Group Theory

Daniel Arreola

0 Notation

IDK

1 Definitions and Examples

1.1 Semigroups and Monoids

[1.1.1] (Semigroups). Let X be a set. A map $* : X \times X \to X$ is called a **binary operation** (or simply, operation) on X. For any $x, y \in X$, the image of (x, y) under the map $*$ is called the **product** of x and y and is denoted by $x * y$, similar to how we traditionally write $x + y$ and $x \cdot y$ for the operations of addition and multiplication. There are two ways to interpret the product of three elements $x, y, z \in X$ in the order that they are listed, namely $(x * y) * z$ and $x * (y * z)$. The operation $*$ is said to be **associative** if the two expressions are equal for all $x, y, z \in X$. A **semigroup** is a pair $\langle X, * \rangle$ consisting of a set X and an associative binary operation $*$ on X.

Let $\langle X, * \rangle$ be a semigroup. The product of a list $x_1, \ldots, x_n \in X$ is defined inductively by

$$\prod_{i=1}^{1} x_i = x_1, \qquad \prod_{i=1}^{k} x_i = \left(\prod_{i=1}^{k-1} x_i \right) * x_k \quad \text{for } k = 2, \ldots, n.$$

For example, $\prod_{i=1}^{4} x_i = ((x_1 * x_2) * x_3) * x_4$. Owing to the associativity of the operation, it can be shown by induction that

$$\left(\prod_{i=1}^{j} x_i \right) * \left(\prod_{i=1}^{n-j} x_{j+i} \right) = \prod_{i=1}^{n} x_i$$

for any $j = 1, \ldots, n-1$. What this means is that we may insert parentheses into a finite product of elements of X in any way we want and the result will be the same. Hence, we will sometimes omit parenthesis when writing finite products in a semigroup and simply write $x_1 * \cdots * x_n$.

[1.1.2] Example. Let $X = \mathbb{N}$. For any $x, y \in X$, let $x \wedge y$ denote the greatest common divisor of x and y. Then $\wedge$ defines an associative binary operation on X, so $\langle X, \wedge \rangle$ is a semigroup.

[1.1.3] (Monoids). Let $\langle X, * \rangle$ be a semigroup. An element $e \in X$ such that $e * x = x = x * e$ for all $x \in X$ is called an **identity element**. If $e' \in X$ is another identity element, then $e' = e' * e = e$. Hence if X contains an identity element, it is unique. A semigroup which contains an identity element is called a **monoid**.

[1.1.4] Example. Let A be any set. Let A^A denote the set of all functions from A to A. For any $f, g \in A^A$, let $f \circ g$ denote the composition f and g, i.e., $(f \circ g)(x) = f(g(x))$ for all $x \in A$. The map $(f, g) \mapsto f \circ g$ is an associative operation on A^A. Moreover, the function $\iota : A \to A$ given by $\iota(x) = x$ for all $x \in A$ is an identity element in A^A. Hence $\langle A^A, \circ \rangle$ is a monoid.

[1.1.5] Remark. Writing the symbol $*$ can get tiresome when dealing with abstract semigroups, so we will save ourselves from writing more than we have to by omitting the operation from every place we can get away with. Rather than writing $x * y$ to denote the product of x and y, we will simply write xy. Having removed the need to indicate that $*$ is the operation when discussing products, we will simply say that X is a semigroup when $\langle X, * \rangle$ is a semigroup. Note that we will only make these simplications when there is no danger of ambiguity. We will always write the symbol for an operation when we feel it is important to emphasize it. For instance, it is standard to use additive notation and write $x + y$ to denote the "product" of two elements of a commutative semigroup.

Let M be a monoid. Given any two subsets $A, B \subseteq M$, we write AB to denote the set of all products of an element of A with an element of B. Thus $AB = \{ab \mid a \in A, b \in B\}$. This gives 2^M the structure of a monoid.

1.2 Groups

A **group** G is a monoid which contains an inverse for each of its elements.

2 Subgroups

2.1 Cosets

Given any two subsets $A, B \subseteq G$, we write AB to denote the set of all products of an element of A with an element of B. Thus $AB = \{ab \mid a \in A, b \in B\}$. This gives 2^G the structure of a monoid.

[2.1.1] Theorem (Tower Law)**.** Let G be a group and suppose $K \leq H \leq G$. Then

$$[G : K] = [G : H][H : K].$$

Proof: Write $G = \bigsqcup_{i \in I} g_i H$ and $H = \bigsqcup_{j \in J} h_j K$. We claim that $G = \bigsqcup_{i,j} g_i h_j K$. To see that this union is disjoint, suppose $g_i h_j K = g_s h_t K$. Then since $K \leq H$, $g_i H = g_s H$, so $i = s$. But then $h_j K = h_t K$, so $j = t$. Therefore the map $G/H \times H/K \to G/K$ given by $(g_i H, h_j K) \mapsto g_i h_j K$ is a bijection, completing the proof. □

The preceding theorem has many corollaries. A classic application of the above theorem is as follows. Suppose G is a finite group and that H is a subgroup. The index of the trivial subgroup in G and H is equal to the order of G and H, respectively. Hence (2.1.1) implies $|G| = [G : H]|H|$. This result can be traced back to Lagrange.

[2.1.2] Corollary. If G is a finite group and H is a subgroup, then $|H|$ divides $|G|$.

3 Homomorphisms

Homomorphisms are an important topic in algebra...

We begin our discussion by with a group $\langle G, * \rangle$. Let S be a set with the same cardinality as G, and let $f : S \to G$ be a bijection. Then we can turn S into a group by defining a binary operation $\star$ on S by

$$s_1 \star s_2 = f^{-1}(f(s_1) * f(s_2)) \qquad \forall s_1, s_2 \in S.$$

[3.0.1] Example. Let R be the set of positive real numbers excluding 1, and define a binary operation on R by $a \star b = a^{\ln b}$. We'll show that $(R, \star)$ is a group by finding a bijection f from R to a well known group and showing that $\star$ is an operation of the form defined in the proposition. Define $f : R \to \mathbb{R}^{\times}$ by $f(r) = \ln r$. Then f is a bijection and

$$r_1 \star r_2 = r_1^{\ln r_2} = e^{\ln r_1 \ln r_2} = f^{-1}(f(r_1) * f(r_2)),$$

so by our work above, we know that $(R, \star)$ is a group.

