NOTES ON ALGEBRA

Marc Culler - Fall 2004

1. Groups

Definition 1.1. A *group* is a set G together with a binary operation $\cdot : G \times G \to G$ such that

G1 $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ for all $g, h, k \in G$;

G2 there exists an element $e \in G$ such that $e \cdot g = g = g \cdot e$ for all $g \in G$;

G3 there exists a function $\mathrm{inv} : G \to G$ such that $\mathrm{inv}\, g \cdot g = g \cdot \mathrm{inv}\, g = e$ for all $g \in G$.

The element e is the *identity* of G and $\mathrm{inv}\, g$ is the *inverse* of g. Elements g and h of G *commute* if $g \cdot h = h \cdot g$.

Definition 1.2. A group $(G, \cdot)$ is said to be *abelian* if it satisfies

Ab $g \cdot h = h \cdot g$ for all $g, h \in G$.

Proposition 1.3. *Let $(G, \cdot)$ be a group and let $g \in G$.*

(1) If x is an element of G such that $g \cdot x = g$ or $x \cdot g = g$ then $x = e$;

(2) if x is an element of G such that $g \cdot x = e$ or $x \cdot g = e$ then $x = \mathrm{inv}\, g$.

Exercise 1.1. Prove 1.3.

Proposition 1.4. *Let $(G, \cdot)$ be a group. Then*

(1) $\mathrm{inv}(\mathrm{inv}\, g) = g$ for all $g \in G$;

(2) $inv(g \cdot h) = \mathrm{inv}\, h \cdot \mathrm{inv}\, g$ for all $g, h \in G$.

Exercise 1.2. Prove Proposition 1.4.

1.5. From now on we will omit the name of the operation and write "G is a group" when we mean $(G, \cdot)$ is a group. We will usually omit the operation in formulas, writing gh in place of $g \cdot h$. We may refer to a a set X of elements of a group G as a *subset* of G, and write $X \subset G$.

Date: September 8, 2005.

Exercise 1.3. Let $(G, \cdot)$ be a group and suppose that $g_1, \ldots, g_n$ are elements of G. Define what is meant by a "bracketing" of the expression $g_1 g_2 \cdots g_n$, and by an "evaluation" of a bracketing. Show that every bracketing of $g_1 g_2 \cdots g_n$ evaluates to the same element of G.

1.6. Suppose that $(G, \cdot)$ is a group and $g \in G$. Define $g^0 = e$, $g^1 = g$, and $g^{-1} = \operatorname{inv} g$. For any integer n with $|n| > 1$, define g^n inductively as follows:

$$g^n = g^{n-1} \cdot g \text{ for } n > 1$$
$$g^n = g^{n+1} \cdot g^{-1} \text{ for } n < -1$$

Exercise 1.4. Let $(G, \cdot)$ be a group and $g \in G$. Show that $g^n \cdot g^m = g^{n+m}$ for all integers m and n, and that $(g^n)^{-1} = g^{-n}$ for all integers n.

Exercise 1.5. Let G be an abelian group. Show that $(gh)^n = g^n h^n$ for all $g, h \in G$ and all integers n.

Definition 1.7. If G is a group with a finite number of elements then G is a *finite group*. The *order* of G is the number of elements of G, and is denoted $|G|$. If G has infinitely many elements then G is an *infinite group*, and we write $|G| = \infty$.

2. Subgroups

Proposition 2.1. *Let $(G, \cdot)$ be a group and let H be a non-empty subset of G such that*

(i) $a \cdot b \in H$ *for all* $a, b \in H$;

(ii) $\operatorname{inv} a \in H$ *for all* $a \in H$.

Then $\cdot : G \times G \to G$ sends $H \times H$ into H, so the restriction of $\cdot$ to $H \times H$ (still denoted by $\cdot$) is a binary operation on H, and $(H, \cdot)$ is a group.

Exercise 2.1. Prove 2.1.

Definition 2.2. In the situation of Proposition 2.1 we say that H is a *subgroup* of G and write $H \leq G$, or $H < G$ in case $H \leq G$ and $H \neq G$.

Exercise 2.2. Let G be a group. Show that the intersection of any nonempty family of subgroups of G is a subgroup of G.

Definition 2.3. Let G be a group and let X be any set of elements of G. Define $\langle X \rangle$ to be the intersection of all subgroups of G that contain X. (This is a nonempty family since G is a subgroup of G.) If $X = \{x_1, \ldots, x_n\}$ then we may denote $\langle X \rangle$ as $\langle x_1, \ldots, x_n \rangle$ (instead of $\langle \{x_1, \ldots, x_n\} \rangle$).

Exercise 2.2 implies that $\langle X \rangle$ is a subgroup of G, and it is clearly the smallest subgroup of G that contains X. Note that $\langle \emptyset \rangle = \{e\}$.

Exercise 2.3. Let G be a group and let X be any set of elements of G. Show that $\langle X \rangle$ consists of all elements $g \in G$ such that $g = g_1 \cdots g_k$, where $g_1, \ldots, g_k$ are elements of $X \cup \mathrm{inv}(X)$.

Definition 2.4. A group G is *cyclic* if $G = \langle a \rangle$ for some $a \in G$.

Definition 2.5. A set X of elements of G *generates* G if $\langle X \rangle = G$.

Definition 2.6. A subgroup H of a group G is *proper* if $H \neq \{e\}$ and $H \neq G$.

Exercise 2.4. Show that a group which has no proper subgroups is cyclic.

Problem 2.5. Show that a group cannot be the union of two proper subgroups. Give an example of a group that is the union of three proper subgroups.

Definition 2.7. If a is an element of a group G then the *order of* a is defined to be the order of the subgroup $\langle a \rangle$, and is written $|a|$.

Exercise 2.6. Let a be an element of a group G. Show that if $|a| = \infty$ then $a^n = a^m$ if and only if $n = m$. Show that if $|a| = n < \infty$ then $a^n = e$ and $a, a^2, \ldots, a^{n-1}$ are all distinct elements of G. Show that if $a^m = e$ for some integer m then $|n|$ divides m.

3. Group homomorphisms

Definition 3.1. Suppose that G and H are groups. A function $\phi\colon G \to H$ is a *homomorphism* if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. A homomorphism $\phi\colon G \to H$ is an *isomorphism* if there exists a homomorphism $\psi\colon H \to G$ such that $\psi \circ \phi = \mathrm{id}_G$ and $\phi \circ \psi = \mathrm{id}_H$. An isomorphism from G to G is an *automorphism* of G.

Exercise 3.1. A homomorphism of groups $\phi\colon G \to H$ is an isomorphism if and only if it is a bijection.

Exercise 3.2. Show that if $\phi\colon G \to H$ is a homomorphism of groups then $\phi(e) = e$ and $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.

Exercise 3.3. Let G be a group and let $\mathrm{Aut}\, G$ denote the set of all automorphisms of G together with the composition operation. Show that $\mathrm{Aut}\, G$ is a group.

Exercise 3.4. Let $\mathcal{C}$ be a category. If A and B are objects of $\mathcal{C}$ and α is a morphism from A to B, we will say that α is an *isomorphism* if there exists a morphism β from B to A such that $\beta \circ \alpha = \mathrm{id}_A$ and $\alpha \circ \beta = \mathrm{id}_B$. An isomorphism from A to A is called an *automorphism* of A. Let $\mathrm{Aut}\, A$ denote the set of automorphims of A together with the composition operation. Show that $\mathrm{Aut}\, A$ is a group.

Definition 3.2. Suppose that G and H are groups and $\phi\colon G \to H$ is a homomorphism. Set

$$\ker \phi = \{g \in G \mid \phi(g) = e\}$$
$$\mathrm{im}\, \phi = \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}$$

Proposition 3.3. *Let $\phi\colon G \to H$ be a homomorphism of groups. Then $\ker \phi$ is a subgroup of G and $\mathrm{im}\, \phi$ is a subgroup of H.*

Exercise 3.5. Prove 3.3.

Problem 3.6. Let G be a group such that $(ab)^2 = a^2b^2$ for all $a, b \in G$. Show that G is abelian.

Problem 3.7. Let G be a group. Suppose there are three consecutive integers n such that $(ab)^n = a^n b^n$ for all $a, b \in G$. Show that G is abelian.

Problem 3.8. Show that all groups with 1, 2, 3 or 4 elements are abelian.

4. Cosets

Proposition 4.1. *Let H be a subgroup of a group G. Define two relations on G as follows:*

- $a \underset{L}{\sim} b$ *if* $a^{-1}b \in H$;
- $a \underset{R}{\sim} b$ *if* $ab^{-1} \in H$.

Both $\underset{L}{\sim}$ and $\underset{R}{\sim}$ are equivalence relations. Moreover, the equivalence class of $\underset{L}{\sim}$ containing $a \in G$ is the set $aH \doteq \{ah \mid h \in H\}$, and the equivalence class of $\underset{R}{\sim}$ containing $a \in G$ is the set $Ha \doteq \{ha \mid h \in H\}$.

