphi L_a \varphi^{-1} = L_{\varphi(a)}$, and that it lies in K^l for every $a \in K$ and $\varphi \in \mathrm{Aut}(K)$; since $\mathrm{Hol}(K) = \langle K^l, \mathrm{Aut}(K)\rangle$, it follows that $K^l \lhd \mathrm{Hol}(K)$ and that $\mathrm{Hol}(K) = K^l \mathrm{Aut}(K)$. If $a \in K$, then $L_a(1) = a$; therefore, $L_a \in \mathrm{Aut}(K)$ if and only if $a = 1$; that is, $K^l \cap \mathrm{Aut}(K) = 1$.

(ii) $\mathrm{Hol}(K)/K^l = K^l \mathrm{Aut}(K)/K^l \cong \mathrm{Aut}(K)/(K^l \cap \mathrm{Aut}(K)) \cong \mathrm{Aut}(K)$.

(iii) If $a, b, x \in K$, then $L_a R_b(x) = a(xb^{-1})$ and $R_b L_a(x) = (ax)b^{-1}$, so that associativity gives $K^r \leq C_{\mathrm{Hol}(K)}(K^l)$. For the reverse inclusion, assume that $\eta \in \mathrm{Hol}(K)$ satisfies $\eta L_a = L_a \eta$ for all $a \in K$. Now $\eta = L_b \varphi$ for some $b \in K$ and $\varphi \in \mathrm{Aut}(K)$. If $x \in K$, then $\eta L_a(x) = L_b \varphi L_a(x) = b\varphi(a)\varphi(x)$ and $L_a \eta(x) = L_a L_b \varphi(x) = ab\varphi(x)$. Hence, $b\varphi(a) = ab$ for all $a \in K$; that is, $\varphi = \gamma_{b^{-1}}$. It follows that $\eta(x) = L_b \varphi(x) = b(b^{-1}xb) = xb$, and so $\eta = R_{b^{-1}} \in K^r$, as desired. ■

Here is the converse of Theorem 7.15.

Theorem 7.17. *If a group K is a direct factor whenever it is (isomorphic to) a normal subgroup of a group, then K is complete.*

Proof. We identify K with the subgroup $K^l \leq \mathrm{Hol}(K)$. Since K^l is normal, the hypothesis gives a subgroup B with $\mathrm{Hol}(K) = K^l \times B$. Now $B \leq C_{\mathrm{Hol}(K)}(K^l) = K^r$, because every element of B commutes with each element of K^l. It follows that if $\varphi \in \mathrm{Aut}(K) \leq \mathrm{Hol}(K)$, then $\varphi = L_a R_b$ for some $a, b \in K$. Hence, $\varphi(x) = axb^{-1}$ for all $x \in K$. But now $axyb^{-1} = \varphi(x)\varphi(y) = axb^{-1}ayb^{-1}$, so that $1 = b^{-1}a$; therefore, $\varphi = \gamma_a \in \mathrm{Inn}(K)$.

Since $\mathrm{Hol}(K) = K^l \times B$ and $B \leq K^r \leq \mathrm{Hol}(K)$, Exercise 7.17 below shows that $K^r = B \times (K^r \cap K^l)$. If $\varphi \in K^l \cap K^r$, then $\varphi = L_a = R_b$, for $a, b \in K$. For all $c \in K$, $L_a(c) = R_b(c)$ gives $ac = cb^{-1}$; if $c = 1$, then $a = b^{-1}$, from which it follows that $a \in Z(K)$. Therefore, $K^r \cap K^l = Z(K)$ and $K \cong B \times Z(K)$. If $1 \neq$

$\varphi \in \mathrm{Aut}(Z(K))$, then it is easy to see that $\tilde{\varphi}: B \times Z(K) \to B \times Z(K)$, defined by $(b, z) \mapsto (b, \varphi z)$, is an automorphism of K; $\tilde{\varphi}$ must be outer, for conjugation by $(\beta, \zeta) \in B \times Z(K) \cong K$ sends (b, z) into $(\beta, \zeta)(b, z)(\beta^{-1}, \zeta^{-1}) = (\beta b \beta^{-1}, z)$. But K has no outer automorphisms, so that $\mathrm{Aut}(Z(K)) = 1$ and, by Example 7.6, $|Z(K)| \leq 2$. If $Z(K) \cong \mathbb{Z}_2$, then it is isomorphic to a normal subgroup N of $\mathbb{Z}_4$ which is not a direct factor. But K is isomorphic to the normal subgroup $B \times N$ of $B \times \mathbb{Z}_4$ which is not a direct factor, contradicting the hypothesis. Therefore, $Z(K) = 1$ and K is complete. ■

The holomorph allows one to extend commutator notation. Recall that the commutator $[a, x] = axa^{-1}x^{-1} = x^a x^{-1}$. Now let G be a group and let $A = \mathrm{Aut}(G)$. We may regard G and A as subgroups of $\mathrm{Hol}(G)$ (by identifying G with G^l). For $x \in G$ and $\alpha \in A$, define

$$[\alpha, x] = \alpha(x)x^{-1},$$

and define

$$[A, G] = \langle [\alpha, x]: \alpha \in A, x \in G \rangle.$$

The next lemma will be used to give examples of nilpotent groups arising naturally.

Lemma 7.18. *Let G and A be subgroups of a group H, and let $G = G_0 \geq G_1 \geq \cdots$ be a series of normal subgroups of G such that $[A, G_i] \leq G_{i+1}$ for all i. Define $A_1 = A$ and*

$$A_j = \{\alpha \in A: [\alpha, G_i] \leq G_{i+j} \text{ for all } i\}.$$

Then $[A_j, A_l] \leq A_{j+l}$ for all j and l, and $[\gamma_j(A), G_i] \leq G_{i+j}$ for all i and j.

Proof. The definition of A_j gives $[A_j, G_i] \leq G_{i+j}$ for all i. It follows that $[A_j, A_l, G_i] = [A_j, [A_l, G_i]] \leq [A_j, G_{l+i}] \leq G_{j+l+i}$. Similarly, $[A_l, A_j, G_i] \leq G_{j+l+i}$. Now $G_{j+l+i} \lhd \langle G, A \rangle$, because both G and A normalize each G_i. Since $[A_j, A_l, G_i][A_l, A_j, G_i] \leq G_{j+l+i}$, the three subgroups lemma (Exercise 5.48 (ii)) gives $[G_i, [A_j, A_l]] = [[A_j, A_l], G_i] \leq G_{j+l+i}$. Therefore, $[A_j, A_l] \leq A_{j+l}$, by definition of A_{j+l}. It follows, for all j, that $A_j \lhd A$, because $[A_j, A] = [A_j, A_1] \leq A_{j+1} \leq A_j$, and so $A = A_1 \geq A_2 \geq \cdots$ is a central series for A. By Exercise 5.38(ii), $\gamma_j(A) \leq A_j$ for all j, so that, for all i, $[\gamma_j(A), G_i] \leq [A_j, G_i] \leq G_{j+i}$, as desired. ■

Definition. Let $G = G_0 \geq G_1 \geq \cdots \geq G_r = 1$ be a series of normal subgroups of a group G. An automorphism $\alpha \in \mathrm{Aut}(G)$ ***stabilizes*** this series if $\alpha(G_i x) = G_i x$ for all i and all $x \in G_{i-1}$. The ***stabilizer*** A of this series is the subgroup

$$A = \{\alpha \in \mathrm{Aut}(G): \alpha \text{ stabilizes the series}\} \leq \mathrm{Aut}(G).$$

Thus, α stabilizes a normal series $G = G_0 \geq G_1 \geq \cdots \geq G_r = 1$ if and only if $\alpha(G_i) \leq G_i$ and the induced map $G_i/G_{i+1} \to G_i/G_{i+1}$, defined by $G_{i+1}x \mapsto G_{i+1}\alpha(x)$, is the identity map for each i.

Theorem 7.19. *The stabilizer A of a series of normal subgroups $G = G_0 \geq G_1 \geq \cdots \geq G_r = 1$ is a nilpotent group of class $\leq r - 1$.*

Proof. Regard both G and A as subgroups of $\mathrm{Hol}(G)$. For all i, if $x \in G_i$ and $\alpha \in A$, then $\alpha(x) = g_{i+1}x$ for some $g_{i+1} \in G_{i+1}$, and so $\alpha(x)x^{-1} \in G_{i+1}$. In commutator notation, $[A, G_i] \leq G_{i+1}$. By Lemma 7.18, $[\gamma_j(A), G_i] \leq G_{i+j}$ for all i and j. In particular, for $i = 0$ and $j = r$, we have $[\gamma_r(A), G] \leq G_r = 1$; that is, for all $x \in G$ and $\alpha \in \gamma_r(A)$, we have $\alpha(x)x^{-1} = 1$. Therefore, $\gamma_r(A) = 1$ and A is nilpotent of class $\leq r - 1$. ■

For example, let $\{v_1, \ldots, v_n\}$ be a basis of a vector space V over a field k, and define $V_{i-1} = \langle v_i, v_{i+1}, \ldots, v_n \rangle$. Hence,

$$V = V_0 > V_1 > \cdots > V_n = 0$$

is a series of normal subgroups of the (additive abelian) group V. If $A \leq \mathrm{GL}(V)$ is the group of automorphisms stabilizing this series, then A is a nilpotent group of class $\leq n - 1$. If each $\alpha \in A \cap \mathrm{GL}(V)$ is regarded as a matrix (relative to the given basis), then it is easy to see that $A \cap \mathrm{GL}(V) = \mathrm{UT}(n, k)$, the group of all unitriangular matrices. Therefore, $\mathrm{UT}(n, k)$ is also nilpotent of class $\leq n - 1$. Compare this with Exercise 5.44.