[3.0.2] Example. Let R be the same set as in Example 3.0.1, and define an operation on R by $a * b = ab - a - b + 2$. Then $(S, *)$ is a group. The correct bijection is $f : R \to \mathbb{R}^\times$ defined by $f(r) = r - 1$.

Intuitively, what we are doing is "borrowing" the operation from G by mapping our elements in S to G, taking their product, then pulling back to S. We can think of f as a relabeling of the elements of G or vice versa. That is, $\langle G, * \rangle$ and $\langle S, \star \rangle$ are essentially the same group, their only difference being how the elements are labeled. We want to generalize this notion of "sameness" of groups, and to do so we introduce the following definition.

[3.0.3] Definition. Let $\langle G, * \rangle$ and $\langle H, \star \rangle$ be groups. A function $f : G \to H$ is called a *homomorphism* if $f(a * b) = f(a) \star f(b)$ for all $a, b \in G$.

4 Group Actions

Whenever we have a set X equipped with some kind of algebraic structure, it is interesting to study its set of automorphisms (i.e. the set of structure preserving bijections from $X \to X$). This set is denoted $\mathrm{Aut}X$. Let G be a group and let X be a set with any kind of algebraic structure. A homomorphism $G \to \mathrm{Aut}X$ is a *group action*. In this section we will focus on studying groups acting on sets without considering the algebraic structure, i.e., we will be studying homomorphisms $G \to S_X$. That said, we will be doing so in a slightly different way by redefining what we mean by a group action in the context of sets.

[4.0.1] Definition. Let G be a group and let X be a set. A group action of G on X is a map $\mu : G \times X \to X$ (written $\mu : (g, x) \mapsto g \cdot x$) such that for all $g, h \in G$ and $x \in X$

1. $g \cdot (h \cdot x) = (gh) \cdot x$
2. $e \cdot x = x$

We say that G acts on X if there is a map satisfying the two axioms above.

Technically, the definition we gave is that of a *left* group action. Similarly, we may define a right group action as a map $X \times G \to X$ (written $(x, g) \mapsto x \cdot g$) satisfying $x \cdot e = x$ and $(x \cdot g) \cdot h = x \cdot (gh)$ for all $g, h \in G$ and $x \in X$. However, one can verify that every right group action can be realized as a left group action, and vice versa. Hence, whenever we speak of a group action, we mean a left group action unless otherwise specified.

[4.0.2] Exercise. Let $\rho : X \times G \to X$ be a right group action. Show that $\mu : G \times X \to X$ given by $\mu(g, x) = \rho(x, g^{-1})$ defines a left group action.

With these remarks out of the way, let's take a look at some examples of group actions.

[4.0.3] Example (The trivial action)**.** Every group G acts on any nonempty set X in the trivial way. Namely, $g \cdot x = x$ for all $g \in G$ and $x \in X$. Admittedly, this is not a very interesting action. But given a set X, it may be interesting to ask which groups must act on trivially on X. Or given a group G, we may ask what sets must G act trivially on.

[4.0.4] Example. Let $G = \mathbb{Z}/3$ and $X = \mathbb{Z}^3$. Then G acts on X via the rule

$$k \cdot (x_1, x_2, x_3) = (x_{1+k}, x_{2+k}, x_{3+k})$$

where the indices are reduced mod 3.

[4.0.5] Example. Let X be a nonempty set. The symmetric group S_n acts on X^n via the rule

$$\sigma \cdot (x_i) = (x_{\sigma^{-1}(i)}).$$

Indeed, let $\sigma, \tau \in S_n$ and $(x_i) \in X^n$. Write $y_i = x_{\tau^{-1}(i)}$ for all i. Then

$$\sigma \cdot (\tau \cdot (x_i)) = \sigma \cdot (x_{\tau^{-1}(i)}) = \sigma \cdot (y_i) = (y_{\sigma^{-1}(i)}) = (x_{\tau^{-1}(\sigma^{-1}(i))}) = (x_{(\sigma\tau)^{-1}(i)}) = (\sigma\tau) \cdot (x_i).$$

Since $\iota \cdot (x_i) = (x_{\iota(i)}) = (x_i)$, we have a group action, as claimed.

The above example could be considered a special case of the following.

[4.0.6] Example. If G acts on a set X, and Y is any set. Given any $g \in G$ and $f \in Y^X$ let ${}^g f$ denote the function which maps $x \mapsto g^{-1} \cdot x$. Then G acts on Y^X by the rule

$$g \cdot f = {}^g f.$$

To see this, let $g, h \in G$ and $f \in Y^X$. For any $x \in X$ we have ${}^e f(x) = f(x)$ and

$${}^g({}^h f)(x) = {}^h f(g^{-1}x) = f(h^{-1}g^{-1}x) = f((gh)^{-1}x) = {}^{gh} f(x).$$

So $e \cdot f = f$ and $g \cdot (h \cdot f) = (gh) \cdot f$.

The previous example is indeed a special case of this one since elements of X^n are the same thing as functions $\{1, \dots, n\} \to X$. The group S_n acts on the set $\{1, \dots, n\}$ in the natural way.

We will now show that the element-wise definition of a group action coincides with the object-wise one given at the beginning of the chapter. Let the group G act on the set X. Show that actions are homomorphisms into $\mathrm{Aut}X$, which is S_X.

4.1 Orbits, Stabilizers, Counting

In what follows, we introduce some basic notions about group actions.

[4.1.1] Exercise. Let G be a group acting on a set X. Show that the relation on X defined by

$$x \sim y \iff x = g \cdot y \text{ for some } g \in G$$

is an equivalence relation.

The equivalence class of $x \in X$ under the relation defined in the exercise is called the *orbit* of x and is denoted O_x. Hence X is a disjoint union of orbits under the action of G. The *stabilizer* of x, denoted G_x, is the set of elements of G that fix x: $G_x = \{g \in G \mid g \cdot x = x\}$.

We may also talk about fixed sets of X. For example, for any $g \in G$ the symbol X^g denotes the set of elements of X that are fixed by g. That is, $X^g = \{x \in X \mid g \cdot x = x\}$. More generally, given subsets $H \subseteq G$ and $Y \subseteq X$, we define $Y^H = \{y \in Y \mid h \cdot y = y \text{ for all } h \in H\}$. It is clear that $Y^H = \bigcap_{h \in H} Y^h$.

When G acts on a finite set X, it is useful to have a notation for the number of orbits of size k. We will write m_k for this number. Hence $|X/G| = \sum_k m_k$ and $|X| = \sum_k k m_k$.

[4.1.2] Exercise. Prove that G_x is a subgroup of G.