Exercise 4.1. Prove Proposition 4.1.

Definition 4.2. If H is a subgroup of a group G then the sets of the form $aH \doteq \{ah \mid h \in H\}$ are called *left cosets* of H in G and the sets of the form $Ha \doteq \{ha \mid h \in H\}$ are called *right cosets* of H in G The set of left cosets of H in G is denoted G/H and the set of right cosets of H in G is denoted $H\backslash G$

Corollary 4.3. *Let H be a subgroup of a group G. The left (right) cosets of H in G form a partition of G into disjoint subsets.*

Definition 4.4. Suppose that H is a subgroup of a group G and that there are only finitely many left cosets of H in G. Then the number of left cosets of H in G is denoted $[G : H]$, and is called the *index of H in G*. If there are infinitely many left cosets of H in G then we say *H has infinite index in G* and write $[G : H] = \infty$.

Proposition 4.5. *Let H be a subgroup of G. Any two left (right) cosets of H in G are in one-to-one correspondence.*

Exercise 4.2. Prove Proposition 4.5.

Theorem 4.6. *(Lagrange's Theorem) If G is a finite group and H is a subgroup of G then $|G| = |H|[G : H]$. In particular, $|H|$ and $[G : H]$ are divisors of $|G|$.*

Proof. By Proposition 4.1 the left cosets of H in G form a partition of the elements of G into disjoint subsets. By Proposition 4.5 each left coset has the same number of elements. Moreover, since the coset eH is equal (as a set) to H, every left coset of H in G has $|H|$ elements. Thus $|G| = n|H|$ where $n = [G : H]$ is the number of left cosets of H in G. □

Exercise 4.3. Suppose that H is a subgroup of G. Show that there is a one-to-one correspondence between the left cosets of H in G and the right cosets of H in G. In particular, the number of right cosets of H in G is also given by $[G : H]$.

Exercise 4.4. Show that a group of prime order is cyclic.

Exercise 4.5. Let G be a group. Suppose that $H_1, \ldots, H_k$ are subgroups of finite index in G, for some positive integer k. Show that $H_1 \cap \cdots \cap H_k$ is a subgroup of finite index in G.

5. Normal subgroups and quotients

Definition 5.1. Suppose that $\phi\colon G \to H$ is a homomorphism. If $h \in \operatorname{im}\phi \leq H$ then the *fiber of ϕ over h* is the set

$$\phi^{-1}(h) \doteq \{g \in G \mid \phi(g) = h\} \subseteq G.$$

5.2. Suppose that $\phi\colon G \to H$ is a homomorphism. We have seen that $\ker\phi$ and $\operatorname{im}\phi$ are subgroups of G and H respectively. Here are some observations about this situation that should be kept in mind:

- The subgroup $\ker\phi \leq G$ has the following additional property: if $x \in \ker\phi$ then $gxg^{-1} \in \ker\phi$ for all $g \in G$. (We have $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1}$ and $\phi(g)\phi(x)\phi(g)^{-1} = e \Leftrightarrow \phi(x) = e$.)

- There is a one-to-one correspondence $h \leftrightarrow \phi^{-1}(h)$ between the set of elements of the subgroup $\operatorname{im}\phi \leq H$ and the set of fibers of ϕ over elements of $\operatorname{im}\phi$.
- Two elements a and b of G lie in the same fiber of ϕ if and only if $ab^{-1} \in \ker\phi$. (We have $\phi(a) = \phi(b) \Leftrightarrow \phi(ab^{-1}) = e$.)

Definition 5.3. A subgroup H of a group G is said to be *normal* if $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. If H is a normal subgroup of G we write $H \trianglelefteq G$, or $H \triangleleft G$ if $H \neq G$.

Exercise 5.1. If G is an abelian group then every subgroup of G is normal.

Exercise 5.2. If $N \trianglelefteq G$ then $gN = Ng$ for all $g \in G$.

5.4. In view of the previous exercise, we will not distinguish between left and right cosets of a normal subgroup. Also, the exercise implies that the equivalence relations $\underset{L}{\sim}$ and $\underset{R}{\sim}$ are identical in the case of a normal subgroup.

Exercise 5.3. Show that $N \trianglelefteq G$ if and only if $N = gNg^{-1} \doteq \{gng^{-1} \mid n \in N\}$ for all $g \in G$.

Problem 5.4. Show that any subgroup of index 2 is normal.

Problem 5.5. Suppose that a group G has a subgroup H of finite index. Show that G has a normal subgroup of finite index which is contained in H.

Proposition 5.5. *Suppose that N is a normal subgroup of a group G and let Q denote the set of cosets of N in G. There is an operation $\cdot : Q \times Q \to Q$ such that $aN \cdot bN = (ab)N$ for all $a, b \in G$, and Q forms a group under this operation. In particular, the function $\pi : G \to Q$ given by $\pi(g) = gN$ is a surjective homomorphism.*

Proof. Since the equivalence relations $\underset{L}{\sim}$ and $\underset{R}{\sim}$ are identical, according to 5.4, we drop the subscripts and write $x \sim y$ if $xy^{-1} \in N$. We will show that if $a_1 \sim a_2$ and $b_1 \sim b_2$ then $a_1 b_1 \sim a_2 b_2$. This implies that if $a_1 N = a_2 N$ and $b_1 N = b_2 N$ then $a_1 b_1 N = a_2 b_2 N$. In particular we obtain a well-defined operation on cosets by setting $aN \cdot bN = abN$.

Suppose that $a_1 \sim a_2$ and $b_1 \sim b_2$. Then $a_1 = a_2 n$ and $b_1 = b_2 n'$ for some $n, n' \in N$. Now

$$a_1 b_1 = a_2 n b_2 n' = a_2 b_2 (b_2^{-1} n b n').$$

Since $b_2^{-1} n b \in N$ and $n' \in N$ we have $a_1 b_1 \sim a_2 b_2$, as required.

It is clear from the definition that the operation $\cdot$ is associative. To show that Q forms a group under the operation $\cdot$ we take the coset N to be the identity element e of Q and we set $\operatorname{inv} aN = a^{-1}N$. Since $aN \cdot N = aN = N \cdot aN$, and $aN \cdot a^{-1}N = N = a^{-1}N \cdot aN$, the group axioms hold with these choices of e and inv. $\square$

Definition 5.6. Let $N \trianglelefteq G$. The group given by Proposition 5.5 is called the *quotient of G by N* and is usually denoted G/N. (This is the same as the notation for the set of left cosets, but in the case that N is normal the set of cosets is understood to comee equipped with the operation given by Proposition 5.5.) The surjective homomorphism $\pi\colon G \to G/N$ defined by $\pi(g) = gN$ is called the *quotient homomorphism* or the *natural homomorphism*.

6. Conjugacy, normalizers, centralizers, and centers

Definition 6.1. Let G be a group. Two elements $a, b \in G$ are *conjugate* if $gag^{-1} = b$ for some $g \in G$.

Exercise 6.1. Conjugacy is an equivalence relation on the set of elements of any group. In particular, the conjugacy classes form a partition of the elements of a group into disjoint subsets.

Definition 6.2. The equivalence classes under the conjugacy relation are called *conjugacy classes*.

Definition 6.3. If A is any nonempty set of elements of group G then the *normalizer* of A in G is

$$N_G(A) \doteq \{g \in G \mid gAg^{-1} = A\}.$$

Exercise 6.2. If A is any nonempty set of elements of a finite group G then

$$N_G(A) = \{g \in G \mid gAg^{-1} \subset A\}.$$

Give an example of an infinite group where this fails.

Exercise 6.3. Suppose G is a group and H and K are subgroups of G such that $H \leq K \leq G$. Show that $H \trianglelefteq K$ if and only if $K \leq N_G(H)$.

Definition 6.4. If A is any nonempty set of elements of a group G then the *centralizer* of A in G is

$$C_G(A) \doteq \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}.$$

We use a different notation for the centralizer of a singleton: $C_G(a) \doteq C_G(\{a\})$.

Exercise 6.4. If A is any non-empty set of elements of a group G then $C_G(A)$ is a subgroup of G.

Definition 6.5. The *center* of a group G is the subgroup

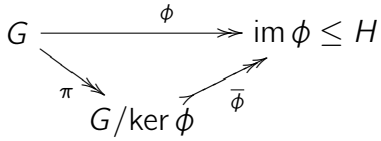
$$Z(G) \doteq C_G(G) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in G\}.$$

That is, the center consists of all elements that commute with every element of G.

Exercise 6.5. The center of a group G is a normal subgroup of G.