If $G = G_0 \geq G_1 \geq \cdots \geq G_r = 1$ is any (not necessarily normal) series of a group G (i.e., G_i need not be a normal subgroup of G_{i-1}), then P. Hall (1958) proved that the stabilizer of this series is always nilpotent of class $\leq \frac{1}{2}r(r-1)$.

Exercises

7.7. If G is a finite nonabelian p-group, then $p^2 \mid |\mathrm{Aut}(G)|$.

7.8. If G is a finite abelian group, then $\mathrm{Aut}(G)$ is abelian if and only if G is cyclic.

7.9. (i) If G is a finite abelian group with $|G| > 2$, then $\mathrm{Aut}(G)$ has even order.
(ii) If G is not abelian, then $\mathrm{Aut}(G)$ is not cyclic. (*Hint.* Show that $\mathrm{Inn}(G)$ is not cyclic.)
(iii) There is no finite group G with $\mathrm{Aut}(G)$ cyclic of odd order > 1.

7.10. Show that $|\mathrm{GL}(2, p)| = (p^2 - 1)(p^2 - p)$. (*Hint.* How many ordered bases are in a two-dimensional vector space over $\mathbb{Z}_p$?)

7.11. If G is a finite group and $\mathrm{Aut}(G)$ acts transitively on $G^\# = G - \{1\}$, then G is an elementary abelian group.

7.12. If H and K are finite groups whose orders are relatively prime, then $\mathrm{Aut}(H \times K) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. Show that this may fail if $(|H|, |K|) > 1$. (*Hint.* Take $H = \mathbb{Z}_p = K$.)

7.13. Prove that $\mathrm{Aut}(\mathbf{Q}) \cong S_4$. (*Hint.* $\mathrm{Inn}(\mathbf{Q}) \cong \mathbf{V}$ and it equals its own centralizer in $\mathrm{Aut}(\mathbf{Q})$; use Theorem 7.1 with $G = \mathrm{Aut}(\mathbf{Q})$ and $H = \mathrm{Inn}(\mathbf{Q})$.)

7.14. (i) Show that $\mathrm{Hol}(\mathbb{Z}_2) \cong \mathbb{Z}_2$, $\mathrm{Hol}(\mathbb{Z}_3) \cong S_3$, $\mathrm{Hol}(\mathbb{Z}_4) \cong D_8$, and $\mathrm{Hol}(\mathbb{Z}_6) \cong D_{12}$.
(ii) If P is a Sylow 5-subgroup of S_5, then $\mathrm{Hol}(\mathbb{Z}_5) \cong N_{S_5}(P)$. (*Hint.* See Exercise 4.20.)

7.15. Prove that $\mathrm{Aut}(D_8) \cong D_8$, but that $\mathrm{Aut}(D_{16}) \ncong D_{16}$.

7.16. Is $\mathrm{Aut}(A_4) \cong S_4$? Is $\mathrm{Aut}(A_6) \cong S_6$?

7.17. If $G = B \times K$ and $B \leq L \leq G$, then $L = B \times (L \cap K)$.

7.18. If $H \lhd G$, prove that

$$\{\varphi \in \mathrm{Aut}(G)\colon \varphi \text{ fixes } H \text{ pointwise and } \varphi(g)H = gH \text{ for all } g \in G\}$$

is an abelian subgroup of $\mathrm{Aut}(G)$.

7.19. (i) Prove that the alternating groups A_n are never complete.
(ii) Show that if G is a complete group with $G \neq G'$, then G is not the commutator subgroup of any group containing it. Conclude that S_n, for $n \neq 2, 6$, is never a commutator subgroup.

7.20. If G is a complete group, then $\mathrm{Hol}(G) = G^l \times G^r$. Conclude, for $n \neq 2$ and $n \neq 6$, that $\mathrm{Hol}(S_n) \cong S_n \times S_n$.

7.21. Prove that every automorphism of a group G is the restriction of an inner automorphism of $\mathrm{Hol}(G)$.

7.22. Let G be a group and let $f \in S_G$. Prove that $f \in \mathrm{Hol}(G)$ if and only if $f(xy^{-1}z) = f(x)f(y)^{-1}f(z)$ for all $x, y, z \in G$.

Semidirect Products

Definition. Let K be a (not necessarily normal) subgroup of a group G. Then a subgroup $Q \leq G$ is a ***complement*** of K in G if $K \cap Q = 1$ and $KQ = G$.

A normal subgroup K of a group G need not have a complement and, even if it does, a complement need not be unique. In S_3, for example, every subgroup of order 2 serves as a complement to A_3. On the other hand, if they exist, complements are unique to isomorphism, for

$$G/K = KQ/K \cong Q/(K \cap Q) = Q/1 \cong Q.$$

A group G is the direct product of two normal subgroups K and Q if $K \cap Q = 1$ and $KQ = G$.

Definition. A group G is a ***semidirect product*** of K by Q, denoted by $G = K \rtimes Q$, if $K \lhd G$ and K has a complement $Q_1 \cong Q$. One also says that G ***splits*** over K.

We do not assume that a complement Q_1 is a normal subgroup; indeed, if Q_1 is a normal subgroup, then G is the direct product $K \times Q_1$.

In what follows, we denote elements of K by letters a, b, c in the first half of the alphabet, and we denote elements of Q by letters x, y, z at the end of the alphabet.

Before we give examples of semidirect products, let us give several different descriptions of them.

Lemma 7.20. *If K is a normal subgroup of a group G, then the following statements are equivalent:*

(i) *G is a semidirect product of K by G/K (i.e., K has a complement in G);*
(ii) *there is a subgroup $Q \leq G$ so that every element $g \in G$ has a unique expression $g = ax$, where $a \in K$ and $x \in Q$;*
(iii) *there exists a homomorphism $s\colon G/K \to G$ with $vs = 1_{G/K}$, where $v\colon G \to G/K$ is the natural map; and*
(iv) *there exists a homomorphism $\pi\colon G \to G$ with $\ker \pi = K$ and $\pi(x) = x$ for all $x \in \operatorname{im} \pi$ (such a map π is called a **retraction** of G and $\operatorname{im} \pi$ is called a **retract** of G).*

Proof. (i) $\Rightarrow$ (ii) Let Q be a complement of K in G. Let $g \in G$. Since $G = KQ$, there exist $a \in K$ and $x \in Q$ with $g = ax$. If $g = by$ is a second such factorization, then $xy^{-1} = a^{-1}b \in K \cap Q = 1$. Hence $b = a$ and $y = x$.

(ii) $\Rightarrow$ (iii) Each $g \in G$ has a unique expression $g = ax$, where $a \in K$ and $x \in Q$. If $Kg \in G/K$, then $Kg = Kax = Kx$; define $s\colon G/K \to G$ by $s(Kg) = x$. The routine verification that s is a well defined homomorphism with $vs = 1_{G/K}$ is left as an exercise for the reader.

(iii) $\Rightarrow$ (iv) Define $\pi\colon G \to G$ by $\pi = sv$. If $x = \pi(g)$, then $\pi(x) = \pi(\pi(g)) = svsv(g) = sv(g) = \pi(g) = x$ (because $vs = 1_{G/K}$). If $a \in K$, then $\pi(a) = sv(a) = 1$, for $K = \ker v$. For the reverse inclusion, assume that $1 = \pi(g) = sv(g) = s(Kg)$. Now s is an injection, by set theory, so that $Kg = K$ and so $g \in K$.

(iv) $\Rightarrow$ (i) Define $Q = \operatorname{im} \pi$. If $g \in Q$, then $\pi(g) = g$; if $g \in K$, then $\pi(g) = 1$; *a fortiori*, if $g \in K \cap Q$, then $g = 1$. If $g \in G$, then $g\pi(g^{-1}) \in K = \ker \pi$, for $\pi(g\pi(g^{-1})) = 1$. Since $\pi(g) \in Q$, we have $g = [g\pi(g^{-1})]\pi(g) \in KQ$. Therefore, Q is a complement of K in G and G is a semidirect product of K by Q. ■

EXAMPLE 7.7. S_n is a semidirect product of A_n by $\mathbb{Z}_2$.

Take $Q = \langle (1\ 2) \rangle$ to be a complement of A_n.

EXAMPLE 7.8. D_{2n} is a semidirect product of $\mathbb{Z}_n$ by $\mathbb{Z}_2$.

If $D_{2n} = \langle a, x \rangle$, where $\langle a \rangle \cong \mathbb{Z}_n$ and $\langle x \rangle \cong \mathbb{Z}_2$, then $\langle a \rangle$ is normal and $\langle x \rangle$ is a complement of $\langle a \rangle$.

EXAMPLE 7.9. For any group K, $\operatorname{Hol}(K)$ is a semidirect product of K^I by $\operatorname{Aut}(K)$.

This is contained in Lemma 7.16.

EXAMPLE 7.10. Let G be a solvable group of order mn, where $(m, n) = 1$. If G contains a normal subgroup of order m, then G is a semidirect product of K by a subgroup Q of order n.

This follows from P. Hall's theorem (Theorem 5.28).

EXAMPLE 7.11. $\mathrm{Aut}(S_6)$ is a semidirect product of S_6 by $\mathbb{Z}_2$.

This follows from Theorem 7.10 and Corollary 7.13.