[4.1.3] Theorem (Orbit-Stabilizer Theorem)**.** Suppose a group G acts on a set X. For any $x \in X$ we have $|O_x| = [G : G_x]$. In particular if G is finite, then $|G| = |O_x| \cdot |G_x|$.

Proof: Since $gG_x = hG_x \iff h^{-1}g \in G_x \iff h^{-1}g \cdot x = x \iff g \cdot x = h \cdot x$, the map $G/G_x \to O_x$ given by $gG_x \mapsto g \cdot x$ is bijective. If G is finite, then $[G : G_x] = |G|/|G_x|$ so we are done. □

The Orbit-Stabilizer theorem tells us that the size of an orbit always divides the order of the group.

[4.1.4] Proposition. Let H, K be finite subgroups of a group G. Then

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

Proof: For any $(h, k) \in H \times K$ and $x \in HK$, define $(h, k) \cdot x = hxk^{-1}$. This defines a group action. For any $hk \in HK$ we have $(h, k^{-1}) \cdot e = hk$, so every element of HK belongs to the orbit of e. Hence the action is transitive. The stabilizer of e is the set

$$\left\{(h, k) \in H \times K \;\middle|\; hek^{-1} = e\right\} = \{(h, k) \in H \times K \mid h = k\} = \{(h, h) \in H \times K \mid h \in H \cap K\},$$

which has $|H \cap K|$ elements. The orbit-stabilizer theorem then implies

$$|HK| = |O_e| = \frac{|H \times K|}{|(H \times K)_e|} = \frac{|H||K|}{|H \cap K|}.$$

□

[4.1.5] Exercise. Let $n \geq 1$, and let $\binom{n}{k}$ denote the number of k-element subsets of $\{1, \ldots, n\}$. Show that if $k \in \{1, \ldots, n\}$, then

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

[Hint: Consider the natural action of S_n on the collection of k-element subsets of $\{1, \ldots, n\}$. Show that this action is transitive and that the stabilizer of $\{1, \ldots, k\}$ is isomorphic to $S_k \times S_{n-k}$.]

[4.1.6] Exercise (Dummit and Foote, 4.3.33)**.** This exercise gives a formula for the size of each conjugacy class in S_n. Let σ be a permutation in S_n and let $m_1, \ldots, m_s$ be the *distinct* integers which appear in the cycle type of σ (including 1-cycles). For each $i \in \{1, \ldots, s\}$ assume σ has k_i cycles of length m_i (so that $\sum_{i=1}^{s} k_i m_i = n$). Prove that the number of conjugates of σ is

$$\frac{n!}{\prod_{i=1}^{s} k_i! m_i^{k_i}}.$$

[4.1.7] Exercise. Let $\lambda \vdash n$. For any $k \in \{1, \ldots, n\}$, let p_k denote the number of parts of λ that equal k. Prove that the number of permutations in S_n of cycle type λ is

$$\frac{n!}{\prod_k k^{p_k} p_k!}.$$

Conclude that the order of the centralizer of a permutation of cycle type λ is $\prod_k k^{p_k} p_k!$.

[4.1.8] Proposition. Suppose G is a finite group acting on a finite set X. Then

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Proof: Consider the set $S = \{(g, x) \in G \times X \mid g \cdot x = x\}$. We can count the number of elements in S by summing over G or by summing over X. Considering both counts gives

$$|S| = \sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|.$$

Using the equality above and the orbit-stabilizer theorem, we have

$$\frac{1}{|G|} \sum_{g \in G} |X^g| = \sum_{x \in X} \frac{|G_x|}{|G|} = \sum_{x \in X} \frac{1}{|O_x|}.$$

The conclusion follows from the more general fact given in the exercise below. □

[4.1.9] Exercise. Suppose $\sim$ is an equivalence relation on a set X. Show that

$$|X/\sim| = \sum_{x \in X} \frac{1}{|x/\sim|}.$$

4.2 Conjugation

Let $g, a \in G$. Define

$$g^a = a^{-1} g a.$$

Then

$$(g^a)^b = b^{-1} g^a b = b^{-1} a^{-1} g a b = (ab)^{-1} g (ab) = g^{ab}.$$

4.3 The Function Action

Let $f : G \to H$ be a function between groups. For $a \in G$ define a new function $f^a : G \to H$ via the rule

$$f^a(x) = f(a)^{-1} f(ax).$$

Then

$$(f^a)^b(x) = f^a(b)^{-1} f^a(bx) = (f(a)^{-1} f(ab))^{-1} f(a)^{-1} f(abx) = f(ab)^{-1} f(abx) = f^{ab}(x).$$

We say that a function between groups is *identity preserving* if the map sends the identity to the identity. Note that for any $a \in G$ we have $f^a(e) = f(a)^{-1} f(ae) = f(a)^{-1} f(a) = e$, so f^a is always identity preserving. Furthermore if f is identity preserving, then $f(x) = f(e)^{-1} f(ex) = f^e(x)$ for all x. Hence G acts on the set of identity preserving maps $G \to H$.

[4.3.1] Exercise. Prove that an identity preserving function $f : G \to H$ is a group homomorphism if and only if the size of the orbit of f under the function action is 1.

[4.3.2] Exercise. Show that if f is a bijection, then so is f^x. Hence G acts on the set of identity preserving bijections from $G \to H$.

Reference: https://arxiv.org/pdf/1506.07235.pdf

4.4 Actions of p-groups

[4.4.1] Theorem (Fixed Point Congruence)**.** Let G be a finite p-group acting on a finite set X. Then

$$|X| \equiv m_1 \pmod{p}.$$

Proof: Let the orbits in X be $O_1, O_2, \ldots, O_t$ so that

$$|X| = \sum_{i=1}^{t} |O_i|.$$

Since G is a p-group, the Orbit-Stabilizer theorem implies that $|O_i|$ is a power of p for every i. Then reducing the equation above modulo p counts the number of orbits of size 1, which is m_1. □

[4.4.2] Theorem (Cauchy)**.** Let G be a finite group and p a prime divisor of $|G|$. Then G has an element of order p.