7. Isomorphism Theorems

Theorem 7.1 (First Isomorphism Theorem)**.** *Let $\phi\colon G \to H$ be a homomorphism of groups. There is an isomorphism $\overline{\phi}\colon G/ker\phi \to \operatorname{im}\phi$ such that $\overline{\phi}\circ\pi = \phi$, where $\pi\colon G \to G/\ker\phi$ denotes the quotient homomorphism. In other words, the following diagram commutes:*



Proof. Suppose that a and b are contained in the same coset of $\ker\phi$. Then $a = bk$ for some $k \in \ker\phi$ and hence $\phi(a) = \phi(bk) = \phi(b)e = \phi(b)$. We may therefore define $\overline{\phi}(a\ker\phi) = \phi(a)$. It is clear that $\overline{\phi}\circ\pi = \phi$ and that $\operatorname{im}\overline{\phi} = \operatorname{im}\phi$. It remains to show that $\overline{\phi}$ is an injective homomorphism. To see that $\overline{\phi}$ is a homomorphism, observe that

$$\overline{\phi}(a\ker\phi \cdot b\ker\phi) = \overline{\phi}(ab\ker\phi) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(a\ker\phi)\cdot\overline{\phi}(b\ker\phi).$$

To see that $\overline{\phi}$ is injective, observe that

$$\begin{aligned}
\overline{\phi}(a\ker\phi) = \overline{\phi}(b\ker\phi) &\Leftrightarrow \phi(a) = \phi(b)\\
&\Leftrightarrow \phi(ab^{-1}) = e\\
&\Leftrightarrow ab^{-1} \in \ker\phi\\
&\Leftrightarrow a\ker\phi = b\ker\phi.
\end{aligned}$$

□

Exercise 7.1. Let $\mathbb{Z}$ denote the group of integers under addition. Show that $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group, and that every cyclic group is isomorphic either to $\mathbb{Z}$, or to $\mathbb{Z}/n\mathbb{Z}$ for some non-zero integer n. The name C_n will be reserved for a finite cyclic group of order n.

Definition 7.2. Suppose that G is a group and that X and Y are subsets of G. We define the subset XY of G as

$$XY = \{xy \mid x \in X \text{ and } y \in Y\}.$$

Exercise 7.2. Suppose that H is a normal subgroup of a group G. Let $A = aH$ and $B = bH$ be two cosets of H. Show that $AB = abH$. (This gives an alternative definition of the operation in the quotient group G/H.)

If H and K are arbitrary subgroups of a group G, there is no reason to expect that HK will be a subgroup of G. However, the following proposition shows that HK is a subgroup if H normalizes K.

Proposition 7.3. *Suppose that H and K are subgroups of a group G and that $H \leq N_G(K)$. Then HK is a subgroup of G, and $HK = \langle H \cup K \rangle$.*

Exercise 7.3. Prove Proposition 7.3

Theorem 7.4 (Second Isomorphism Theorem)**.** *Suppose that H and K are subgroups of a group G and that $H \leq N_G(K)$. Then $K \trianglelefteq HK$, $H \cap K \trianglelefteq H$ and HK/K is isomorphic to $H/H \cap K$.*

Proof. Since $H \leq N_G(K)$ and $K \leq N_G(K)$ it follows that $HK \leq N_G(K)$ and hence that K is a normal subgroup of HK. Similarly, it follows that $hKh^{-1} = K$ and $hHh^{-1} = H$ for all $h \in H$, and hence that $h(H \cap K)h^{-1} = H \cap K$. Thus $H \cap K$ is a normal subgroup of H.

Clearly HK is the union of all cosets hK for $h \in H$. Given elements $h \in H$, $k \in K$, their product hk is an element of H if and only if $k \in H \cap K$. Therefore $hK \cap H = h(K \cap H)$ for every coset hK of K.

We define $\phi\colon HK/K \to H/H \cap K$ by $\phi(hK) = hK \cap H = h(K \cap H)$. It is easy to check that ϕ is an isomorphism. □

Exercise 7.4. Let H and K be subgroups of a group G. Show that

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

regardless of whether HK is a subgroup of G.

Theorem 7.5 (Third Isomorphism Theorem)**.** *Let G be a group and let N and K be normal subgroups of G with $N \leq H \leq G$. Then $H/N \trianglelefteq G/N$ and G/H is isomorphic to $(G/N)/(H/N)$.*

Proof. Define a homomorphism $\phi\colon G/N \to G/H$ by $\phi(gN) = gH$. The map is well-defined since $gN \subset gH$ and gH is the unique coset of H that contains gN. It is clear from the definition that ϕ is a surjective homomorphism. Moreover, $\phi(gN) = H$ if and only if $g \in H$, so $\ker\phi = H/N$. The result now follows from the First Isomorphism Theorem. □

Theorem 7.6 (Correspondence Theorem)**.** *Let G be a group and N a normal subgroup of G. There is a one-to-one correspondence between subgroups of G/N and subgroups of G containing N, given by $H \leftrightarrow H/N$ for $N \leq H \leq G$. This correspondence (in both*

directions) takes normal subgroups to normal subgroups and finite index subgroups to subgroups of the same index.

Exercise 7.5. Prove the Correspondence Theorem.

8. Group Actions

Definition 8.1. If X is a set, we define $S(X)$ to be the set of bijections from X to X, together with the operation of composition. Note that $S(X)$ is a group, by Exercise 3.4. The group $S(X)$ is called the *group of permutations* of X. As a shortcut, we write S_n for the group of permutations of the set $\{1, \ldots, n\} \subset \mathbb{Z}$.

Definition 8.2. A *left action* of a group G on a set X is a homomorphism from G to $S(X)$. (More generally, a left action of a group G on an object X of a category $\mathcal{C}$ is a homomorphism from G to $\operatorname{Aut} X$.)

When a homomorphism from G to $S(X)$ is regarded as a left action of G on X, it is customary to say that X is a left G-set, without giving a name to the homomorphism, and to write $g \cdot x$ or gx in place of $(\phi(g))(x)$, for $g \in G$ and $x \in X$.

Definition 8.3. An *mohomorphism* from a group G to a group H is is function $\psi \colon G \to H$ such that $\psi(gh) = \psi(h)\psi(g)$ for all $g, h \in G$. A *right action* of a group G on a set X is an mohomorphism from G to $S(X)$. When a mohomorphism ψ is regarded as a right action we write $x \cdot g$ in place of $\psi(g)(x)$, for $g \in G$ and $x \in X$.

WARNING: The traditional terminology for a mohomorphism is *antihomomorphism*.

8.4. If X is a left G-set then

- $e \cdot x = x$ for all $x \in X$;
- $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and $x \in X$.

8.5. If X is a right G-set then

- $x \cdot e = x$ for all $x \in X$;
- $x \cdot (gh) = (x \cdot g) \cdot h$ for all $g, h \in G$ and $x \in X$.

8.6. A *G-set* or an *action* will be understood to mean a left G-set or a left action, if no side is specified. It is the reader's job to reformulate statements about left actions as statements about right actions.

Definition 8.7. Suppose that X is a G-set. The *orbit* of $x \in X$ is the subset

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

The *stabilizer* of x is the subgroup

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

An action, or a G-set, is *transitive* if there is only one orbit.

The *kernel* of an action of G on X is, tautologically, the kernel of the action *qua* a homomorphism: that is, $\{g \in G \mid g \cdot x = x \text{ for all } x \in X\}$. An action is *faithful* if it has a trivial kernel.

An action of a group G on X is *free* if $G_x = \{e\}$ for all $x \in X$.

Exercise 8.1. If G is a group and X is a G-set then the orbits form a partition of X.

Proposition 8.8. *Let G be a group, let X be a G-set and let $x \in X$. There is a one-to-one correspondence between the orbit $G \cdot x$ and the set G/G_x of left cosets of the stabilizer of x, given by*

$$g \cdot x \leftrightarrow gG_x.$$

Exercise 8.2. Prove Proposition 8.8

8.9. Here is a list of important G-sets that are naturally associated to a group G.

- The set of elements of a group G forms a left (right) G-set under left (right) multiplication:

  $$g \cdot x = gx \quad (x \cdot g = xg) \qquad \text{for all } g, x \in G.$$

  These are free, transitive actions.

- The set of elements of a group G forms a left (right) G-set under left (right) conjugation:

  $$g \cdot x = gxg^{-1} \quad (x \cdot g = g^{-1}xg) \qquad \text{for all } g, x \in G.$$

  The orbits under either conjugation action are the conjugacy classes in G. The stabilizer of an element $x \in G$ is $C_G(x)$.

- If $H \leq G$ then the left (right) cosets of H form a left (right) G-set under left (right) multiplication:

  $$g \cdot xH = gxH \quad (Hx \cdot g = Hxg) \qquad \text{for all } g, x \in G.$$

  These are transitive actions. The stabilizer of xH (Hx) is xHx^{-1} ($x^{-1}Hx$).

- The set of subgroups of G forms a left (right) G-set under left (right) conjugation:

  $$g \cdot H = gHg^{-1} \quad (H \cdot g = g^{-1}Hg) \qquad \text{for all } g, x \in G.$$

  The orbit of H is the conjugacy class of H. The stabilizer of H is $N_G(H)$.