EXAMPLE 7.12. If $G = \langle a \rangle$ is cyclic of order 4 and $K = \langle a^2 \rangle$, then G is not a semidirect product of K by G/K.

Since normality is automatic in an abelian group, an abelian group G is a semidirect product if and only if it is a direct product. But G is not a direct product. Indeed, it is easy to see that no primary cyclic group is a semidirect product.

EXAMPLE 7.13. Both S_3 and $\mathbb{Z}_6$ are semidirect products of $\mathbb{Z}_3$ by $\mathbb{Z}_2$.

Example 7.13 is a bit jarring at first, for it says, in contrast to direct product, that a semidirect product of K by Q is not determined to isomorphism by the two subgroups. When we reflect on this, however, we see that a semidirect product should depend on "how" K is normal in G.

Lemma 7.21. *If G is a semidirect product of K by Q, then there is a homomorphism $\theta\colon Q \to \mathrm{Aut}(K)$, defined by $\theta_x = \gamma_x | K$; that is, for all $x \in Q$ and $a \in K$,*

$$\theta_x(a) = xax^{-1}.$$

Moreover, for all $x, y, 1 \in Q$ and $a \in K$,

$$\theta_1(a) = a \qquad \text{and} \qquad \theta_x(\theta_y(a)) = \theta_{xy}(a).$$

Proof. Normality of K gives $\gamma_x(K) = K$ for all $x \in Q$. The rest is routine. ■

Remark. It follows that K is a group with operators Q.

The object of our study is to recapture G from K and Q. It is now clear that G also involves a homomorphism $\theta\colon Q \to \mathrm{Aut}(K)$.

Definition. Let Q and K be groups, and let $\theta\colon Q \to \mathrm{Aut}(K)$ be a homomorphism. A semidirect product G of K by Q ***realizes*** θ if, for all $x \in Q$ and $a \in K$,

$$\theta_x(a) = xax^{-1}.$$

In this language, Lemma 7.21 says that every semidirect product G of K by Q determines some θ which it realizes. Intuitively, "realizing θ" is a way of

describing how K is normal in G. For example, if θ is the trivial map, that is, $\theta_x = 1_K$ for every $x \in G$, then $a = \theta_x(a) = xax^{-1}$ for every $a \in K$, and so $K \leq C_G(Q)$.

Definition. Given groups Q and K and a homomorphism $\theta: Q \to \mathrm{Aut}(K)$, define $G = K \rtimes_\theta Q$ to be the set of all ordered pairs $(a, x) \in K \times Q$ equipped with the operation

$$(a, x)(b, y) = (a\theta_x(b), xy).$$

Theorem 7.22. *Given groups Q and K and a homomorphism $\theta: Q \to \mathrm{Aut}(K)$, then $G = K \rtimes_\theta Q$ is a semidirect product of K by Q that realizes θ.*

Proof. We first prove that G is a group. Multiplication is associative:

$$\begin{aligned} &[(a, x)(b, y)](c, z) && (a, x)[(b, y)(c, z)] \\ &= (a\theta_x(b), xy)(c, z) && = (a, x)(b\theta_y(c), yz) \\ &= (a\theta_x(b)\theta_{xy}(c), xyz), && = (a\theta_x(b\theta_y(c)), xyz). \end{aligned}$$

The formulas in Lemma 7.21 (K is a group with operators Q) show that the final entries in each column are equal.

The identity element of G is $(1, 1)$, for

$$(1, 1)(a, x) = (1\theta_1(a), 1x) = (a, x);$$

the inverse of (a, x) is $((\theta_{x^{-1}}(a))^{-1}, x^{-1})$, for

$$((\theta_{x^{-1}}(a))^{-1}, x^{-1})(a, x) = ((\theta_{x^{-1}}(a))^{-1}\theta_{x^{-1}}(a), x^{-1}x) = (1, 1).$$

We have shown that G is a group.

Define a function $\pi: G \to Q$ by $(a, x) \mapsto x$. Since the only "twist" occurs in the first coordinate, it is routine to check that π is a surjective homomorphism and that $\ker \pi = \{(a, 1): a \in K\}$; of course, $\ker \pi$ is a normal subgroup of G. We identify K with $\ker \pi$ via the isomorphism $a \mapsto (a, 1)$. It is also easy to check that $\{(1, x): x \in Q\}$ is a subgroup of G isomorphic to Q (via $x \mapsto (1, x)$), and we identify Q with this subgroup. Another easy calculation shows that $KQ = G$ and $K \cap Q = 1$, so that G is a semidirect product of K by Q.

Finally, G does realize θ:

$$(1, x)(a, 1)(1, x)^{-1} = (\theta_x(a), x)(1, x^{-1}) = (\theta_x(a), 1). \quad \blacksquare$$

Since $K \rtimes_\theta Q$ realizes θ, that is, $\theta_x(b) = xbx^{-1}$, there can be no confusion if we write $b^x = xbx^{-1}$ instead of $\theta_x(b)$. The operation in $K \rtimes_\theta Q$ will henceforth be written

$$(a, x)(b, y) = (ab^x, xy).$$

Theorem 7.23. *If G is a semidirect product of K by Q, then there exists $\theta: Q \to \mathrm{Aut}(K)$ with $G \cong K \rtimes_\theta Q$.*

Proof. Define $\theta_x(a) = xax^{-1}$ (as in Lemma 7.21). By Lemma 7.20 (ii), each $g \in G$ has a unique expression $g = ax$ with $a \in K$ and $x \in Q$. Since multiplication in G satisfies

$$(ax)(by) = a(xbx^{-1})xy = ab^x xy,$$

it is easy to see that the map $K \rtimes_\theta Q \to G$, defined by $(a, x) \mapsto ax$, is an isomorphism. ■

We now illustrate how this construction can be used.

EXAMPLE 7.14. The group T of order 12 (see Theorem 4.24) is a semidirect product of $\mathbb{Z}_3$ by $\mathbb{Z}_4$.

Let $\mathbb{Z}_3 = \langle a \rangle$, let $\mathbb{Z}_4 = \langle x \rangle$, and define $\theta\colon \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$ by sending a into the generator; that is, θ_x is squaring. In more detail,

$$a^x = a^2 \qquad \text{and} \qquad (a^2)^x = a,$$

while x^2 acts on $\langle a \rangle$ as the identity automorphism: $a^{x^2} = a$.

The group $G = \mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_4$ has order 12. If $s = (a^2, x^2)$ and $t = (1, x)$, then the reader may check that

$$s^6 = 1 \qquad \text{and} \qquad t^2 = s^3 = (st)^2,$$

which are the relations in T.

EXAMPLE 7.15. Let p be a prime, let $K = \langle a, b \rangle$ be an elementary abelian group of order p^2, and let $Q = \langle x \rangle$ be a cyclic group of order p. Define $\theta\colon Q \to \mathrm{Aut}(K) \cong \mathrm{GL}(2, p)$ by

$$x^i \mapsto \begin{bmatrix} 1 & 0 \\ i & 1 \end{bmatrix}.$$

Thus, $a^x = ab$ and $b^x = b$. The commutator $a^x a^{-1}$ is seen to be b. Therefore, $G = K \rtimes_\theta Q$ is a group of order p^3 with $G = \langle a, b, x \rangle$, and these generators satisfy relations

$$a^p = b^p = x^p = 1, \qquad b = [x, a], \qquad \text{and} \qquad [b, a] = 1 = [b, x].$$

If p is odd, then we have the nonabelian group of order p^3 and exponent p; if $p = 2$, then $G \cong D_8$ (as the reader may check). In Example 7.8, we saw that $D_8 \cong \mathbb{Z}_4 \rtimes_\theta \mathbb{Z}_2$; we have just seen here that $D_8 \cong \mathbf{V} \rtimes_\theta \mathbb{Z}_2$. A group may thus have distinct factorizations into a semidirect product.

EXAMPLE 7.16. Let p be an odd prime, let $K = \langle a \rangle$ be cyclic of order p^2, and let $Q = \langle x \rangle$ be cyclic of order p. By Theorem 7.3, $\mathrm{Aut}(K) \cong \mathbb{Z}_{p(p-1)} \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_p$; indeed, by Theorem 6.9, the cyclic summand $\mathbb{Z}_p = \langle \alpha \rangle$, where $\alpha(a) = a^{1+p}$. If one defines $\theta\colon Q \to \mathrm{Aut}(K)$ by $\theta_x = \alpha$, then the group $G = K \rtimes_\theta Q$ has order p^3, generators x, a, and relations $x^p = 1$, $a^{p^2} = 1$, and $xax^{-1} = a^x = a^{1+p}$. We have constructed the second nonabelian group of order p^3 (see Exercise 4.32).

Theorem 9.78. $M_{12} \cong \mathrm{Aut}(X, \mathscr{B})$, *where* $(X, \mathscr{B})$ *is a Steiner system of type* $S(5, 6, 12)$.

Remark. There is only one Steiner system with these parameters.