Proof: Let X be the set of identity preserving functions from $\mathbb{Z}/p\mathbb{Z}$ to G. Then G acts on X via the function action. Note that since $|G|$ is divisible by p, $|X| = |G|^{p-1} \equiv 0 \pmod{p}$. Hence by the fixed point congruence theorem, the number of orbits of size 1 is a multiple of p. Since the trivial homomorphism $\mathbb{Z}/p\mathbb{Z} \to G$ belongs to an orbit of size 1, there must be at least $p-1$ other orbits of size 1. These correspond to non-trivial homomorphisms from $\mathbb{Z}/p\mathbb{Z} \to G$, and the existence of these implies the existence of an element of order p. □

5 Quotient Groups

Fundamental to the theory of numbers is the tool of modular arithmetic. Fix an integer n. We define an equivalence relation $\equiv$ on $\mathbb{Z}$ by $a \equiv b$ if and only if $a-b$ is divisible by n (which is to say that $a-b \in n\mathbb{Z}$). The important property of $\equiv$ is that it plays nicely with addition: if a, b, c, d are integers such that $a \equiv b$ and $c \equiv d$, then $a+c \equiv b+d$ since $a+c-(b+d) = (a-b)+(c-d) \in n\mathbb{Z}$. Now, $\mathbb{Z}/{\equiv}$ is a set with n elements. We can turn this set into a group by defining the multiplication $\overline{x}\,\overline{y} = \overline{xy}$.

In essence, we have formed a group out of equivalence classes. This motivates the following definition.

[5.0.1] Definition. Let G be a group. A *congruence* on G is an equivalence relation $\sim$ which satisfies the following two *compatibility properties*:

1. If $g_1 \sim g_2$ and $h_1 \sim h_2$, then $g_1h_1 \sim g_2h_2$.
2. If $g_1 \sim g_2$, then $g_1^{-1} \sim g_2^{-1}$.

[5.0.2] Definition. Let $\sim$ be a congruence on a group G. Then the *quotient group of G by $\sim$* is the group whose elements are in the set $G/{\sim}$ and whose operation is given by $(a/{\sim})(b/{\sim}) = ab/{\sim}$.

[5.0.3] Definition. A subgroup N of a group G is called *normal* if $gNg^{-1} = N$ for all $g \in G$.

[5.0.4] Proposition. If $\sim$ is a congruence on G, then $e/{\sim}$ is a normal subgroup. Moreover, given a normal subgroup N, the relation $\sim$ on G defined by $a \sim b$ if and only if $ab^{-1} \in N$ is a congruence.

Proof: Suppose $\sim$ is a congruence on G. If $a \sim b$ and $b \sim e$, then $ab^{-1} \sim e$, so $e/{\sim}$ is a subgroup of G. To show that it is normal, let $g \in G$ and let $n \in e/{\sim}$. Then $gng^{-1} \sim geg^{-1} = e$.

For the second part of the statement, verifying that $\sim$ is an equivalence relation is trivial. To show that $\sim$ is a congruence, suppose $n_1 \sim n_2$ and $m_1 \sim m_2$, so $n_1 n_2^{-1}$ and $m_1 m_2^{-1}$ are elements of N. Since N is normal, there is some $m' \in N$ such that $n_2(m_1 m_2^{-1})n_2^{-1} = m'$. Then

$$n_1 m_1 (n_2 m_2)^{-1} = n_1 m_1 m_2^{-1} n_2^{-1} = n_1 n_2^{-1} m' \in N$$

so $n_1 m_1 \sim n_2 m_2$. To finish the proof, we have $(n_1 n_2^{-1})^{-1} = n_2 n_1^{-1} \in N$, so since N is normal, $n_1^{-1}(n_2 n_1^{-1})n_1 = n_1^{-1} n_2 \in N$. That is, $n_1^{-1} \sim n_2^{-1}$, so $\sim$ is a congruence. □

We now make the connection between homomorphisms with congruence relations.

[5.0.5] Definition. Let $\varphi : G \to H$ be a group homomorphism. The *redundancy of* φ is the relation $\sim$ on G defined by $a \sim b$ iff $\varphi(a) = \varphi(b)$.

[5.0.6] Proposition. Let $\varphi : G \to H$ be a group homomorphism. Then the redundancy of φ is a congruence on G.

Proof: Let $\sim$ denote the redundancy of φ. Clearly $\sim$ is an equivalence relation. Now suppose $g_1 \sim g_2$ and $h_1 \sim h_2$. Then $\varphi(g_1 h_1) = \varphi(g_1)\varphi(h_1) = \varphi(g_2)\varphi(h_2) = \varphi(g_2 h_2)$, so $g_1 h_1 \sim g_2 h_2$. Also, $\varphi(g_1^{-1}) = \varphi(g_1)^{-1} = \varphi(g_2)^{-1} = \varphi(g_2^{-1})$, so $g_1^{-1} \sim g_2^{-1}$. □

[5.0.7] Theorem (First Isomorphism Theorem)**.** Let $\varphi : G \to H$ be a homomorphism, and let $\sim$ be the redundancy of φ. Then $G/\!\sim\, \simeq \operatorname{Im}\varphi$.

Proof: Define $\phi : G/\!\sim\, \to \operatorname{Im}\varphi$ by $\phi(g/\!\sim) = \varphi(g)$. If $\phi(a/\!\sim) = \phi(b/\!\sim)$, then $\varphi(a) = \varphi(b)$, so $a/\!\sim\, = b/\!\sim$. Thus ϕ is an injection, and since it is clearly a surjection, ϕ is a bijection. Now let $a/\!\sim, b/\!\sim\, \in G/\!\sim$. Then

$$\phi((a/\!\sim)(b/\!\sim)) = \phi(ab/\!\sim) = \varphi(ab) = \varphi(a)\varphi(b) = \phi(a/\!\sim)\phi(b/\!\sim),$$

so ϕ is an isomorphism. □

6 Exact Sequences

[6.0.1] Definition. A sequence of groups and homomorphisms

$$\begin{tikzcd} \cdots \arrow[r, "\phi_{i-2}"] & G_{i-1} \arrow[r, "\phi_{i-1}"] & G_i \arrow[r, "\phi_i"] & G_{i+1} \arrow[r, "\phi_{i+1}"] & \cdots \end{tikzcd}$$

is said to be *exact at* G_n if $\operatorname{Im}\phi_{n-1} = \operatorname{Ker}\phi_n$. The sequence is said to be *exact* if it is exact at every G_i, except an initial source or final target.

An exact sequence of groups need not be finite. However, the sequences that we are interested will be. In fact, we will almost exclusively be working with exact sequences of a specific length.

[6.0.2] Definition. A *short exact sequence* is an exact sequence of the form

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\varphi"] & B \arrow[r, "\psi"] & C \arrow[r] & 1 \end{tikzcd}$$

where 1 represents the trivial group.