Exercise 8.3. Let G be a finite group. If $g \in G$ then the number of elements in the conjugacy class of g is equal to $[G : C_G(g)]$. If $H \leq G$ then the number of conjugates of H is equal to $[G : N_G(H)]$.

Theorem 8.10 (The Class Equation)**.** *Let G be a finite group and let $\{C_1, \ldots, C_k\}$ be the set of all conjugacy classes in G which contain more than one element. For $i = 1, \ldots, k$, choose $g_i \in C_i$. Then $[G : C_G(g_i)] > 1$ for each i and*

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

Moreover, each term in the sum is a divisor of $|G|$.

Exercise 8.4. Interpret the fact that the orbits of the conjugation action form a partition of G to prove Theorem 8.10.

Problem 8.5. Let G be a finite group of order p^n where p is prime and $n > 0$. Prove that $Z(G) \neq \{e\}$.

Problem 8.6. Let p be a prime number. Prove that every group of order p^2 is abelian.

Problem 8.7. Let G be a group of order p^n, where p is prime. Show that G has a normal subgroup of order p^k for every k with $0 \leq k \leq n$.

9. Cauchy's Theorem

Exercise 9.1. If G is a finite cyclic group and p is a prime which divides $|G|$, then G has an element of order p.

Lemma 9.1. *If G is a finite abelian group and p is a prime which divides $|G|$ then G has an element of order p.*

Proof. The proof is by (strong) induction on $|G|$. The statement is vacuous if $|G| = 1$. If $|G| = 2$ or $|G| = 3$ the conclusion follows from Exercise 9.1 together with Exercise 4.4. For the induction step, suppose that G is a finite abelian group with $|G| > 3$ and assume that the conclusion holds for any abelian group H with $|H| < |G|$.

Suppose that p is a prime that divides $|G|$. Let $g \neq e$ be any non-trivial element of G and consider the cyclic subgroup $\langle g \rangle$. If p divides $|g|$ then there is an element of order p in $\langle g \rangle \leq G$, by Exercise 9.1. We may therefore assume that p does not divide $|g|$.

Since G is abelian, every subgroup of G is normal and we may form the quotient group $Q = G/\langle g \rangle$. We have $|Q| = |G|/|g| < |G|$ and, since p does not divide $|g|$, we also have that p divides $|Q|$. Thus our induction hypothesis implies that Q has an element q of order p. Let $a \in G$ be an element that maps to q under the natural homomorphism from G

onto $Q = G/\langle g\rangle$. Then the cyclic group $\langle a\rangle$ maps onto the cyclic group $\langle q\rangle \leq Q$. Since $|q| = p$, the First Isomorphism Theorem implies that p divides the order of the cyclic group $\langle a\rangle$. By Exercise 9.1 we conclude that there is an element of order p in $\langle a\rangle \leq G$. This completes the induction step. □

Theorem 9.2 (Cauchy's Theorem)**.** *If G is a finite group and p is a prime which divides $|G|$ then G has an element of order p.*

Proof. The proof is based on the Class Equation (8.10). As in the lemma, the proof is by induction on $|G|$. The same argument that was used in the proof of the lemma shows that the conclusion holds if $|G| < 4$. For the induction step, suppose that G is a finite group with $|G| > 3$ and assume that the conclusion holds for any finite group H with $|H| < |G|$.

Suppose that p is a prime that divides $|G|$. If there is any proper subgroup $H < G$ such that the order of $|H|$ is divisible by p, then the induction hypothesis implies that H, and hence G, has an element of order p. We may therefore assume that no proper subgroup of G has order divisible by p. In particular, every subgroup of G has index divisible by p.

Now consider the Class Equation. In the notation of 8.10, we have

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)],$$

where $[G : C_G(g_i)] > 1$ for each $i = 1, \ldots k$. Our assumption implies that p divides $[G : C_G(g_i)]$ for each $i = 1, \ldots, k$, and we are given that p divides $|G|$. It follows that p divides $|Z(G)|$. We therefore conclude that $Z(G) = G$ since otherwise $Z(G)$ would be a proper subgroup of G with order divisible by p, contrary to our assumption. If $Z(G) = G$ then G is abelian, and it follows from the lemma that G has an element of order p. This completes the induction step. □

10. The Sylow Theorems

Definition 10.1. If p is a prime number, a group G is defined to be *a p-group* if the order of every element is a power of p. A *p-subgroup* of a group G is a subgroup of G which is a p-group.

Problem 10.1. Prove that a finite group G is a p-group if and only if $|G| = p^n$ for some integer n.

Definition 10.2. A *Sylow p-subgroup* of a group G is a p-subgroup of G which is maximal in the sense that it is not a subgroup of any p-subgroup other than itself. The set of Sylow p-subgroups of G will be denoted $\mathcal{S}_p(G)$. If G is finite, the number of Sylow p-subgroups of G will be denoted $n_p(G)$.

Problem 10.2. Show that any group has a Sylow p-subgroup for each prime p. (For infinite groups, use Zorn's Lemma.)

Exercise 10.3. Let P be a Sylow p-subgroup of a finite group G. Show that any conjugate of P is a Sylow p-subgroup of G.

10.3. In view of Exercise 10.3 we will regard $\mathcal{S}_p(G)$ as a G-set under the conjugation action. If H is any subgroup of G then H also acts on $\mathcal{S}_p(G)$. The theorems in this section are proved by considering the P-orbits in $\mathcal{S}_p(G)$, where $P \leq G$ is a Sylow p-subgroup. Recall that if $P \in \mathcal{S}_p(G)$, then the stabilizer of P under the conjugation action by G is the normalizer $N_G(P)$.

Problem 10.4. Let P be a Sylow p-subgroup of a finite group G. Show that $[N_G(P) : P]$ is not divisible by p.

Problem 10.5. Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Show that $P_2 \leq N_G(P_1)$ if and only if $P_2 = P_1$.

Lemma 10.4. *Let P be a Sylow p-subgroup of a finite group G. The singleton $\{P\}$ is a P-orbit in $\mathcal{S}_p(G)$. Every other P-orbit in $\mathcal{S}_p(G)$ has p^k elements for some $k > 0$.*

Proof. Let $Q \in \mathcal{S}_p(G)$. Let $\mathcal{O}$ denote the P-orbit of Q. The size of $\mathcal{O}$ is the index in P of the stabilizer of Q, which divides $|P|$ by Lagrange's Theorem. By Problem 10.1, we have $|P| = p^n$ for some n. Thus $\mathcal{O}$ has size p^k for some $k \geq 0$. We must show that $k = 0$ if and only if $Q = P$.

The stabilizer of Q under the P-action is $P \cap N_G(Q)$. Thus

$$k = 0 \Leftrightarrow P = P \cap N_G(Q) \Leftrightarrow P \leq N_G(Q) \Leftrightarrow P = Q,$$

where the last equivalence was shown in Problem 10.5. □

Since a subset $X \subset \mathcal{S}_p(G)$ is invariant under the action of P if and only if it is a union of P-orbits, we have the following.

Corollary 10.5. *Let P be a Sylow p-subgroup of a finite group G. Suppose that the subset $X \subset \mathcal{S}_p(G)$ is invariant under the action of P. Then $\#X \equiv 1 \pmod{p}$ if $P \in X$, and $\#X \equiv 0 \pmod{p}$ if $P \notin X$*

Theorem 10.6. *Any two Sylow p-subgroups of a finite group G are conjugate. In particular, $n_p(G)$ divides $|G|$ and $n_p(G) \equiv 1 \pmod{p}$.*

Proof. Let $\mathcal{O} \subset \mathcal{S}_p(G)$ be a G-orbit. To prove that any two Sylow p-subgroups are conjugate we will show that $\mathcal{O} = \mathcal{S}_p(G)$. Suppose not. Choose $P \in \mathcal{O}$ and $Q \in \mathcal{S}_p(G) - \mathcal{O}$. Since $\mathcal{O}$ is a G-orbit, it is invariant under the action of both P and Q. Since $P \in \mathcal{O}$, Corollary 10.5 implies that $\#X \equiv 1 \pmod{p}$. Since $Q \notin \mathcal{O}$, Corollary 10.5 also implies that $\#X \equiv 0 \pmod{p}$. This contradiction shows that $\mathcal{O} = \mathcal{S}_p(G)$.

Since $n_p(G) = \#\mathcal{S}_p(G) = \#\mathcal{O} = [G : N_G(P)]$ we see that $n_p(G)$ divides $|G|$. Since $\mathcal{O}$ is invariant under the action of P for any $P \in \mathcal{S}_p(G)$, Corollary 10.5 implies that

$$n_p(G) = \#\mathcal{O} \equiv 1 \pmod{p}.$$

□

Theorem 10.7. *Let G be a finite group of order $p^n q$, where p does not divide q. Then every Sylow p-subgroup of G has order p^n.*

Proof. Let P be a Sylow p-subgroup of G. We need only show that $[G : P]$ is not divisible by p. We have $[G : P] = [G : N_G(P)][N_G(P) : P]$ and we have already seen in Problem 10.4 that $[N_G(P) : P]$ is not divisible by p. But $[G : N_G(P)] = n_p(G)$ and, according to Theorem 10.6, $n_p(G) \equiv 1 \pmod{p}$. Thus $[G : P]$ is not divisible by p. □

It is strange that one has to count the number of Sylow p-subgroups before counting the number of elements in each Sylow p-subgroup.