Proof. Let $(X, \mathscr{B})$ be the Steiner system constructed in Theorem 9.76. Now $M_{12} \leq \mathrm{Aut}(X, \mathscr{B})$ because every $g \in M_{12}$ carries blocks to blocks. For the reverse inclusion, let $\varphi \in \mathrm{Aut}(X, \mathscr{B})$. Composing with an element of M_{12} if necessary, we may assume that φ permutes $T = \{\infty, \omega, \Omega\}$ and φ permutes GF(9). Regarding GF(9) as an affine plane over $\mathbb{Z}_3$, we see from Lemma 9.77 that $\varphi|\mathrm{GF}(9)$ is an affine automorphism. By Exercise 9.39, there is $g \in M_{12}$ which permutes T and with $g|\mathrm{GF}(9) = \varphi|\mathrm{GF}(9)$. Now $\varphi g^{-1} \in \mathrm{Aut}(X, \mathscr{B})$, for $M_{12} \leq \mathrm{Aut}(X, \mathscr{B})$, φg^{-1} permutes T, and φg^{-1} fixes the other 9 points of X. We claim that φg^{-1} fixes every block B in $\mathscr{B}$. This is clear if $|B \cap T| = 0$, 1, or 3. In the remaining case, say, $B = \{\infty, \omega, x_1, \ldots, x_4\}$, then $\varphi g^{-1}(B)$ must contain either ∞ or ω as well as the x_i, so that $|B \cap \varphi g^{-1}(B)| \geq 5$. Since 5 points determine a block, $B = \varphi g^{-1}(B)$, as claimed. Theorem 9.63 forces $\varphi g^{-1} = 1$, and so $\varphi = g \in M_{12}$, as desired. ■

Theorem 9.79. $M_{11} \cong \mathrm{Aut}(X', \mathscr{B}')$, *where* $(X', \mathscr{B}')$ *is a Steiner system of type* $S(4, 5, 11)$.

Remark. There is only one Steiner system with these parameters.

Proof. Let $(X', \mathscr{B}')$ be the contraction at Ω of the Steiner system $(X, \mathscr{B})$ of Theorem 9.76. It is clear that $M_{11} \leq \mathrm{Aut}(X', \mathscr{B}')$. For the reverse inclusion, regard $\varphi \in \mathrm{Aut}(X', \mathscr{B}')$ as a permutation of X with $\varphi(\Omega) = \Omega$. Multiplying by an element of M_{11} if necessary, we may assume that φ permutes $\{\infty, \omega\}$. By Lemma 9.77, a block $B' \in \mathscr{B}'$ containing ∞ and ω has the form $B' = \{\infty, \omega\} \cup \ell$, where ℓ is a line in the affine plane over $\mathbb{Z}_3$. As in the proof of Theorem 9.78, $\varphi|\mathrm{GF}(9)$ is an affine isomorphism, so there is $g \in M_{12}$ with $g|\mathrm{GF}(9) = \varphi|\mathrm{GF}(9)$. As in the proof of Theorem 9.72, an examination of $g(\mathrm{star}(\Omega))$ shows that $g(\Omega) = \Omega$, so that $g \in (M_{12})_\Omega = M_{11}$. The argument now finishes as that for Theorem 9.78: $\varphi g^{-1} \in \mathrm{Aut}(X', \mathscr{B}')$; φg^{-1} fixes $\mathscr{B}'$; $\varphi = g \in M_{11}$. ■

The subgroup structures of the Mathieu groups are interesting. There are other simple groups imbedded in them: for example, M_{12} contains copies of A_6, PSL(2, 9), and PSL(2, 11), while M_{24} contains copies of M_{12}, A_8, and PSL(2, 23). The copy Σ of S_6 in M_{12} leads to another proof of the existence of an outer automorphism of S_6.

Theorem 9.80. S_6 *has an outer automorphism of order* 2.

Remark. See Corollary 7.13 for another proof.

Proof. Recall from Lemma 9.75 that if $X = \{\infty, \omega, \Omega\} \cup \mathrm{GF}(9)$ and Σ ($\cong S_6$) is the subgroup of M_{12} in Lemma 9.75, then X has two Σ-orbits, say, $Z = Y \cup \{0\}$ and $Z' = Y' \cup \{0'\}$, each of which has 6 points. If $\sigma \in \Sigma$ has order 5, then σ is a product of two disjoint 5-cycles (only one 5-cycle fixes too many points), hence it fixes, say, 0 and 0′. It follows that if $U = \langle\sigma\rangle$, then each of Z and Z' consists of two U-orbits, one of size 5 and one of size 1. Now $H = (M_{12})_{0,0'} \cong M_{10}$, and U is a Sylow 5-subgroup of H. By Theorem 9.66, $N = N_{M_{12}}(U)$ acts 2-transitively on $\mathscr{F}(U) = \{0, 0'\}$, so there is $\alpha \in N$ of order 2 which interchanges 0 and 0′.

Since α has order 2, $\alpha = \tau_1 \ldots \tau_m$, where the τ_i are disjoint transpositions and $m \leq 6$. But M_{12} is sharply 5-transitive, so that $4 \leq m$; also, $M_{12} \leq A_{12}$, so that $m = 4$ or $m = 6$.

We claim that α interchanges the sets $Z = Y \cup \{0\}$ and $Z' = Y' \cup \{0'\}$. Otherwise, there is $y \in Y$ with $\alpha(y) = z \in Y$. Now $\alpha\sigma\alpha = \sigma^i$ for some i (because α normalizes $\langle\sigma\rangle$). If $\sigma^i(y) = u$ and $\sigma(z) = v$, then $u, v \in Y$ because $Y \cup \{0\}$ is a Σ-orbit. But $u = \sigma^i(y) = \alpha\sigma\alpha(y) = \alpha\sigma(z) = \alpha(v)$, and it is easy to see that y, z, u, and v are all distinct. Therefore, the cycle decomposition of α involves $(0\ 0')$, $(y\ z)$, and $(v\ u)$. There is only one point remaining in Y, say a, and there are two cases: either $\alpha(a) = a$ or $\alpha(a) \in Y'$. If α fixes a, then there is $y' \in Y'$ moved by α, say, $\alpha(y') = z' \in Y'$. Repeat the argument above: there are points $u', v' \in Y'$ with transpositions $(y'\ z')$ and $(v'\ u')$ involved in the cycle decomposition of α. If a' is the remaining point in Y', then the transposition $(a\ a')$ must also occur in the factorization of α because α is not a product of 5 disjoint transpositions. In either case, we have $a \in Y$ and $a' \in Y'$ with $\alpha = (0\ 0')(y\ z)(v\ u)(a\ a')\beta$, where β permutes $Y' - \{a'\}$. But $\alpha\sigma\alpha(a) = \sigma^i(a) \in Z$; on the other hand, if $\sigma(a') = b' \in Y'$, say, then $\alpha\sigma\alpha(a) = \alpha\sigma(a') = \alpha(b')$, so that $\alpha(b') \in Y$. Since a' is the only element of Y' that α moves to Y, $b' = a'$ and $\sigma(a') = b' = a'$; that is, σ fixes a'. This is a contradiction, for σ fixes only 0 and 0′.

It is easy to see that α normalizes Σ. Recall that $\sigma \in \Sigma$ if and only if $\sigma(Z) = Z$ (and hence $\sigma(Z') = Z'$). Now $\alpha\sigma\alpha(Z) = \alpha\sigma(Z') = \alpha(Z') = Z$, so that $\alpha\sigma\alpha \in \Sigma$. Therefore, $\gamma = \gamma_\alpha$ (conjugation by α) is an automorphism of Σ.

Suppose there is $\beta \in \Sigma$ with $\alpha\sigma^*\alpha = \beta\sigma^*\beta^{-1}$ for all $\sigma^* \in \Sigma$; that is, $\beta^{-1}\alpha \in C = C_{M_{12}}(\Sigma)$. If $C = 1$, then $\alpha = \beta \in \Sigma$, and this contradiction would show that γ is an outer automorphism. If $\sigma^* \in \Sigma$, then $\sigma^* = \sigma\sigma'$, where σ permutes Z and fixes Z' and σ' permutes Z' and fixes Z. Schematically,

$$\sigma^* = (z\ x\ \ldots)(z'\ x'\ \ldots);$$

if $\mu \in M_{12}$, then (as any element of S_{12}),

$$\mu\sigma^*\mu^{-1} = (\mu z\ \mu x\ \ldots)(\mu z'\ \mu x'\ \ldots).$$

In particular, if $\mu \in C$ (so that $\mu\sigma^*\mu^{-1} = \sigma^*$), then either $\mu(Z) = Z$ and $\mu(Z') = Z'$ or μ switches Z and Z'. In the first case, $\mu \in \Sigma$, by Lemma 9.75, and $\mu \in C \cap \Sigma = Z(\Sigma) = 1$. In the second case, $\mu\sigma\mu^{-1} = \sigma'$ (and $\mu\sigma'\mu^{-1} = \sigma$), so that σ and σ' have the same cycle structure for all $\sigma^* = \sigma\sigma' \in \Sigma$. But there

is $\sigma^* \in \Sigma$ with σ a transposition. If such μ exists, then σ^* would be a product of two disjoint transpositions and hence would fix 8 points, contradicting M_{12} being sharply 5-transitive. ■

There is a similar argument, using an imbedding of M_{12} into M_{24}, which exhibits an outer automorphism of M_{12}. There are several other proofs of the existence of the outer automorphism of S_6; for example, see Conway and Sloane (1993).

The Steiner systems of types $S(5, 6, 12)$ and $S(5, 8, 24)$ arise in algebraic coding theory, being the key ingredients of (ternary and binary) ***Golay codes***. The Steiner system of type $S(5, 8, 24)$ is also used to define the ***Leech lattice***, a configuration in $\mathbb{R}^{24}$ arising in certain sphere-packing problems as well as in the construction of other simple sporadic groups.

CHAPTER 10

Abelian Groups

Commutativity is a strong hypothesis, so strong that all finite abelian groups are completely classified. In this chapter, we focus on finitely generated and, more generally, countable abelian groups.