Let's figure out exactly (pun intended) what a sequence of this form is telling us. Notice that we did not specify the first and last homorphisms in the sequence. This is because there is only one possible choice for each of these: the trivial map. Exactness at A tells us that the image of the trivial map is the kernel of φ, i.e., $\operatorname{Ker}\varphi = \{e\}$. But this is equivalent to saying that φ is injective! On the other hand, exactness at C tells us that the image of ψ is the kernel of the trival map. But the kernel of the trivial map is all of its domain, so $\operatorname{Im}\psi = C$. That is, ψ is surjective.

[6.0.3] Example. Let G be a group and N a normal subgroup. Let $\iota : N \to G$ be the natrual inclusion, and let $\pi : G \to G/N$ be the natural projection. Then

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] & G/N \arrow[r] & 1 \end{tikzcd}$$

is a short exact sequence since ι is injective, π is surjective, and $\operatorname{Im}\iota = N = \operatorname{Ker}\pi$.

[6.0.4] Theorem (Splitting Headache)**.** Consider the short exact sequence of groups

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\varphi"] & B \arrow[r, "\psi"] & C \arrow[r] & 1 \end{tikzcd}$$

If B is abelian, then the following are equivalent:

1. There is a homomorphism $\varphi' : B \to A$ such that $\varphi' \circ \varphi = \mathrm{Id}_A$.
2. There is a homomorphism $\psi' : B \to C$ such that $\psi \circ \psi' = \mathrm{Id}_C$.
3. $B \simeq A \times C$.

Proof: We will show that (1) $\iff$ (3) and (2) $\iff$ (3).

(1 $\Rightarrow$ 3) For any $b \in B$ we have $\varphi(\varphi'(b))^{-1}b \in \operatorname{Ker}\varphi'$, so that $B = \operatorname{Im}\varphi \operatorname{Ker}\varphi'$. Now suppose $h \in \operatorname{Im}\varphi \cap \operatorname{Ker}\varphi'$, i.e., $h = \varphi(a)$ for some $a \in A$ and $\varphi'(h) = e$. Then $a = \varphi'(\varphi(a)) = \varphi'(h) = e$, so $h = \varphi(e) = e$, and thus $\operatorname{Im}\varphi \cap \operatorname{Ker}\varphi' = \{e\}$. Since B is abelian, $\operatorname{Im}\varphi$ and $\operatorname{Ker}\varphi'$ are normal subgroups. Therefore, $B = \operatorname{Im}\varphi \operatorname{Ker}\varphi' \simeq \operatorname{Im}\varphi \times \operatorname{Ker}\varphi'$. Now $\operatorname{Ker}\varphi' \simeq B/\operatorname{Im}\varphi = B/\operatorname{Ker}\psi \simeq C$, so $B \simeq \operatorname{Im}\varphi \times \operatorname{Ker}\varphi' \simeq A \times C$.

(3 $\Rightarrow$ 1) Let $f : B \to A \times C$ be an isomorphism. Let $g : A \times C \to A$ be the natural projection. Let $a \in A$. Since $A \simeq \operatorname{Im}\varphi$, necessarily $f(\varphi(a)) = (a, e)$. So $(g \circ f)(\varphi(a)) = g(a, e) = a$. Thus taking $\varphi' = g \circ f$ does the trick.

(2 $\Rightarrow$ 3)

(3 $\Rightarrow$ 2) □

[6.0.5] Remark. The assumption that B is abelian in Theorem 6.0.4 is paramount. We need $\operatorname{Im}\varphi$ and $\operatorname{Im}\psi'$ to be a normal subgroups in order to form the direct product. There is a more general form of Theorem 6.0.4 which involves semidirect products, but we don't need that much generality for what we are trying to prove.

7 Finite Abelian Groups

Throughout this section, G denotes a finite abelian group.

[7.0.1] Proposition. Let $S \subseteq G$. The order of $\langle S \rangle$ divides the product of the orders of the elements of S.

Proof: Write $S = \{s_1, \ldots, s_t\}$. Define $S_k = \langle s_1, \ldots, s_k \rangle$ and $m_k = \prod_{j=1}^{k} |s_j|$. It is clear that $|S_1|$ divides $m_1 = |s_1|$. Moreover, if $|S_i|$ divides m_i for some i, then the second isomorphism theorem implies

$$|S_{i+1}| = |S_i \langle s_{i+1} \rangle| = \frac{|S_i||\langle s_{i+1} \rangle|}{|S_i \cap \langle s_{i+1} \rangle|}$$

divides m_{i+1}. Hence S_k divides m_k for all k. In particular, $|S_t|$ divides m_t, and this is what the proposition states. □

[7.0.2] Theorem. If p is a prime dividing $|G|$, then G has an element of order p.

Proof: Write $G = \langle g_1, \ldots, g_t \rangle$ and let $m = \prod_{j=1}^{t} |g_j|$. By Proposition 7.0.1, $|G|$ divides m, so p divides m. It follows that p divides $|g_j|$ for some j, so $|g_j| = pd$ for some integer d. Then g_j^d is an element of order p. □

[7.0.3] Lemma. Let G be a finite abelian group. The order of any element in G divides the maximal order of the elements of G.

Proof: First we will show that if G contains elements g_1 and g_2 of order n_1 and n_2, respectively, then G contains an element of order $\operatorname{lcm}(n_1, n_2)$. Begin by factoring n_1 and n_2 into primes:

$$n_1 = p_1^{a_1} \cdots p_r^{a_r} \qquad n_2 = p_1^{b_1} \cdots p_r^{b_r}.$$

Now define

$$k_1 = \prod_{a_i \geq b_i} p_i^{a_i} \qquad k_2 = \prod_{a_i < b_i} p_i^{b_i}.$$

Note that $k_1 k_2 = \operatorname{lcm}(n_1, n_2)$ and $\gcd(k_1, k_2) = 1$. By construction, $g_1^{n_1/k_1}$ has order k_1 and $g_2^{n_2/k_2}$ has order k_2. Since k_1 and k_2 are relatively prime, the order of $g_1^{n_1/k_1} g_2^{n_2/k_2}$ is $k_1 k_2 = \operatorname{lcm}(n_1, n_2)$ as desired.