Exercise 10.6. Let P be a Sylow p-subgroup of a finite group G. Show that P is a normal subgroup if and only if $n_p(G) = 1$.

Exercise 10.7. Let G be an abelian group and let p be a prime number. Show that $P = \{g \in G \mid |g| = p^k \text{ for some } k\}$ is the unique Sylow p-subgroup of G.

11. Direct products and direct sums

Definition 11.1. Let G and H be groups. The *direct product* of G and H, denoted $G \times H$, is the set $\{(g, h) \mid g \in G \text{ and } h \in H\}$ with the operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$. More generally, if $(G_\alpha)_{\alpha \in I}$ is an indexed family of groups then the direct product $\prod_{\alpha \in I} G_\alpha$ is the set $\{(g_\alpha)_{\alpha \in I} \mid g_\alpha \in G_\alpha\}$ with the operation $(g_\alpha)_{\alpha \in I} \cdot (h_\alpha)_{\alpha \in I} = (g_\alpha h_\alpha)_{\alpha \in I}$. If the index set I is finite, say $I = \{1, \ldots, n\}$, we may write $G_1 \times \cdots \times G_n$ for $\prod_{i=1}^n G_i$. For each $\beta \in I$ the *projection homomorphism* $\pi_\beta \colon \prod_{\alpha \in I} G_\alpha \to G_\beta$ is defined by $\pi_\beta((g_\alpha)_{\alpha \in I}) = g_\beta$.

It is easily checked that the direct product of any indexed family of groups is a group.

Exercise 11.1. If A is a group then $\{e\} \times A$ is isomorphic to A. If A and B are groups then $A \times B$ is isomorphic to $B \times A$. If A, B and C are groups then $(A \times B) \times C$ and $A \times (B \times C)$ are both isomorphic to $A \times B \times C$.

Proposition 11.2. *Let $(G_\alpha)_{\alpha\in I}$ be an indexed family of groups. The direct product $\prod_{\alpha\in I} G_\alpha$ has the following universal mapping property: if H is an arbitrary group and if $\sigma_\alpha\colon H \to G_\alpha$ is a homomorphism for each $\alpha \in I$ then there exists a unique homomorphism $\phi\colon H \to \prod_{\alpha\in I} G_\alpha$ such that $\pi_\alpha \circ \phi = \sigma_\alpha$ for all $\alpha \in I$.*

Exercise 11.2. Prove Proposition 11.2.

Exercise 11.3. Let $(G_\alpha)_{\alpha\in I}$ be an indexed family of groups. Show that the subset

$$\{(g_\alpha)_{\alpha\in I} \mid g_\alpha \in G_\alpha \text{ and } g_\alpha = e \text{ for all but finitely many } \alpha\}$$

is a normal subgroup of $\prod_{\alpha\in I} G_\alpha$.

Definition 11.3. If $(G_\alpha)_{\alpha\in I}$ is an indexed family of groups then the direct sum $\bigoplus_{\alpha\in I} G_\alpha$ is the subgroup of $\prod_{\alpha\in I} G_\alpha$ consisting of all sequences $(g_\alpha)_{\alpha\in I}$ such that $G_\alpha = e$ for all but finitely many α. For each $\beta \in I$ the *inclusion homomorphism* $\iota_\beta\colon G_\beta \to \bigoplus_{\alpha\in I} G_\alpha$ sends each element $g \in G_\beta$ to $(g_\alpha)_{\alpha\in I}$ where $g_\beta = g$ and $g_\alpha = e$ for all $\alpha \neq \beta$.

11.4. The notions of direct product and direct sum coincide in the case of a finite family of groups: $\bigoplus_{i=1}^n G_i = \prod_{i=1}^n G_i$.

The next proposition can be paraphrased as saying that the direct sum is a co-product in the category of abelian groups.

Proposition 11.5. *Let $(G_\alpha)_{\alpha\in I}$ be an indexed family of abelian groups. The direct sum $\bigoplus_{\alpha\in I} G_\alpha$ has the following universal mapping property: if H is an abelian group and if $\nu_\alpha\colon G_\alpha \to H$ is a homomorphism for each $\alpha \in I$ then there exists a unique homomorphism $\phi\colon \bigoplus_{\alpha\in I} G_\alpha \to H$ such that $\phi \circ \iota_\alpha = \nu_\alpha$ for all $\alpha \in I$.*

Exercise 11.4. Prove Proposition 11.5 and show that the statement would be false without the assumption that H is abelian.

Proposition 11.6. *Let G be a group. If H and K are normal subgroups of G such that $G = HK$ and $H \cap K = \{e\}$, then $G \cong H \times K$. More generally, if $H_1, \ldots, H_n$ are normal subgroups of G such that $G = \langle \cup_{i=1}^n H_i \rangle$, and $H_j \cap \langle \cup_{i\neq j} H_j \rangle = \{e\}$ for each j, then $G \cong \prod_{i=1}^n H_i$.*

Exercise 11.5. Prove Proposition 11.6

Proposition 11.7. *Let G be a finite group. If H and K are normal subgroups of G such that $|G| = |H|\,|K|$ and $|H \cap K| = 1$, then $G \cong H \times K$. More generally, if $H_1, \ldots, H_n$ are normal subgroups of G such that $|G| = |H_1| \cdots |H_n|$, and $|H_j \cap \langle \cup_{i\neq j} H_j \rangle| = 1$ for each j, then $G \cong \prod_{i=1}^n H_i$.*

Exercise 11.6. Prove Proposition 11.7

Exercise 11.7. Suppose that G is a group and that H and K are normal subgroups of G such that $H \cap K = \{e\}$. Prove that $hk = kh$ for all $h \in H$ and $k \in K$.

Exercise 11.8. Give an example of a group G containing three normal subgroups H_1, H_2 and H_3 such that (1) $H_1H_2H_3 = G$; (2) $H_i \cap H_j = \{e\}$ when $i \neq j$, and (3) G is not isomorphic to $H_1 \times H_2 \times H_3$.

12. Finite abelian groups

Lemma 12.1. *Let G be a finite abelian p-group. Let $g \in G$ be an element of maximal order. Then there exists a subgroup $H < G$ such that $\langle g \rangle \cdot H = G$ and $\langle g \rangle \cap H = \{e\}$.*

Proof. We have $|G| = p^n$ for some non-negative integer n. The proof is by induction on n. The cases $n = 0$ and $n = 1$ are clear. Assume that $n > 1$ and that the conclusion holds for any group of order p^k where $k < n$.

The conclusion clearly holds if $\langle g \rangle = G$ since then we can take $H = \{e\}$. Therefore we focus on the case where $\langle g \rangle \neq G$. In this case we claim that G has an element x of order p which is not contained in $\langle g \rangle$. To prove the claim consider the (non-trivial) quotient group $G/\langle g \rangle$. By Cauchy's Theorem this group has an element of order p. Thus there exists $h \in G$ such that $h \notin \langle g \rangle$ but $h^p \in \langle g \rangle$. Observe that h^p cannot be a generator of the cyclic group $\langle g \rangle$, because that would imply that $|h| = p|g| > |g|$, contradicting our hypothesis that g has maximal order in G. Therefore $h = g^{pm}$ for some $m > 0$. Now consider the element $x = hg^{-m}$. We have $x \notin \langle g \rangle$ and $x^p = h^p g^{-mp} = e$. This implies the claim. Moreover, since x has prime order, we have $\langle g \rangle \cap \langle x \rangle = \{e\}$.

Now form the quotient $\hat{G} \doteq G/\langle x \rangle$ and consider the natural homomorphism $\phi \colon G \to \hat{G}$. Since $\langle g \rangle \cap \langle x \rangle = \{e\}$, we have $|\phi(g)| = |g|$. But for any element $h \in G$ we have $|\phi(h)| \leq |h|$. Thus $\hat{g} \doteq \phi(g)$ has maximal order in $\hat{G}$. By induction, there is a subgroup $\hat{K} < \hat{G}$ such that $\langle \hat{g} \rangle \cdot \hat{K} = \hat{G}$ and $\langle \hat{g} \rangle \cap \hat{K} = \{e\}$. We set $K = \phi^{-1}(\hat{K})$. Since $\ker \phi \leq K \leq K \cdot \langle g \rangle$, and since $\phi(K \cdot \langle g \rangle) = \hat{K} \cdot \langle \hat{g} \rangle = \hat{G}$ we conclude that $K \cdot \langle g \rangle = G$. Also, since $\phi(K \cap \langle g \rangle) = \hat{K} \cap \langle \hat{g} \rangle = \{e\}$, we have $K \cap \langle g \rangle \leq \ker \phi = \langle x \rangle$. Obviously $K \cap \langle g \rangle \leq \langle g \rangle$. Thus $K \cap \langle g \rangle \leq \langle x \rangle \cap \langle g \rangle = \{e\}$, which completes the induction step. □

Exercise 12.1. Prove that any finite abelian p-group is isomorphic to a direct sum of cyclic p-groups.