Basics

A valuable viewpoint in studying an abelian group G is to consider it as an extension of simpler groups. Of course, this reduces the study of G to a study of the simpler groups and an extension problem.

In this chapter, we assume that ***all groups are abelian*** and we again adopt additive notation.

Definition. A sequence of groups and homomorphisms

$$\cdots \to A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \to \cdots$$

is an ***exact sequence*** if the image of each map is the kernel of the next map. A ***short exact sequence*** is an exact sequence of the form

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0.$$

There is no need to label the arrow $0 \to A$, for there is only one such homomorphism, namely, $0 \mapsto 0$; similarly, there is no need to label the only possible homomorphism $C \to 0$: it must be the constant map $x \mapsto 0$. In the short exact sequence above, $0 = \operatorname{im}(0 \to A) = \ker f$ says that f is an injection and $A \cong \operatorname{im} f$; also, $\operatorname{im} g = \ker(C \to 0) = C$ says that g is a surjection. Finally, the first isomorphism theorem gives $B/\operatorname{im} f = B/\ker g \cong \operatorname{im} g = C$.

If $A \leq B$ and f is the inclusion, then $\operatorname{im} f = A$ and $B/A \cong C$. Thus, B is an extension of A by C if and only if there is a short exact sequence $0 \to A \to B \to C \to 0$.

Definition. If G is a group, its ***torsion subgroup*** is

$$tG = \{x \in G: nx = 0 \text{ for some nonzero integer } n\}.$$

Note that tG is a fully invariant subgroup of G.

When G is not abelian, then tG may not be a subgroup. For example, Exercise 2.17 shows that tG is not a subgroup when $G = \mathrm{GL}(2, \mathbb{Q})$.

Definition. A group G is ***torsion*** if $tG = G$; it is ***torsion-free*** if $tG = 0$.

The term torsion is taken from Algebraic Topology; the homology groups of a "twisted" manifold have elements of finite order.

Theorem 10.1. *The quotient group G/tG is torsion-free, and so every group G is an extension of a torsion group by a torsion-free group.*

Proof. If $n(g + tG) = 0$ in G/tG for some $n \neq 0$, then $ng \in tG$, and so there is $m \neq 0$ with $m(ng) = 0$. Since $mn \neq 0$, $g \in tG$, $g + tG = 0$ in G/tG, and G/tG is torsion-free. ■

If an abelian group is a semidirect product, then it is a direct product or, in additive terminology, it is a direct sum. The first question is whether the extension problem above is only virtual or if there exists a group G whose torsion subgroup is not a ***direct summand*** of G (i.e., there is no subgroup $A \leq G$ with $G = tG \oplus A$). Let us first generalize one of the constructions we have already studied.

Definition. Let K be a possibly infinite set and let $\{A_k: k \in K\}$ be a family of groups[1] indexed by K. The ***direct product*** (or *complete direct sum* or *strong direct sum*), denoted by $\prod_{k \in K} A_k$, is the group whose elements are all "vectors" (a_k) in the cartesian product of the A_k and whose operation is

$$(a_k) + (b_k) = (a_k + b_k).$$

The ***direct sum*** (or weak direct sum), denoted by $\sum_{k \in K} A_k$, is the subgroup of $\prod_{k \in K} A_k$ consisting of all those elements (a_k) for which there are only finitely many k with $a_k \neq 0$.

If the index set K is finite, then $\prod_{k \in K} A_k = \sum_{k \in K} A_k$; if the index set K is

[1] These constructions make sense for nonabelian groups as well. They have already arisen, for example, in our remark in Chapter 7 that different wreath products $K \wr Q$ (complete and restricted) arise when Q acts on an infinite set Ω.

infinite and infinitely many $A_k \neq 0$, then the direct sum is a proper subgroup of the direct product.

Definition. If $x \in G$ and n is a nonzero integer, then x is ***divisible by n in G*** if there is $g \in G$ with $ng = x$.

Were the operation in G written multiplicatively, then one would say that x has an nth *root* in G. Exercise 1.31 shows that an element of order m is divisible by every n with $(n, m) = 1$.

Theorem 10.2. *There exists a group G whose torsion subgroup is not a direct summand of G.*

Proof. Let P be the set of all primes, and let $G = \prod_{p \in P} \mathbb{Z}_p$. If q is a prime and $x = (x_p) \in G$ is divisible by q, then there is $y = (y_p)$ with $qy_p = x_p$ for all p; it follows that $x_q = 0$. Therefore, if x is divisible by every prime, then $x = 0$.

We claim that G/tG contains a nonzero element which is divisible by every prime. If this were true, then $G \neq tG \oplus H$ for some subgroup H, because $H \cong G/tG$. If $a_p \in \mathbb{Z}_p$ is a generator, then $a = (a_p)$ has infinite order: if $na = 0$, then $na_p = 0$ for all p, so that p divides n for all p and hence $n = 0$. Therefore $a \notin tG$, and its coset $a + tG$ is a nonzero element of G/tG. If q is a prime, then a_p is divisible by q in $\mathbb{Z}_p$ for all $p \neq q$, by Exercise 1.31; there is thus $y_p \in \mathbb{Z}_p$ with $qy_p = a_p$ for all $p \neq q$. Define $y_q = 0$ and define $y = (y_p)$. Now $a - qy \in tG$ (for its coordinates are all 0 except for a_q in position q). Hence

$$q(y + tG) = qy + tG = a - (a - qy) + tG = a + tG,$$

and so $a + tG$ is divisible by every prime q. ■

We restate Lemma 7.20 for abelian groups.

Lemma 10.3. *If G is an abelian group and $A \leq G$, then the following statements are equivalent.*

(i) *A is a direct summand of G (there is a subgroup $B \leq G$ with $A \cap B = 0$ and $A + B = G$).*
(ii) *There is a subgroup $B \leq G$ so that each $g \in G$ has a unique expression $g = a + b$ with $a \in A$ and $b \in B$.*
(iii) *There exists a homomorphism $s\colon G/A \to G$ with $vs = 1_{G/A}$, where $v\colon G \to G/A$ is the natural map.*
(iv) *There exists a retraction $\pi\colon G \to A$; that is, π is a homomorphism with $\pi(a) = a$ for all $a \in A$.*

The following criterion is a generalization of Exercise 2.75 (which characterizes finite direct sums).

Lemma 10.4. *Let $\{A_k: k \in K\}$ be a family of subgroups of a group G. The following statements are equivalent.*

(i) $G \cong \sum_{k \in K} A_k$.
(ii) *Every $g \in G$ has a unique expression of the form*

$$g = \sum_{k \in K} a_k,$$

where $a_k \in A_k$, the k are distinct, and $a_k \neq 0$ for only finitely many k.
(iii) $G = \langle \bigcup_{k \in K} A_k \rangle$ *and, for each* $j \in K$, $A_j \cap \langle \bigcup_{k \neq j} A_k \rangle = 0$.

Proof. Routine. ■

Theorem 10.5. *If V is a vector space over a field K, then, as an additive group, V is a direct sum of copies of K.*

Proof. Let X be a basis of V. For each $x \in X$, the one-dimensional subspace Kx spanned by x, is, as a group, isomorphic to K. The reader may check, using Lemma 10.4, that $V = \sum_{x \in X} Kx$. ■

There is a notion of independence for abelian groups.

Definition. A finite subset $X = \{x_1, \ldots, x_n\}$ of nonzero elements of a group G is ***independent*** if, for all $m_i \in \mathbb{Z}$, $\sum m_i x_i = 0$ implies $m_i x_i = 0$ for each i. An infinite set X of nonzero elements in G is ***independent*** if every finite subset is independent.

If X is an independent subset of a group G and $\sum m_x x = 0$, then $m_x x = 0$ for each x. If G is torsion-free, then $m_x = 0$ for all x; however, if G has torsion, then one may conclude only that m_x is a multiple of the order of x.

Lemma 10.6. *A set X of nonzero elements of a group G is independent if and only if*

$$\langle X \rangle = \sum_{x \in X} \langle x \rangle.$$

Proof. Assume that X is independent. If $x_0 \in X$ and $y \in \langle x_0 \rangle \cap \langle X - \{x_0\} \rangle$, then $y = mx_0$ and $y = \sum m_i x_i$, where the x_i are distinct elements of X not equal to x_0. Hence

$$-mx_0 + \Sigma m_i x_i = 0,$$

so that independence gives each term 0; in particular, $0 = mx_0 = y$.

The proof of the converse, also routine, is left to the reader. ■

Recall, in the context of abelian groups, that *p-groups* are called *p-primary groups.*

Theorem 10.7 (Primary Decomposition). *Every torsion group G is a direct sum of p-primary groups.*

Proof. For a prime p, define

$$G_p = \{x \in G: p^n x = 0 \text{ for some } n \geq 0\}$$

(G_p is called the ***p-primary component*** of G.) The proof of Theorem 6.1, *mutatis mutandis*, show that $G \cong \sum_p G_p$. ■

Theorem 10.8. *If G and H are torsion groups, then $G \cong H$ if and only if $G_p \cong H_p$ for all primes p.*

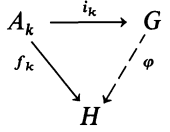
Proof. If $\varphi: G \to H$ is a homomorphism, then $\varphi(G_p) \leq H_p$ for all primes p. In particular, if φ is an isomorphism, then $\varphi(G_p) \leq H_p$ and $\varphi^{-1}(H_p) \leq G_p$ for all p. It follows easily that $\varphi | G_p$ is an isomorphism $G_p \to H_p$.