Now let $g \in G$ be an element of maximal order m, and let $h \in G$ have order n. We wish to show that $n|m$. By the previous paragraph, we know that there is an element $a \in G$ such that $|a| = \operatorname{lcm}(m, n) \geq m$. Since m is maximal, we have $|a| \leq m$, so $|a| = m$. That is, $\operatorname{lcm}(m, n) = m$. Thus $n|m$, which is what we wanted to show. □

[7.0.4] Lemma. Let G be a finite abelian group, let g be an element of maximal order, and let $N = \langle g \rangle$. Then there is a homomorphism $\rho : G \to N$ such that ρ is the identity map on N.

Proof: Since G is finite, it is finitely generated: $G = \langle g, g_1, \ldots, g_t \rangle$ for some $g_1, \ldots, g_t \in G$. We can assume that none of the g_i's are in N. □

[7.0.5] Theorem (Classification of Finite Abelian Groups)**.** Every finite abelian group G is isomorphic to a direct product of cyclic groups. In particular,

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z},$$

where $n_j | n_{j-1}$ for all $2 \leq j \leq t$.

Proof: The proof is by induction on $|G|$. The result is trivial when $|G| = 2$. Suppose the statement is true for all abelian groups of order strictly less than $|G|$. If G is cyclic, then there is nothing to prove, so suppose otherwise. Let $g \in G$ be an element of maximal order m, and let $N = \langle g \rangle$. Now consider the short exact sequence of abelian groups

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] & G/N \arrow[r] & 1 \end{tikzcd}$$

where ι is the inclusion map and π is the natural projection. By Lemma 7.0.4, there is a homomorphism $\rho : G \to N$ such that $\rho \circ \iota = \mathrm{Id}_N$, so the sequence splits: $G \simeq N \times G/N$. By the induction hypothesis,

$$G/N \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

where $n_s | n_{s-1} | \cdots | n_1$. Since n_1 is the order of an element of G/N, it follows by Lemma 7.0.3 that $n_1 | m$. Thus

$$G \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

where $n_s | n_{s-1} | \cdots | n_1 | m$, completing the induction. □

[7.0.6] Exercise. Let $G = \{\sigma_1, \ldots, \sigma_n\}$ be an abelian subgroup of S_n and let $x_1, \ldots, x_n \in R$. Let $A = [\sigma_i(x_j)]$. Prove that $\det(A)$ is a product of n linear factors.

8 n-abelian Groups

A group G is called n-abelian if $(ab)^n = a^n b^n$ for all $a, b \in G$.
https://math.stackexchange.com/a/132813
https://math.stackexchange.com/a/929123
https://math.stackexchange.com/a/41004
https://ysharifi.wordpress.com/2018/11/11/groups-satisfying-xynxnyn/

[8.0.1] Exercise. Prove that if G is n, $n+1$, and $n+2$-abelian for some n, then G is abelian.

[8.0.2] Exercise. Suppose G is a finite, n-abelian group. Show that if $(|G|, n(n-1)) = 1$, then G is abelian.

9 Permutation Groups

- Cycle decomposition.
- Cycle Type. Bijection with partitions of n. $(\bullet\ \bullet\ \bullet)(\bullet\ \bullet\ \bullet)(\bullet\ \bullet)$

Let X be a set, and denote by S_X the set of all bijections from X to X. Elements of S_X are called *permutations of* X. If X is a finite set, say $|X| = n$, then it is easy to see that $|S_X| = n!$.

[9.0.1] Proposition. Every permutation is a product of disjoint cycles.

[9.0.2] Theorem. For $n > 1$ there is a unique nontrivial homomorphism $\text{sgn} : S_n \to \mathbb{C}^\times$, called the sign homomorphism.

Proof: Recall that S_n acts linearly on $\mathbb{C}[X_1, \ldots, X_n]$ by permuting the X_i's. Consider the polynomial

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

Note that since Δ contains one factor $X_i - X_j$ for all $i < j$, $\sigma\Delta$ must contain either $X_i - X_j$ or $X_j - X_i = -(X_i - X_j)$, but not both, for all $i < j$. Hence

$$\sigma\Delta = \prod_{i<j} (X_{\sigma(i)} - X_{\sigma(j)}) = \pm\Delta$$

for all $\sigma \in S_n$. Hence S_n acts on the set $\{\Delta, -\Delta\}$. Let $\text{sgn} : S_n \to \mathbb{C}^\times$ be such that $\sigma(\Delta) = \text{sgn}(\sigma)\Delta$ for all $\sigma \in S_n$. Then for any $\sigma, \tau \in S_n$ we have

$$\text{sgn}(\sigma\tau)\Delta = \sigma\tau\Delta = \sigma(\tau\Delta) = \sigma(\text{sgn}(\tau)\Delta) = \text{sgn}(\tau)\sigma\Delta = \text{sgn}(\tau)\text{sgn}(\sigma)\Delta.$$

Hence $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$, so sgn is a homomorphism. It is easy to see that $(1\ 2) \cdot \Delta = -\Delta$, so $\text{sgn}((1\ 2)) = -1$, so sgn is nontrivial.

To establish uniqueness, suppose $f : S_n \to \mathbb{C}^\times$ is a non-trivial homomorphism. Let $\tau \in S_n$ be any two-cycle. We claim that f is completely determined by its value at τ. Indeed, we could write any $\sigma \in S_n$ as a product of two-cycles $\sigma = \tau_1 \cdots \tau_j$. Since all two-cycles are conjugate, there exist $\rho_1, \ldots, \rho_j \in S_n$ such that $\tau_i = \rho_i \tau \rho_i^{-1}$ for all $i = 1, \ldots, j$. Since $\mathbb{C}^\times$ is commutative, we have that $f(\tau_i) = f(\rho_i \tau \rho_i^{-1}) = f(\rho_i) f(\tau) f(\rho_i)^{-1} = f(\rho_i) f(\rho_i)^{-1} f(\tau) = f(\tau)$ for all i. Thus

$$f(\sigma) = f(\tau_1 \cdots \tau_j) = f(\tau_1) \cdots f(\tau_j) = f(\tau) \cdots f(\tau) = f(\tau)^j,$$

showing that f is determined by its value at τ, as claimed. Finally, since $|\tau| = 2$, we must have $f(\tau) = \pm 1$. By our work above, we know that if $f(\tau) = 1$, then f is the trivial map. Since f is nontrivial, we must have $f(\tau) = -1$. Note then that $f((1\ 2)) = -1 = \operatorname{sgn}((1\ 2))$, so f is the sign homomorphism. □

We call the kernel of sgn the *alternating group on n elements* and denote it by A_n. In practice, one does not calculate the sign of a permuation using the construction in (9.0.2). Instead one uses the following observation. Let $k > 1$ and let $\sigma = (a_1\ \cdots\ a_k)$ be a k-cycle in S_n. Write $\tau_j = (a_j\ a_{j+1})$ for all $j = 1, \ldots, k-1$. Then $\sigma = \tau_1 \cdots \tau_{k-1}$. Hence $\sigma \in A_n$ if and only if k is odd.