Theorem 12.2. *Any finite abelian group is isomorphic to a direct sum of cyclic groups of prime power order.*

Problem 12.2. Prove Theorem 12.2

Exercise 12.3. Show that if m and n are relatively prime integers then $C_n \times C_m \cong C_{mn}$.

Problem 12.4. Let G be a finite abelian group. Suppose that for every prime p the number of elements of order p in G is at most $p-1$. Prove that G is cyclic.

Exercise 12.5. Classify the abelian groups of order 72.

13. Semi-direct products

Definition 13.1. A *short exact sequence of groups* is a diagram

$$N \overset{\iota}{\rightarrowtail} G \overset{\phi}{\twoheadrightarrow} Q \ ,$$

where ι is an injective homomorphism, ϕ is a surjective homomorphism and $\operatorname{im}\iota = \ker\phi$. When such a short exact sequence exists, G is said to be an *an extension of N by Q.* In particular, if N is a normal subgroup of G and the quotient G/N is isomorphic to Q then G is an extension of N by Q.

If G is an extension of N by Q as above, and if there also exists a homomorphism $\sigma\colon Q \to G$ such that $\phi \circ \sigma = \mathrm{id}_Q$, then G is called a *split extension* and σ is called a *section*. This situation is described by the following diagram:

$$N \overset{\iota}{\rightarrowtail} G \underset{\phi}{\overset{\sigma}{\rightleftarrows}} Q \ .$$

13.2. Not all extensions are split! An example is provided by the quaternion group Q_8. This group can be described as consisting of the eight invertible 2×2 complex matrices $\{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$, where 1 denotes the identity matrix and

$$\mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Observe that $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$, $\mathbf{ij} = \mathbf{k}$ and $\mathbf{ji} = -\mathbf{k}$. The center of Q_8 is $\{\pm 1\}$ and the quotient $Q_8/Z(Q_8)$ is isomorphic to the Klein 4-group V. Thus Q_8 is an extension of C_2 by V. The only element of order 2 in Q_8 is the central element -1, so there cannot exist a section $\sigma\colon V \to Q_8$.

Definition 13.3. Suppose that H and K are groups and that $\phi\colon K \to \operatorname{Aut} H$ is a homomorphism. (Thus ϕ can be regarded as an action of K on H by automorphisms.) Write ϕ_k to denote the automorphism $\phi(k)$, so we have $\phi_{hk} = \phi_h \circ \phi_k$. Define the *semi-direct product of H by K (via ϕ)*, denoted $H \rtimes_\phi K$, to be the set of ordered pairs $\{(h,k) \mid h \in H \text{ and } k \in K\}$ together with the operation

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

Exercise 13.1. Let H and K be groups and let $\phi\colon K \to \operatorname{Aut} H$ be an action of K on H by automorphisms. Show that $H \rtimes_\phi K$ is a group, and that $H \rtimes_\phi K$ is a split extension of H by K.

Exercise 13.2. Let G be a group. Suppose that H and K are subgroups of G such that $H \trianglelefteq G$, $G = HK$, and $H \cap K = \{e\}$. Define $\phi\colon K \to \operatorname{Aut} H$ by $\phi(k) = \phi_k$, where $\phi_k(h) = khk^{-1}$. Show that ϕ is a homomorphism and that $G \cong H \rtimes_\phi K$.

Exercise 13.3. Let N be a normal subgroup of a group G and let $\pi\colon G \to G/N$ be the natural homomorphism. Suppose that there is a homomorphism $\sigma\colon G/N \to G$ with $\pi \circ \sigma = \mathrm{id}_{G/N}$ (i.e. σ is a section). Prove that $G \cong N \rtimes_\phi Q$ for some homomorphism $\phi\colon Q \to \operatorname{Aut} N$.

Proposition 13.4. *Let H and K be groups and let $\phi\colon K \to \operatorname{Aut} H$ and $\psi\colon K \to \operatorname{Aut} H$ be actions of K on H by automorphisms. Suppose that there exist automorphisms $\alpha \in \operatorname{Aut} H$ and $\beta \in \operatorname{Aut} K$ such that $\psi_{\beta(k)} = \alpha \circ \phi_k \circ \alpha^{-1}$ for all $k \in K$. Then $H \rtimes_\phi K \cong H \rtimes_\psi K$.*

Exercise 13.4. Prove Proposition 13.4.

13.5. It is useful to consider groups of the form $C_n \rtimes_\phi K$. This requires understanding the structure of the group $\operatorname{Aut} C_n$. To give a concrete description of $\operatorname{Aut} C_n$, choose a generator x of C_n, so $C_n = \{e, x, x^2, \ldots, x^{n-1}\}$. For each integer k there is a homomorphism $\phi_k\colon C_n \to C_n$ defined by $\phi_k(x^i) = x^{ki}$. Clearly $\phi_k = \phi_{k'}$ if and only if $k \equiv k' \pmod n$. If $\phi\colon C_n \to C_n$ and $\psi\colon C_n \to C_n$ are homomorphisms then $\phi = \psi$ if and only if $\phi(x) = \psi(x)$. Thus every homomorphism from C_n to itself is equal to ϕ_k for some k. Finally, observe that $\phi_j \circ \phi_k = \phi_{jk}$

Exercise 13.5. Show that ϕ_k is an automorphism of C_k if and only if k is a unit mod n (i.e. if and only if k has a multiplicative inverse mod n). Conclude that the group $\operatorname{Aut}(C_n)$ is isomorphic to the abelian group $U(n)$, which is defined to be the multiplicative group of units mod n.

Proposition 13.6. *If p is prime then $\operatorname{Aut} C_p$ is a cyclic group of order $p-1$.*

Proof. The most natural proof of this takes us outside of group theory. So be it! The fact that we need is this: a polynomial of degree n with coefficients in a field F has at most n roots in F.

Identify $\operatorname{Aut} C_p$ with $U(p)$, the multiplicative group of non-zero elements in the field $F_p = \mathbb{Z}/p\mathbb{Z}$. We have $|U(p)| = p-1$ since every non-zero element of F_p is a unit.

For any prime q the elements of order q in $U(p)$ are roots of the polynomial $x^q - 1$. There are at most q such roots. One of the roots is the multiplicative identity 1, which is not

an element of order q. Thus there are at most $q-1$ elements of order q in $U(p)$. It now follows from Problem 12.4 that $U(p)$ is cyclic. □

Exercise 13.6. Let p be a prime and let G be a finite cyclic group. Let $\phi\colon G \to \operatorname{Aut} C_p$ and $\psi\colon G \to \operatorname{Aut} C_p$ be actions of G on C_p by automorphisms. Show that $C_p \rtimes_\phi G \cong C_p \rtimes_\psi G$ if and only if $|\phi(G)| = |\psi(G)|$.

Exercise 13.7. Let $p > 2$ be a prime. Show that a non-abelian extension of C_p by C_2 is isomorphic to the dihedral group D_{2p}.

Exercise 13.8. Classify the semi-direct products $C_8 \rtimes_\phi C_2$ up to isomorphism.

14. Permutations

Recall that the permutation groups $S(X)$ and S_n were defined in 8.1.

Definition 14.1. If $\sigma \in S(X)$ is a permutation, we define the *fixed set* of σ to be

$$\operatorname{Fix}\sigma = \{x \in X \mid \sigma(x) = x\}$$

and the *support* of σ to be the complement of the fixed set:

$$\operatorname{Supp}\sigma = \{x \in X \mid \sigma(x) \neq x\}.$$

14.2. One (cumbersome) notation that is sometimes used to describe a permutation in S_n is a $2 \times n$ matrix where the first row is $1, \ldots, n$ and the second row is $\sigma(1), \ldots, \sigma(n)$. For example,

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

denotes the permutation that sends 1 to 2, 2 to 3, 3 to 1, 4 to 5 and 5 to 4.

Exercise 14.1. The order of S_n is $n!$.

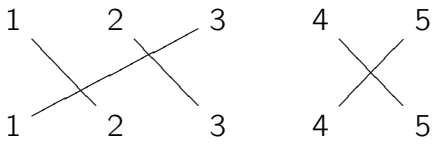
Exercise 14.2. Suppose that X and Y are sets and that there exists a bijection $\phi\colon X \to Y$. Show that $S(X)$ is isomorphic to $S(Y)$.

Definition 14.3. Let $\sigma \in S_n$. A *flip* of σ is a subset $\{i, j\}$ of $\{1, \ldots, n\}$ such that either

- $i < j$ and $\sigma(i) > \sigma(j)$; or
- $j < i$ and $\sigma(j) > \sigma(i)$.