Conversely, assume that there are isomorphisms $\varphi_p: G_p \to H_p$ for all primes p. By Theorem 10.4(ii), each $g \in G$ has a unique expression of the form $g = \sum_p a_p$, where only a finite number of the $a_p \neq 0$. Then $\varphi: G \to H$, defined by $\varphi(\sum a_p) = \sum \varphi_p(a_p)$, is easily seen to be an isomorphism. ■

Because of these last two results, most questions about torsion groups can be reduced to questions about p-primary groups.

Here are two technical results about direct sums and products that will be useful.

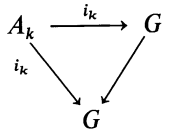
Theorem 10.9. *Let G be an abelian group, let $\{A_k: k \in K\}$ be a family of abelian groups, and let $\{i_k: A_k \to G: k \in K\}$ be a family of homomorphisms. Then $G \cong \sum_{k \in K} A_k$ if and only if, given any abelian group H and any family of homomorphisms $\{f_k: A_k \to H: k \in K\}$, then there exists a unique homomorphism $\varphi: G \to H$ making the following diagrams commute ($\varphi i_k = f_k$):*



Proof. We show first that $G = \sum A_k$ has the stated property. Define $j_k: A_k \hookrightarrow G$ to be the inclusion. By Lemma 10.4, every $g \in G$ has a unique expression of the form $g = \sum_{k \in K} a_k$, with $a_k \neq 0$ for only finitely many k. It follows that $\psi(g) = \sum f_k(a_k)$ is a well defined function; it is easily checked that ψ is a homomorphism making the kth diagram commute for all k; that is, $\psi j_k = f_k$ for all k.

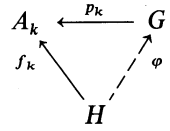
Assume now that G is any group satisfying the stated property, and choose the diagram with $H = G$ and $f_k = j_k$. By hypothesis, there is a map $\varphi: G \to \sum A_k$ making the diagrams commute.

Finally, we show that $\psi\varphi$ and $\varphi\psi$ are identities. Both $\psi\varphi$ and 1_G complete the diagram



and so the uniqueness hypothesis gives $\psi\varphi = 1_G$. A similar diagram shows that $\varphi\psi$ is the identity on $\sum A_k$. ■

Theorem 10.10. *Let G be an abelian group, let $\{A_k: k \in K\}$ be a family of abelian groups, and let $\{p_k: G \to A_k: k \in K\}$ be a family of homomorphisms. Then $G \cong \prod_{k\in K} A_k$ if and only if, given any abelian group H and any family of homomorphisms $\{f_k: H \to A_k: k \in K\}$, there exists a unique homomorphism $\varphi: H \to G$ making the following diagrams commute for all k:*



Proof. The argument is similar to the one just given if one defines $p_k: \prod_{l\in K} A_l \to H$ as the projection of a "vector" onto its kth coordinate. ■

EXERCISES

10.1. Let $\{A_k: k \in K\}$ be a family of torsion groups.
(i) The direct sum $\sum_{k\in K} A_k$ is torsion.
(ii) If n is a positive integer and if each A_k has exponent n (i.e., $nA_k = 0$ for all k), then $\prod_{k\in K} A_k$ is torsion.

10.2. If $x \in G$, then any two solutions to the equation $ny = x$ differ by an element z with $nz = 0$. Conclude that y is unique if G is torsion-free.

10.3. If G is a torsion-free group and X is a maximal independent subset, then $G/\langle X\rangle$ is torsion.

10.4. (i) If $G = \sum A_k$, prove that the maps $i_k: A_k \to G$ in Theorem 10.9 are injections.
(ii) If $G = \prod A_k$, prove that the maps $p_k: G \to A_k$ in Theorem 10.10 are surjections.

Free Abelian Groups

Definition. An abelian group F is ***free abelian*** if it is a direct sum of infinite cyclic groups. More precisely, there is a subset $X \subset F$ of elements of infinite order, called a ***basis*** of F, with $F = \sum_{x\in X} \langle x\rangle$; i.e., $F \cong \sum \mathbb{Z}$.

We allow the possibility $X = \varnothing$, in which case $F = 0$.

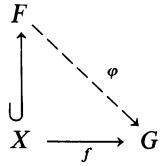
It follows at once from Lemma 10.4 that if X is a basis of a free abelian group F, then each $u \in F$ has a unique expression of the form $u = \sum m_x x$, where $m_x \in \mathbb{Z}$ and $m_x = 0$ for "almost all" $x \in X$; that is, $m_x \neq 0$ for only a finite number of x.

Notice that a basis X of a free abelian group is independent, by Lemma 10.6.

Theorem 10.11. *Let F be a free abelian group with basis X, let G be any abelian group, and let $f: X \to G$ be any function. Then there is a unique homomorphism $\varphi: F \to G$ extending f; that is,*

$$\varphi(x) = f(x) \qquad \text{for all} \quad x \in X.$$

Indeed, if $u = \sum m_x x \in F$, then $\varphi(u) = \sum m_x f(u)$.



Proof. If $u \in F$, then uniqueness of the expression $u = \sum m_x x$ shows that $\varphi: u \mapsto \sum m_x f(u)$ is a well defined function. That φ is a homomorphism extending f is obvious; φ is unique because homomorphisms agreeing on a set of generators must be equal.

Here is a fancy proof. For each $x \in X$, there is a unique homomorphism $\varphi_x: \langle x \rangle \to G$ defined by $mx \mapsto mf(x)$. The result now follows from Lemma 10.6 and Theorem 10.10. ■

Corollary 10.12. *Every (abelian) group G is a quotient of a free abelian group.*

Proof. Let F be the direct sum of $|G|$ copies of $\mathbb{Z}$, and let x_g denote a generator of the gth copy of $\mathbb{Z}$, where $g \in G$. Of course, F is a free abelian group with basis $X = \{x_g: g \in G\}$. Define a function $f: X \to G$ by $f(x_g) = g$ for all $g \in G$. By Theorem 10.11, there is a homomorphism $\varphi: F \to G$ extending f. Now φ is surjective, because f is surjective, and so $G \cong F/\ker \varphi$, as desired. ■

The construction of a free abelian group in the proof of Corollary 10.12 can be modified: one may identify x_g with g. If X is any set, one may thus construct a free abelian group F having X itself as a basis. This is quite convenient. For example, in Algebraic Topology, one wishes to consider formal $\mathbb{Z}$-linear combinations of continuous maps between topological spaces; this can be done by forming the free abelian group with basis the set of all such functions.

The corollary provides a way of describing abelian groups.

Definition. An abelian group G has ***generators*** X ***and relations*** Δ *if* $G \cong F/R$, where F is the free abelian group with basis X, Δ is a set of $\mathbb{Z}$-linear combinations of elements of X, and R is the subgroup of F generated by Δ. If X can be chosen finite, then G is called ***finitely generated***.

EXAMPLE 10.1. $G = \mathbb{Z}_6$ has generator x and relation $6x$.

EXAMPLE 10.2. $G = \mathbb{Z}_6$ has generators $\{x, y\}$, and relations $\{2x, 3y\}$.

EXAMPLE 10.3. $G = \mathbb{Q}$ has generators $\{x_1, \ldots, x_n, \ldots\}$ and relations $\{x_1 - 2x_2, x_2 - 3x_3, \ldots, x_{n-1} - nx_n, \ldots\}$.

EXAMPLE 10.4. If G is free abelian with basis X, then G has generators X and no relations (recall that 0 is the subgroup generated by the empty set). The etymology of the term *free* should now be apparent.

We have just seen that one can describe a known group by generators and relations. One can also use generators and relations to construct a group with prescribed properties.

Theorem 10.13. *There is an infinite p-primary group* $G = \mathbb{Z}(p^\infty)$ *each of whose proper subgroups is finite (and cyclic).*

Proof. Define a group G having

generators: $X = \{x_0, x_1, \ldots, x_n, \ldots\}$

and

relations: $\{px_0, x_0 - px_1, x_1 - px_2, \ldots, x_{n-1} - px_n, \ldots\}$.

Let F be the free abelian group on X, let $R \leq F$ be generated by the relations, and let $a_n = x_n + R \in F/R = G$. Then $pa_0 = 0$ and $a_{n-1} = pa_n$ for all $n \geq 1$, so that $p^{n+1}a_n = pa_0 = 0$. It follows that G is p-primary, for $p^{t+1}\sum_{n=0}^{t} m_n a_n = 0$, where $m_n \in \mathbb{Z}$. A typical relation (i.e., a typical element of R) has the form:

$$m_0 p x_0 + \sum_{n\geq 1} m_n(x_{n-1} - px_n) = (m_0 p + m_1)x_0 + \sum_{n\geq 1} (m_{n+1} - m_n p)x_n.$$

If $a_0 = 0$, then $x_0 \in R$, and independence of X gives the equations $1 = m_0 p + m_1$ and $m_{n+1} = pm_n$ for all $n \geq 1$. Since $R \leq F$ and F is a direct sum, $m_n = 0$ for large n. But $m_{n+1} = p^n m_1$ for all n, and so $m_1 = 0$. Therefore, $1 = m_0 p$, and this contradicts $p \geq 2$. A similar argument shows that $a_n \neq 0$ for all n. We now show that all a_n are distinct, which will show that G is infinite. If $a_n = a_k$ for $k > n$, then $a_{n-1} = pa_n$ implies $a_k = p^{k-n}a_n$, and this gives $(1 - p^{k-n})a_k = 0$; since G is p-primary, this contradicts $a_k \neq 0$.