10 Misc

https://math.stackexchange.com/a/2094996

11 Construction Problems

Given groups A, B, C and homomorphisms $f : A \to B$ and $g : A \to C$, when does there exist a homomorphism $h : B \to C$ such that $g = h \circ f$?

$$\begin{tikzcd}
& A \arrow[ld, "f"'] \arrow[rd, "g"] & \\
B \arrow[rr, dashed, "h"'] & & C
\end{tikzcd}$$

Consider the case where $C = A$ and $g = \iota_A$. The problem becomes: when does there exist a homomorphism $h : B \to A$ such that $\iota_A = h \circ f$?

An application is finding all homomorphisms from $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ for any $m, n \geq 1$.

There are n homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/n$. They are given by $g_0, g_1, \ldots, g_k, \ldots, g_{n-1}$, where $g_k : \mathbb{Z} \to \mathbb{Z}/n$ is defined by $g_k(j) = \overline{jk}$ for all $j \in \mathbb{Z}$. Fix $k \in \{0, 1, \ldots, n-1\}$. Write $d = \gcd(n, k)$ and $r = n/d$. Then $\ker(g_k) = r\mathbb{Z}$ and the image of g_k is the subgroup $d(\mathbb{Z}/n)$ of order r.

$$\begin{tikzcd}
& \mathbb{Z} \arrow[ld, "f"'] \arrow[rd, "g_k"] & \\
\mathbb{Z}/m\mathbb{Z} \arrow[rr, dashed, "h"'] & & \mathbb{Z}/n\mathbb{Z}
\end{tikzcd}$$

12 Miscellaneous Problems

[12.0.1] Exercise. Let G be a group of order $p(p+1)$, where p is a prime. Show that G has either a normal subgroup of order p or one of order $p+1$.

Solution. For any divisor d of $|G|$, let L_d be the set of elements of order d in G. Hence $|G| = \sum_{d|n} |L_d|$. Suppose G does not have a normal subgroup of order p. We will show that G has a normal subgroup of order $p+1$. More specifically, we will show that $p+1$ is a power of a prime q, and that $n_q = 1$.

To begin, since $\gcd(p, p+1) = 1$, we have $n_p \mid p+1$ and $n_p \equiv 1 \mod p$ by the Sylow theorems. Since we are assuming $n_p \neq 1$, then necessarily $n_p = p+1$. Note that each Sylow p-subgroup is cyclic of prime order and contains $p-1$ elements of order p. Any two Sylow p-subgroups intersect trivially, so

$$|L_p| = n_p(p-1) = (p+1)(p-1) = p^2 - 1.$$

Now let q be a prime divisor of $p+1$. By Cauchy's theorem, G contains an element x of order q. Let $P \in \mathrm{Syl}_p(G)$ and let $y \in P$ be a non-identity element. Note that

$$|G : N_G(P)| = n_p = p+1 = |G : P|,$$

so $N_G(P) = P$. In particular, this implies that x and y do not commute since otherwise x would be an element of $N_G(P)$. Hence $x, x^y, x^{y^2}, \ldots, x^{y^{p-1}}$ are p distinct elements of order q. Hence $|L_q| \geq p$, so we have

$$|L_1 \cup L_p \cup L_q| = |L_1| + |L_p| + |L_q| \geq 1 + (p^2 - 1) + p = p(p+1) = |G|.$$

This implies that the inequality $|L_q| \geq p$ is actually an equality. Hence $G = L_1 \cup L_p \cup L_q$ and so the only prime divisors of $|G|$ are p and q. So we actually have $p+1 = q^m$ for some $m \geq 1$. Now let $Q \in \mathrm{Syl}_q(G)$. Then $Q \subseteq L_1 \cup L_q$ since $Q \cap L_p = \varnothing$. But

$$|Q| = q^m = p+1 = |L_1| + |L_q| = |L_1 \cup L_q|.$$

Hence we have $Q = L_1 \cup L_q$, showing that Q is the only Sylow q-subgroup. □

[12.0.2] Exercise. Let G be a group of order $p^2 + pq$, where p and q are primes with $p \geq q$. Show that G is not simple.

Solution. First suppose $p = q$. Then $|G| = 2p^2$. If $p = 2$, then G is a p-group and hence has non-trivial center, so G is not simple. If $p \neq 2$, then $n_p \mid 2$ implies $n_p = 1$ or $n_p = 2$. However, we also have $n_p \equiv 1 \mod p$, so we cannot have $n_p = 2$. Thus $n_p = 1$ in this case, and G is not simple.

Now suppose $p > q$. Then $\gcd(p, p+q) = \gcd(p, q) = 1$. Hence $n_p \mid p+q$. We also have $n_p \equiv 1 \mod p$. Since $p + q < 2p$, then $n_p = 1$ or $n_p = p+1$. But clearly $p+1$ does not divide $p+q$. So we must have $n_p = 1$, so G is not simple. □

[12.0.3] Exercise. Let n be a positive integer. Show that the dihedral group of order 2^{n+1} is nilpotent of class n. (A group G is called nilpotent of class n if $G_{n+1} = \{1\}$ but $G_n \neq \{1\}$, where $G_1 = G$ and recursively $G_{k+1} = [G, G_k]$. You may use the fact that if p is a prime and the order of a group G is p^m, then $G_m = \{1\}$.)

Solution. Let $G = \langle r, s \mid r^{2^n} = s^2 = (sr)^2 = 1 \rangle$ be the standard presentation for the dihedral group of order 2^{n+1}. We claim that $G_{k+1} = \langle r^{2^k} \rangle$ for $1 \leq k \leq n$. The proof is by induction. First note that

$$r^2 = rs^2r = rs(sr) = rs(sr)^{-1} = rsr^{-1}s^{-1} \in [G, G]$$

so $\left\langle r^2 \right\rangle \leq G_2$. But note that $\left\langle r^2 \right\rangle$ is a characteristic subgroup of the normal subgroup $\langle r \rangle$, so $\left\langle r^2 \right\rangle$ is a normal subgroup. We have $|G : \left\langle r^2 \right\rangle| = |G|/|r^2| = 2^{n+1}/2^{n-1} = 4$, so $G/\left\langle r^2 \right\rangle$ is a group of order 4, and hence abelian. It follows that $[G, G] \leq \left\langle r^2 \right\rangle$. Therefore $G_2 = [G, G] = \left\langle r^2 \right\rangle$.