We define $\operatorname{Flips}\sigma$ to be the number of distinct flips of σ.

14.4. Here is a graphical way to count the number of flips of a permutation $\sigma \in S_n$. Write the integers $1, \ldots, n$ in two rows, one above the other, and join each i to $\sigma(i)$ by a line segment. The number of crossing points is equal to $\operatorname{Flips}\sigma$. For example, the diagram below shows that the permutation given in 14.2 has 3 flips:



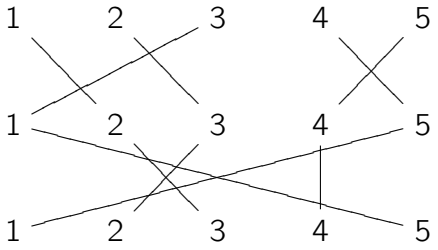
To understand how the number of flips behaves under composition it is helpful to juxtapose the diagrams for two permutations. Here is an example. Suppose

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \text{ and}$$

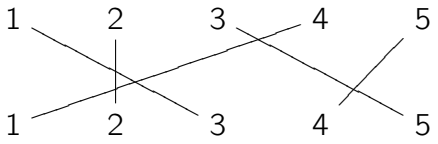
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}, \text{ so}$$

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

Then $\operatorname{Flips}\sigma = 3$, $\operatorname{Flips}\tau = 8$, and $\operatorname{Flips}(\tau\sigma) = 5$. If we juxtapose the diagrams for σ and τ we have



The diagram for $\tau\sigma$, shown below, is obtained by joining the segments of the juxtaposed diagram along the center row and straightening.



Some crossings are removed in the straightening process, but they are always removed in pairs. For example, the segments 1—2—3 and 3—1—5 have a pair of crossings which are removed by straightening. (In this example, a total of 3 pairs of crossings are removed.) This suggests that the number of flips will be additive under composition, provided we count flips modulo 2.

Definition 14.5. For $\sigma \in S_n$ we define $\operatorname{Sign}\sigma \in \{0,1\}$ by

$$\operatorname{Sign}\sigma \equiv \operatorname{Flips}\sigma \pmod 2.$$

We say that σ is *even* if $\operatorname{Sign}\sigma = 0$ and σ is *odd* if $\operatorname{Sign}\sigma = 1$.

Proposition 14.6. *For $\sigma, \tau \in S_n$ we have*

$$\operatorname{Sign}(\tau\sigma) \equiv \operatorname{Sign}\tau + \operatorname{Sign}\sigma \pmod 2.$$

In particular, Sign *defines a homomorphism from S_n to the group $\mathbb{Z}/2\mathbb{Z}$ of integers modulo 2, under addition.*

Proof. First, we observe that $\{i,j\}$ is a flip for $\tau\sigma$ if and only if one of the following mutually exclusive possibilities holds:

(1) $\{i,j\}$ is a flip for σ and $\{\sigma(i),\sigma(j)\}$ is not a flip for τ; or

(2) $\{i,j\}$ is not a flip for σ and $\{\sigma(i),\sigma(j)\}$ is a flip for τ.

Now consider the pairwise disjoint sets

$$A = \{\{i,j\} \mid \{i,j\} \text{ is a flip for } \sigma \text{ and } \{\sigma(i),\sigma(j)\} \text{ is not a flip for } \tau\};$$
$$B = \{\{i,j\} \mid \{i,j\} \text{ is not a flip for } \sigma \text{ and } \{\sigma(i),\sigma(j)\} \text{ is a flip for } \tau\};$$
$$C = \{\{i,j\} \mid \{i,j\} \text{ is a flip for } \sigma \text{ and } \{\sigma(i),\sigma(j)\} \text{ is a flip for } \tau\}.$$

Observe that $A \cup B$ is the set of flips for $\tau\sigma$ and $A \cup C$ is the set of flips for σ. Since A, B and C are pairwise disjoint we have $\operatorname{Flips}(\tau\sigma) = \#A + \#B$ and $\operatorname{Flips}(\sigma) = \#A + \#C$.

The set of flips for τ is equal to $\{\ \{i,j\} \mid \{\sigma^{-1}(i),\sigma^{-1}(j)\} \in B \cup C\ \}$. Since σ is a bijection and B and C are disjoint, we therefore have $\operatorname{Flips}\tau = \#B + \#C$.

Thus

$$\operatorname{Flips}(\tau\sigma) = \#A + \#B$$

and

$$\operatorname{Flips}\tau + \operatorname{Flips}\sigma = \#A + \#C + \#B + \#C \equiv \#A + \#B \pmod 2,$$

which shows that $\operatorname{Sign}(\tau\sigma) \equiv \operatorname{Sign}\tau + \operatorname{Sign}\sigma \pmod 2$. □

Corollary 14.7. *The even permutations in S_n form a normal subgroup.*

Definition 14.8. The *alternating group* A_n is the normal subgroup of S_n consisting of all even permutations.

Definition 14.9. Let $k > 1$ be an integer. A permutation $\sigma \in S(X)$ is a *k-cycle* if there exist distinct elements $x_1, \ldots, x_k$ of X such that

$$\begin{aligned} \sigma(x_j) &= x_{j+1} \text{ for } j = 1, \ldots, k-1 \\ \sigma(x_k) &= x_1 \\ \sigma(x) &= x \text{ for } x \in X - \{x_1, \ldots, x_k\} \end{aligned}$$

The k-cycle σ may be denoted $(x_1 \ \ldots \ x_k)$. Note that this notation is not unique:

$$(x_1 \ \ldots \ x_k) = (x_2 \ \ldots \ x_k \, x_1) = \cdots = (x_k \, x_1 \ \ldots \ x_{k-1}).$$

A permutation is a *cycle* if it is a k-cycle for some $k > 1$, or if it is the identity. A 2-cycle is called a *transposition*.

Note that $\operatorname{Supp}(x_1 \ \ldots \ x_k) = \{x_1, \ldots, x_k\} \subseteq X$. Two cycles $\sigma, \tau \in S(X)$ are said to be *disjoint* if $\operatorname{Supp}\sigma \cap \operatorname{Supp}\tau = \emptyset$.

Exercise 14.3. Show that disjoint cycles in $S(X)$ commute.

Proposition 14.10. *If X is a finite set then any permutation in $S(X)$ is a product of finitely many disjoint cycles.*

Proof. Let $\sigma \in S(X)$. The proof is by induction on $N(\sigma) = \#\operatorname{Supp}\sigma$. If $N(\sigma) = 0$ then σ is the identity permutation, which is a cycle by definition.

Suppose $N(\sigma) = n > 0$, and suppose that every permutation $\tau \in S(X)$ with $N(\tau) < n$ is a product of disjoint cycles. Choose $x \in X$ so that $\sigma(x) \neq x$. Set $x_i = \sigma^i(x)$ for all non-negative integers i. The elements x_i cannot be distinct for all i since X is finite. Let k be the smallest positive integer such that $x_k \in \{x_0, \ldots, x_{k-1}\}$. We claim that $x_0, \ldots, x_{k-1}$ are distinct elements of X. If not, there exist $0 < i < j < k$ with $x_i = x_j$. Thus $\sigma^i(x) = \sigma^j(x)$, so $\sigma^{j-i}(x) = x = x_0$. Since $0 < j - i < k$, this contradicts the minimality of k, proving the claim. Next we claim that $x_k = x_0$. We know that $x_k = x_i$ for some $0 \leq i < k$. Thus $\sigma^i(x) = \sigma^k(x)$, so $x = \sigma^{k-i}$. This would contradict the minimality of k unless $i = 0$. Therefore $x_k = x_0$ as claimed.

Now let γ denote the k-cycle $(x_0 \ \ldots \ x_{k-1})$. Observe that $\gamma^{-1}\sigma(x_i) = x_i$ for $i = 0, \ldots, k-1$. Since $\gamma\sigma(x) = \sigma(x)$ for $x \in X - \{x_0, \ldots, x_{k-1}\}$, the support of σ is the disjoint union

$$\operatorname{Supp}\sigma = \operatorname{Supp}(\gamma^{-1}\sigma) \dot{\cup} \{x_0, \ldots, x_{k-1}\}.$$

In particular, $N(\gamma^{-1}\sigma) < N(\sigma)$ and, by induction, we may write $\gamma^{-1}\sigma = \gamma_1 \cdots \gamma_m$ where $\gamma_1, \ldots, \gamma_m$ are disjoint cycles for some $m > 0$. Since $\gamma^{-1}\sigma(x_i) = x_i$ for $i = 0, \ldots, k-1$ and $\operatorname{Supp}\gamma = \{x_0, \ldots, x_{k-1}\}$, the cycle γ is disjoint from $\gamma_1, \ldots, \gamma_m$. Thus $\sigma = \gamma\gamma_1 \cdots \gamma_m$ is a product of disjoint cycles, completing the induction step. $\square$

Exercise 14.4. Suppose that $\sigma = \gamma_1 \cdots \gamma_m$ and $\sigma = \delta_1 \cdots \delta_n$ are two factorizations of σ as products of disjoint cycles. Show that $\{\gamma_1, \ldots, \gamma_m\} = \{\delta_1, \ldots, \delta_n\}$.