Let $H \leq G$. If H contains infinitely many a_n, then it contains all of them, and $H = G$. If H involves only $a_0, \ldots, a_m$, then $H \leq \langle a_0, \ldots, a_m\rangle \leq \langle a_m\rangle$. Thus, H is a subgroup of a finite cyclic group, and hence H is also a finite cyclic group. ■

The group $\mathbb{Z}(p^\infty)$ has other interesting properties (see Exercise 10.5 below), and we shall return to it in a later section.

Theorem 10.14. *Two free abelian groups* $F = \sum_{x \in X} \langle x \rangle$ *and* $G = \sum_{y \in Y} \langle y \rangle$ *are isomorphic if and only if* $|X| = |Y|$.

Proof. Since $|X| = |Y|$, there is a bijection $f: X \to Y \subset G$, and f determines a homomorphism $\varphi: F \to G$ with $\varphi(x) = f(x)$ for all $x \in X$. Similarly, there is a homomorphism $\psi: G \to F$ with $\psi(y) = f^{-1}(y)$ for all $y \in Y$. But $\varphi\psi$ and $\psi\varphi$ are identities because each fixes every element in a basis, and so $\varphi: F \to G$ is an isomorphism.

Conversely, if p is a prime, then $V = F/pF$ is a vector space over $\mathbb{Z}_p$. We claim that $\overline{X} = \{x + pF: x \in X\}$ is a basis of V. It is clear that $\overline{X}$ spans V. Assume that $\Sigma[m_x](x + pF) = 0$, where $[m_x] \in \mathbb{Z}_p$ and not all $[m_x] = [0]$. If m_x is a representative of $[m_x]$, then $\sum m_x(x + pF) = 0$. In F, this equation becomes $\sum m_x x \in pF$; that is, there are integers n_x with $\sum m_x x = \sum p n_x x$. Independence of a basis gives $m_x = pn_x$ for all x, and so $[m_x] = [0]$ for all x. This contradiction shows that $\overline{X}$ is independent, and hence it is a basis of V. We have shown that $\dim F/pF = |\overline{X}| = |X|$. In a similar way, one shows that $\dim F/pF = |Y|$, so that $|X| = |Y|$. ■

Definition. The ***rank*** of a free abelian group is the cardinal of a basis.

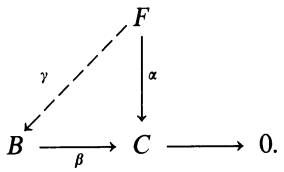
Theorem 10.14 says that two free abelian groups are isomorphic if and only if they have the same rank. The reader will not be misled by the analogy: vector space—free abelian group; dimension—rank.

It is clear that if F and G are free abelian, then

$$\operatorname{rank}(F \oplus G) = \operatorname{rank}(F) + \operatorname{rank}(G),$$

for a basis of $F \oplus G$ can be chosen as the union of a basis of F and a basis of G.

Theorem 10.15 (Projective Property). *Let* $\beta: B \to C$ *be a surjective homomorphism of groups. If* F *is free abelian and if* $\alpha: F \to C$ *is a homomorphism, then there exists a homomorphism* $\gamma: F \to B$ *making the diagram below commute (i.e.,* $\beta\gamma = \alpha$*):*



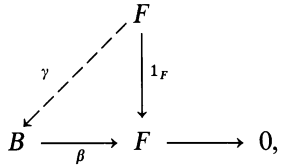
Remark. The converse is also true.

Proof. Let X be a basis of F. For each $x \in X$, surjectivity of α provides $b_x \in B$

with $\beta(b_x) = \alpha(x)$. Define a function $f: X \to B$ by $f(x) = b_x$. By Theorem 10.11 there is a homomorphism $\gamma: F \to B$ with $\gamma(x) = b_x$ for all x. It follows that $\beta\gamma = \alpha$, for they agree on a generating set of F: if $x \in X$, then $\beta\gamma(x) = \beta(b_x) = \alpha(x)$. ■

Corollary 10.16. *If $H \leq G$ and G/H is free abelian, then H is a direct summand of G; that is, $G = H \oplus K$, where $K \leq G$ and $K \cong G/H$.*

Proof. Let $F = G/H$ and let $\beta: G \to F$ be the natural map. Consider the diagram



where 1_F is the identity map. Since F has the projective property, there is a homomorphism $\gamma: F \to B$ with $\beta\gamma = 1_F$. Define $K = \operatorname{im} \gamma$. The equivalence of (i) and (iii) in Lemma 10.3 gives $B = \ker \beta \oplus \operatorname{im} \gamma = H \oplus K$. ■

We give two proofs of the next result. The first is a special case of the second, but it contains the essential idea; the second involves infinite methods which, though routine, may obscure the simple idea.

Theorem 10.17. *Every subgroup H of a free abelian group F of finite rank n is itself free abelian; moreover,* $\operatorname{rank}(H) \leq \operatorname{rank}(F)$.

Proof. The proof is by induction on n. If $n = 1$, then $F \cong \mathbb{Z}$. Since every subgroup H of a cyclic group is cyclic, either $H = 0$ or $H \cong \mathbb{Z}$, and so H is free abelian of rank ≤ 1. For the inductive step, let $\{x_1, \ldots, x_{n+1}\}$ be a basis of F. Define $F' = \langle x_1, \ldots, x_n \rangle$ and $H' = H \cap F'$. By induction, H' is free abelian of rank $\leq n$. Now

$$H/H' = H/(H \cap F') \cong (H + F')/F' \leq F/F' \cong \mathbb{Z}.$$

By the base step, either $H/H' = 0$ or $H/H' \cong \mathbb{Z}$. In the first case, $H = H'$ and we are done; in the second case, Corollary 10.16 gives $H = H' \oplus \langle h \rangle$ for some $h \in H$, where $\langle h \rangle \cong \mathbb{Z}$, and so H is free abelian and $\operatorname{rank}(H) = \operatorname{rank}(H' \oplus \mathbb{Z}) = \operatorname{rank}(H') + 1 \leq n + 1$. ■

We now remove the finiteness hypothesis.

Theorem 10.18. *Every subgroup H of a free abelian group F is free abelian, and* $\operatorname{rank}(H) \leq \operatorname{rank}(F)$.

Proof. That every nonempty set can somehow be well-ordered is equivalent

to the Axiom of Choice (see Appendix IV). Let $\{x_k: k \in K\}$ be a basis of F, and assume that K is well-ordered.

For each $k \in K$, define $F'_k = \langle x_j: j < k\rangle$ and $F_k = \langle x_j: j \leq k\rangle = F'_k \oplus \langle x_k\rangle$; define $H'_k = H \cap F'_k$ and $H_k = H \cap F_k$. Note that $F = \bigcup F_k$ and $H = \bigcup H_k$. Now $H'_k = H \cap F'_k = H_k \cap F'_k$, and so

$$H_k/H'_k = H_k/(H_k \cap F'_k)$$
$$\cong (H_k + F'_k)/F'_k \leq F_k/F'_k \cong \mathbb{Z}.$$

By Corollary 10.16, either $H_k = H'_k$ or $H_k = H'_k \oplus \langle h_k\rangle$, where $\langle h_k\rangle \cong \mathbb{Z}$. We claim that H is free abelian with basis the set of all h_k; it will then follow that $\operatorname{rank}(H) \leq \operatorname{rank}(F)$, for the set of h_k has cardinal $\leq |K| = \operatorname{rank}(F)$.

Since $F = \bigcup F_k$, each $h \in H$ (as any element of F) lies in some F_k; define $\mu(h)$ to be the smallest index k for which $h \in F_k$ (we are using the fact that K is well-ordered). Let H^* be the subgroup of H generated by all the h_k. Suppose that H^* is a proper subgroup of H. Let j be the smallest index in

$$\{\mu(h): h \in H \text{ and } h \notin H^*\},$$

and choose $h' \in H$, $h' \notin H^*$ with $\mu(h') = j$. Now $\mu(h') = j$ gives $h' \in H \cap F_j$, so that

$$h' = a + mh_j, \qquad a \in H'_j \quad \text{and} \quad m \in \mathbb{Z}.$$

Thus, $a = h' - mh_j \in H$, $a \notin H^*$ (lest $h' \in H^*$), and $\mu(a) < j$, a contradiction. Therefore, $H = H^*$.

By Lemma 10.4(ii), it remains to show that linear combinations of the h_k are unique. It suffices to show that if

$$m_1 h_{k_1} + \cdots + m_n h_{k_n} = 0,$$

where $k_1 < \cdots < k_n$, then each $m_i = 0$. Of course, we may assume that $m_n \neq 0$. But then $m_n h_{k_n} \in \langle h_{k_n}\rangle \cap H'_{k_n} = 0$, a contradiction. It follows that H is free abelian. ■

Exercises

10.5. (i) Prove, for each $n \geq 1$, that $\mathbb{Z}(p^\infty)$ has a unique subgroup of order p^n.
(ii) Prove that the set of all subgroups of $\mathbb{Z}(p^\infty)$ is well-ordered by inclusion.
(iii) Prove that $\mathbb{Z}(p^\infty)$ has the DCC but not the ACC.
(iv) Let $R_p = \{e^{2\pi ik/p^n}: k \in \mathbb{Z}, n \geq 0\} \leq \mathbb{C}$ be the multiplicative group of all pth power roots of unity. Prove that $\mathbb{Z}(p^\infty) \cong R_p$.