For the inductive step, suppose $G_k = \langle r^{2^{k-1}} \rangle$ for some $1 < k < n$. Since elements of $\langle r \rangle$ commute with elements $G_k = \langle r^{2^{k-1}} \rangle$, to show the inclusion $G_{k+1} \leq \langle r^{2^k} \rangle$, it suffices to show that commutators of the form $[sr^m, r^{2^{k-1}j}]$ belong to $\langle r^{2^k} \rangle$. Indeed, let $\ell = 2^{k-1}j$. Then

$$\begin{aligned}
[sr^m, r^\ell] &= (sr^m)(r^\ell)(sr^m)^{-1}(r^\ell)^{-1} \\
&= (sr^{m+\ell})(sr^{m-\ell}) \\
&= s(r^{m+\ell}s)r^{m-\ell} \\
&= s(sr^{-m-\ell})r^{m-\ell} \\
&= r^{-2\ell} \\
&= r^{-2^k j}.
\end{aligned}$$

Hence $[G, G_k] \leq \langle r^{2^k} \rangle$. Letting $j = -1$ in the calculation above also shows that $r^{2^k} \in G_{k+1}$. Hence $G_{k+1} = \langle r^{2^k} \rangle$, completing the induction.

To finish, note that $G_n = \langle r^{2^{n-1}} \rangle \neq \{1\}$ and $G_{n+1} = \langle r^{2^n} \rangle = \{1\}$. Therefore G is nilpotent of class n. □

[12.0.4] Exercise. Let $G = \left\langle r, s \mid r^n = s^2 = (sr)^2 = 1 \right\rangle$ be the dihedral group of order $2n$. Show that $r^p s^q = s^q r^{(-1)^q p}$ for any $p, q \in \mathbb{Z}$.

[12.0.5] Exercise. Let G be a finite group. Show that the probability that two randomly chosen elements of G commute is $k(G)/|G|$, where $k(G)$ denotes the number of conjugacy classes of G.

Solution. Let $S := \left\{(g, h) \in G \times G \;\middle|\; ghg^{-1} = h\right\}$. Note that the probability that two randomly chosen elements of G commute is $P = |S|/|G|^2$. By (4.1.8), $k(G) = |S|/|G|$. So $P = k(G)/|G|$. □

[12.0.6] Exercise. Let G be a finite group, P a Sylow p-subgroup, and N a normal subgroup of G. Show that NP/N is a Sylow p-subgroup of G/N.

Solution.

□

[12.0.7] Exercise. Let G be a group and let $g \in G$. Suppose that for each group H and each element $h \in H$, there is a unique group homomorphism $\theta : G \to H$ such that $\theta(g) = h$. Show that G is abelian.

Solution. We claim that $G = \langle g \rangle$. Let $\iota : \langle g \rangle \to G$ be the inclusion map, and let $\theta : G \to \langle g \rangle$ be the unique homomorphism such that $\theta(g) = g$. Then $\theta \circ \iota : \langle g \rangle \to \langle g \rangle$ is a homomorphism satisfying $\theta(\iota(g)) = g$. Hence $\theta \circ \iota$ is the identity map. Similarly, since $\iota \circ \theta : G \to G$ is a homomorphism which fixes g, it must be the identity map by uniqueness. Hence $G = \langle g \rangle$. □

[12.0.8] Exercise. Let G be a finite group of order n. Show that if the number of elements $x \in G$ satisfying $x^d = 1$ is at most d for all divisors d of n, then G is cyclic.

Solution. For any divisor d of n, let L_d be the set of elements of order d in G. Note that if $a \in G$ is an element of order d, then all d elements of $\langle a \rangle$ satisfy the equation $x^d = 1$. Hence $L_d \subseteq \langle a \rangle$. But we know that $\langle a \rangle$ has $\varphi(d)$ elements of order d, so $|L_d| = \varphi(d)$. Since G is the disjoint union of the L_d's, we have

$$n = \sum_{d \mid n} |L_d| \leq \sum_{d \mid n} \varphi(d) = n.$$

Hence $|L_d| = \varphi(d)$ for all d dividing n. In particular, L_n is nonempty, so G is cyclic. □

[12.0.9] Exercise. Let H, K, and L be subgroups of a group G, with $H \subseteq K$. Assume $H \cap L = K \cap L$ and $HL = KL$. Prove $H = K$.

Solution. We claim that $K \cap HL = H(K \cap L)$. Since $H \subseteq K$ and $K \cap L \subseteq K$, we have $H(K \cap L) \subseteq K$. Since $K \cap L \subseteq L$, we have $H(K \cap L) \subseteq HL$. Hence $H(K \cap L) \subseteq K \cap HL$. Now suppose $g \in K \cap HL$ and write $g = hl$ with $h \in H$ and $l \in L$. Then $l = h^{-1}g \in HK \subseteq K$, so $g = hl \in H(K \cap L)$.

Now

$$K = K \cap KL = K \cap HL = H(K \cap L) = H(H \cap L) = H.$$

□

The exercise above is not pointless. It tells us that the lattice of normal subgroups of G is *modular*. Recall that a lattice L is modular if $a \leq b$ implies $a \vee (x \wedge b) = (a \vee x) \wedge b$ for all $a, b, x \in L$. In modular lattices, we have the property: $a \leq b$ with $a \wedge c = b \wedge c$ and $a \vee c = b \vee c$ implies $a = b$.

[12.0.10] Exercise. The number of solutions to $x^2 \equiv 1 \mod n$ is the same as the number of elements $\phi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ satisfying $\phi^2 = \mathrm{id}$.

Solution. Let $a \in \mathbb{Z}/n\mathbb{Z}$ be a generator. If $k \in \{1, \ldots, n-1\}$ is a solution to $x^2 \equiv 1 \mod n$, then the map $a \mapsto a^k$ induces an automorphism of $\mathbb{Z}/n\mathbb{Z}$ satisfying the condition. Conversely, suppose an automorphism ϕ satisfies $\phi^2 = \mathrm{id}$. Write $\phi(a) = a^k$, for some $k = 0, 1, \ldots, n-1$. Then $a = \phi^2(a) = (a^k)^k = a^{k^2}$, so $k^2 \equiv 1 \mod n$ and we have a solution to the equation. □