Exercise 14.5. Show that a k-cycle can be written as a product of $k+1$ transpositions.

Exercise 14.6. Show that any permutation in S_n is a product of transpositions.

Exercise 14.7. Show that a permutation in S_n is even if and only if it is a product of an even number of transpositions.

Exercise 14.8. Show that a permutation in S_n is even if and only if it is a product of 3-cycles.

Definition 14.11. Suppose that $\sigma \in S_n$, and that $\sigma = \gamma_1 \cdots \gamma_m$ is a factorization of σ as a product of disjoint cycles. Suppose that γ_i is a k_i-cycle. Since disjoint cycles commute, we may assume after reordering that $k_1 \geq k_2 \geq \cdots \geq k_m$. By the *cycle structure* of σ we will mean the m-tuple $[k_1, \ldots, k_m]$, where $k_1 \geq k_2 \geq \cdots \geq k_m$. Exercise 14.4 implies that the cycle structure of σ is well-defined, i.e. that every factorization of σ as a product of disjoint cycles gives rise to the same m-tuple.

14.12. As an illustration, the permutation

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

has the disjoint cycle decomposition $\sigma = (123)(45)$, and its cycle structure is $[3, 2]$.

14.13. Suppose that $\gamma = (x_1 \ \ldots \ x_k)$ is a k-cycle in $S(X)$ and that σ is an arbitrary element of $S(X)$. Then $\sigma\gamma\sigma^{-1} = (\sigma(x_1) \ \ldots \ \sigma(x_k))$. In particular, a conjugate of a k-cycle is a k-cycle.

Exercise 14.9. Show that two permutations in S_n are conjugate if and only if they have the same cycle structure.

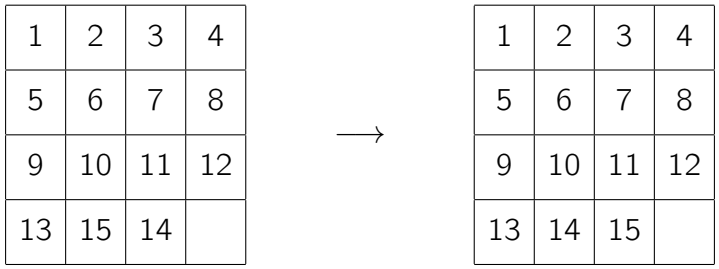
Exercise 14.10. Show that a permutation in S_n is even if and only if there are an even number of even length cycles in its disjoint cycle decomposition.

Exercise 14.11. Suppose that $\sigma \in S_n$ has cycle structure $[k_1, \ldots, k_m]$. Show that

$$|\sigma| = \operatorname{lcm}(k_1, \ldots, k_m).$$

Problem 14.12. Show that the cycles (12) and $(12 \cdots n)$ generate S_n.

Problem 14.13. In 1878 Sam Loyd invented his tremendously popular "14-15" sliding block puzzle. Mr. Loyd offered a prize of $1000 to anyone who could interchange the pieces labeled 14 and 15 by sliding the blocks:



Prove that Mr. Loyd was in no danger of losing his $1000. (According to Bill Wall (`http://www.geocities.com/siliconvalley/lab/7378/loyd.htm`) the U.S. Patent Office refused to issue a patent for the puzzle once it was shown to be impossible.)

15. Simplicity of alternating groups

Definition 15.1. A group G is *simple* if G has no proper normal subgroup.

15.2. Obviously the trivial group $\{e\}$ is simple, and it follows from Lagrange's Theorem that a group of prime order is simple (and cyclic, by Exercise 4.4). The alternating groups A_2 and A_3 are therefore simple.

Lemma 15.3. *If $n \geq 5$ then any two 3-cycles are conjugate in A_n.*

Proof. It suffices to show that any 3-cycle is conjugate in A_n to $(1\,2\,3)$. Let $\sigma = (a\,b\,c)$ be a 3-cycle in A_n and let x and y be two distinct elements of $\{1, \ldots, n\} - \{a, b, c\}$. (There exist two such elements because $n \geq 5$.) Let τ_0 be any permutation in S_n such that $\tau_0(1) = a$, $\tau_0(2) = b$, $\tau_0(3) = c$. If τ_0 is even set $\tau = \tau_0$ and if τ_0 is odd, set $\tau = (x\,y)\tau_0$. Then $\tau \in A_n$ and $\tau(i) = \tau_0(i)$ for $i = 1, 2, 3$. In particular, $\tau^{-1}\sigma\tau = (1\,2\,3)$. □

Lemma 15.4. *Let N be a normal subgroup of A_n for $n \geq 5$. If N contains a 3-cycle then $N = A_n$.*

Proof. Suppose that $N \trianglelefteq A_n$ and that N contains a 3-cycle σ. Since N is normal, it contains all conjugates of σ in A_n. By Lemma 15.3, N contains all 3-cycles. By by Exercise 14.8, this implies that $N = A_n$. □

Theorem 15.5. *If $n \geq 5$ then A_n is a simple group.*

Proof. Let $n \geq 5$ and suppose that $\{e\} \neq N \trianglelefteq A_n$. We will show that $N = A_n$. We begin by showing that N contains a 3-cycle.

Suppose we are given an arbitrary element $\tau \in N$ and that $\sigma \in A_n$ is any 3-cycle. Consider the *commutator*

$$[\tau, \sigma] \doteq \tau\sigma\tau^{-1}\sigma^{-1}.$$

Since $[\tau, \sigma] = \tau(\sigma\tau^{-1}\sigma^{-1})$, we see that $[\tau, \sigma] \in N$. Since $[\tau, \sigma] = (\tau\sigma\tau^{-1})\sigma^{-1}$ we see that $[\tau, \sigma]$ is a product of two 3-cycles, and hence that the support of $[\tau, \sigma]$ contains at most 6 elements of $\{1, \ldots, n\}$.

Now suppose that τ has been chosen among all non-identity elements of N so that $\operatorname{Supp}\tau$ has the mimimal number of elements. We will show that $\operatorname{Supp}\tau$ has 3 elements, which implies that τ is a 3-cycle.

Since $[\tau, \sigma] \in N$ for any 3-cycle $\sigma \in A_n$, we may assume that $\operatorname{Supp}\tau$ has at most 6 elements. Since τ is even, the only possible cycle structures for τ are the following:

$$[2, 2], \quad [3], \quad [3, 3], \quad [4, 2], \quad [5].$$

If $\tau = (a\,b)(c\,d)$ then, since $n \geq 5$, there exists an element $x \in \{1, \ldots, n\}$ which is distinct from a, b, c, d. Let $\sigma = (a\,b\,x)$. Then we have

$$[\tau, \sigma] = (\tau\sigma\tau^{-1})\sigma^{-1} = (b\,a\,x)(x\,b\,a) = (a\,b\,x).$$

If $\tau = (a\,b\,c)(x\,y\,z)$ then take $\sigma = (a\,b\,x)$. We have

$$[\tau, \sigma] = (\tau\sigma\tau^{-1})\sigma^{-1} = (b\,c\,y)(x\,b\,a) = (a\,x\,c\,y\,b).$$

If $\tau = (a\,b\,c\,d)(x\,y)$ then take $\sigma = (a\,b\,c)$. We have

$$[\tau, \sigma] = (\tau\sigma\tau^{-1})\sigma^{-1} = (b\,c\,d)(c\,b\,a) = (a\,d\,b).$$

If $\tau = (a\,b\,c\,d\,f)$ then take $\sigma = (a\,b\,c)$. We have

$$[\tau, \sigma] = (\tau\sigma\tau^{-1})\sigma^{-1} = (b\,c\,d)(c\,b\,a) = (a\,d\,b).$$

In each case the support of $[\tau, \sigma]$ would be smaller than the support of τ, contradicting our choice of τ. We conclude that the cycle structure of τ must be [3], i.e. that τ is a 3-cycle.

Since N contains a 3-cycle, we have $N = A_n$ by Lemma 15.4. Since N was an arbitrary non-trivial normal subgroup, we have shown that A_n has no proper normal subgroup. □

Exercise 15.1. Show that A_4 contains a normal subgroup of order 4 in which every non-identity element has order 2. This subgroup is called the *Klein 4-group* and is named V (for *vier*, presumably).

Problem 15.2. Show that A_4 does not have a subgroup of order 6. Thus A_4 gives an example of a group for which the converse of Lagrange's Theorem is false.

Exercise 15.3. Suppose that $\phi\colon S_n \to G$ is a surjective homomorphism. Show that either ϕ is an isomorphism or $|G| \leq 2$.

Index of Definitions