10.6. (i) Prove that the group G having generators $\{x_0, x_1, x_2, \ldots\}$ and relations $\{px_0, x_0 - p^n x_n, \text{all } n \geq 1\}$ is an infinite p-primary group with $\bigcap_{n=1}^{\infty} p^n G \neq 0$.
(ii) Prove that the group G in (i) is not isomorphic to $\mathbb{Z}(p^\infty)$.

10.7. (i) Prove that an abelian group G is finitely generated if and only if it is a quotient of a free abelian group of finite rank.

(ii) Every subgroup H of a finitely generated abelian group G is itself finitely generated. Moreover, if G can be generated by r elements, then H can be generated by r or fewer elements.

10.8. Prove that the multiplicative group of positive rationals is free abelian (of countably infinite rank). (*Hint.* Exercise 1.52(ii).)

10.9. If F is a free abelian group of rank n, then $\mathrm{Aut}(F)$ is isomorphic to the multiplicative group of all $n \times n$ matrices over $\mathbb{Z}$ with determinant $= \pm 1$.

10.10. An abelian group is free abelian if and only if it has the projective property.

10.11. If F is a free abelian group of rank n and H is a subgroup of rank $k < n$, then F/H has an element of infinite order.

10.12. (i) If $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ is an exact sequence of free abelian groups, prove that $B \cong \mathrm{im}\, f \oplus \ker h$.

(ii) If $n \geq 1$ and $0 \to F_n \to \cdots \to F_1 \to F_0 \to 0$ is an exact sequence of free abelian groups of finite rank, then $\sum_{i=0}^{n} \mathrm{rank}(F_i) = 0$.

10.13. Prove the converse of Corollary 10.16: If a group G is (isomorphic) to a direct summand whenever it is a homomorphic image, then G is free abelian.

10.14. A torsion-free abelian group G having a free abelian subgroup of finite index is itself free abelian.

Finitely Generated Abelian Groups

We now classify all finitely generated abelian groups.

Theorem 10.19. *Every finitely generated torsion-free abelian group G is free abelian.*

Proof. We prove the theorem by induction on n, where $G = \langle x_1, \ldots, x_n \rangle$. If $n = 1$ and $G \neq 0$, then G is cyclic; $G \cong \mathbb{Z}$ because it is torsion-free.

Define $H = \{g \in G: mg \in \langle x_n \rangle \text{ for some positive integer } m\}$. Now H is a subgroup of G and G/H is torsion-free: if $x \in G$ and $k(x + H) = 0$, then $kx \in H$, $m(kx) \in \langle x_n \rangle$, and so $x \in H$. Since G/H is a torsion-free group that can be generated by fewer than n elements, it is free abelian, by induction. By Corollary 10.16, $G = F \oplus H$, where $F \cong G/H$, and so it suffices to prove that H is cyclic. Note that H is finitely generated, being a summand (and hence a quotient) of the finitely generated group G.

If $g \in H$ and $g \neq 0$, then $mg = kx_n$ for some nonzero integers m and k. It is routine to check that the function $\varphi: H \to \mathbb{Q}$, given by $g \mapsto k/m$, is a well defined injective homomorphism; that is, H is (isomorphic to) a finitely generated subgroup of $\mathbb{Q}$, say, $H = \langle a_1/b_1, \ldots, a_t/b_t \rangle$. If $b = \prod_{i=1}^{t} b_i$, then the map $\psi: H \to \mathbb{Z}$, given by $h \mapsto bh$, is an injection (because H is torsion-free). There-

fore, H is isomorphic to a nonzero subgroup of $\mathbb{Z}$, and hence it is infinite cyclic. ■

Theorem 10.20 (Fundamental Theorem). *Every finitely generated abelian group G is a direct sum of primary and infinite cyclic groups, and the number of summands of each kind depends only on G.*

Proof. Theorem 10.19 shows that G/tG is free abelian, so that Corollary 10.16 gives $G = tG \oplus F$, where $F \cong G/tG$. Now tG is finitely generated, being a summand and hence a quotient of G, and Exercise 6.18(ii) shows that tG is finite. The basis theorem for finite abelian groups says that tG is a direct sum of primary cyclic groups.

The uniqueness of the number of primary cyclic summands is precisely Theorem 6.11; the number of infinite cyclic summands is just $\operatorname{rank}(G/tG)$, and so it, too, depends only on G. ■

The next result will give a second proof of the basis theorem.

Theorem 10.21 (Simultaneous Bases). *Let H be a subgroup of finite index in a free abelian group F of finite rank n. Then there exist bases $\{y_1, \ldots, y_n\}$ of F and $\{h_1, \ldots, h_n\}$ of H such that $h_i \in \langle y_i \rangle$ for all i.*

Proof. If $\{x_1, \ldots, x_n\}$ is an ordered basis of F, then each element $h \in H$ has coordinates. Choose an ordered basis and an element h so that, among all such choices, the first coordinate of h is positive and minimal such. If $h = k_1x_1 + \cdots + k_nx_n$, then we claim that k_1 divides k_i for all $i \geq 2$. The division algorithm gives $k_i = q_ik_1 + r_i$, where $0 \leq r_i < k_1$. Therefore,

$$h = k_1(x_1 + q_2x_2 + \cdots + q_nx_n) + r_2x_2 + \cdots + r_nx_n.$$

Define $y_1 = x_1 + q_2x_2 + \cdots + q_nx_n$, and note that $\{y_1, x_2, \ldots, x_n\}$ is an ordered basis of F. Now $h = k_1y_1 + r_2x_2 + \cdots + r_nx_n$. If $r_i \neq 0$ for some i, then the first coordinate of h relative to the ordered basis $\{x_i, y_1, \ldots, x_n\}$ violates the minimality of our initial choice. Therefore, $r_i = 0$ for all $i \geq 2$ and k_1 divides k_i for all $i \geq 2$.

If $h' = m_1y_1 + m_2x_2 + \cdots + m_nx_n$ is any element of H, we claim that k_1 divides m_1. For if $m_1 = qk_1 + r$, where $0 \leq r < k_1$, then $h' - qh \in H$ has first coordinate $r < k_1$, a contradiction. It follows that the map $\pi: H \to H$, given by $h' \mapsto m_1y_1$, is a retraction with image $\langle h \rangle$. By Lemma 10.3, $H = \langle h \rangle \oplus \ker \pi = \langle h \rangle \oplus (H \cap \langle x_2, \ldots, x_n \rangle)$. Since $\langle x_2, \ldots, x_n \rangle$ is free abelian of rank $n - 1$ and $H \cap \langle x_2, \ldots, x_n \rangle$ is a subgroup of finite index, the proof can be completed by induction on n. ■

Corollary 10.22 (Basis Theorem). *Every finite abelian group G is a direct sum of cyclic groups.*

Proof. Write G as F/R, where F is free abelian of finite rank n, say. By Theorem 10.21, there are bases $\{y_1, \ldots, y_n\}$ and $\{h_1, \ldots, h_n\}$ of F and R, respectively, with $h_i = k_i y_i$ for all i. By Theorem 2.30, $G \cong \sum_{i=1}^{n} \mathbb{Z}_{k_i}$. ■

EXERCISES

10.15. If F is a free abelian group of finite rank n, then a subgroup H of F has finite index if and only if H is free abelian of rank n.

10.16. Let $\{x_1, \ldots, x_n\}$ be a basis of a free abelian group F. If $k_1, \ldots, k_n$ are integers with $\gcd(k_1, \ldots, k_n) = 1$, then there are elements $y_2, \ldots, y_n$ such that $\{k_1 x_1 + \cdots + k_n x_n, y_2, \ldots, y_n\}$ is a basis of F.

10.17. Let F be free abelian of rank n and let H be a subgroup of the same rank. Let $\{x_1, \ldots, x_n\}$ be a basis of F, let $\{y_1, \ldots, y_n\}$ be a basis of H, and let $y_j = \sum m_{ij} x_i$. Prove that

$$[F : H] = |\det[m_{ij}]|.$$

(*Hint.* Show that $|\det[m_{ij}]|$ is independent of the choice of bases of F and of H.)

Divisible and Reduced Groups

A reader of Chapter 1, asked to give examples of infinite abelian groups, probably would have responded with $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. We now study a common generalization of the latter three groups.

Definition. A group G is ***divisible*** if each $x \in G$ is divisible by every integer $n \geq 2$; that is, there exists $g_n \in G$ with $ng_n = x$ for all $n \geq 2$.

EXAMPLE 10.5. The following groups are divisible: $\mathbb{Q}$; $\mathbb{R}$; $\mathbb{C}$; the circle group $\mathbf{T}$; $\mathbb{Z}(p^\infty)$; the multiplicative group $F^\times$ of all nonzero elements of an algebraically closed field F (in particular, $\mathbb{C}^\times$).

EXAMPLE 10.6. Every quotient of a divisible group is divisible.

EXAMPLE 10.7. If $\{A_k : k \in K\}$ is a family of groups, Then each of $\sum_{k \in K} A_k$ (and $\prod_{k \in K} A_k$) is divisible if and only if every A_k is divisible.

EXAMPLE 10.8. A torsion-free divisible group G is a vector space over $\mathbb{Q}$.

If $x \in G$ and $n > 0$, then there is a unique $y \in G$ with $ny = x$, by Exercise 10.2. There is thus a function $\mathbb{Q} \times G \to G$, given by $(m/n, x) \mapsto my$ (where $ny = x$), which is a scalar multiplication satisfying the axioms in the definition of vector space.

Theorem 10.23 (Injective Property, Baer, 1940). *Let D be a divisible group and let A be a subgroup of a group B. If $f : A \to D$ is a homomorphism, then f*