BASIC GROUP THEORY

18.904

1. Definitions

Definition 1.1. A *group* $(G, \cdot)$ is a set G with a binary operation

$$\cdot : G \times G \to G,$$

and a unit $e \in G$, possessing the following properties.

(1) Unital: for $g \in G$, we have $g \cdot e = e \cdot g = g$.
(2) Associative: for $g_i \in G$, we have $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.
(3) Inverses: for $g \in G$, there exists $g^{-1} \in G$ so that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

For a group G, a subgroup H is a subset of G which is closed under the multiplication in G, and is closed under taking inverses. A subgroup is a group embedded in G. We write "$H \leq G$".

The cardinality of a finite group is its *order*. If the underlying set of a group G is infinite, the group is said to have infinite order. Sometimes the order of a group is written $|G|$.

A set of elements S of G is said to *generate* G if every element of G may be expressed as a product of elements of S, and inverses of elements of S. That is to say, given $g \in G$, there exists $s_i \in S$ and $\epsilon_i \in \{\pm 1\}$ so that

$$g = s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}.$$

If a group G is a generated by a single element, it is said to be *cyclic*. Every element of a cyclic group G is of the form g^n for some $n \in \mathbb{Z}$.

An arbitrary subset S of G will generate a subgroup of G. We say that this subgroup $\langle S \rangle$ is the *subgroup generated by* S. It is the smallest subgroup of G containing S. Every element of G generates a cyclic subgroup.

A group is *abelian* if it is commutative: for all $g, h \in G$ we have

$$g \cdot h = h \cdot g.$$

Cyclic groups are necessarily abelian (why)?

For an abelian group A it is sometimes customary to use additive notation instead of multiplicative notation for the binary operation. The following chart explains the difference.

Date: September 28, 2005.

Multiplicative	Additive
$\cdot : A \times A \to A$	$+ : A \times A \to A$
$g \cdot h$	$g + h$
$e = 1$	$e = 0$
g^{-1}	$-g$
$g \cdot g^{-1} = 1$	$g - g = 0$
$g^n := \underbrace{g \cdot g \cdot \cdots \cdot g}_{n}$	$ng := \underbrace{g + g + \cdots + g}_{n}$

When using multiplicative notation it is common to omit the multiplication sign:

$$gh := g \cdot h.$$

2. Examples

Many of the examples below are abelian. Abelian groups are the least interesting groups.

Examples:

(1) The trivial group: $\{1\}$. The group contains one element. The operation is given by $1 \cdot 1 = 1$.
(2) The additive integers: $(\mathbb{Z}, +)$. This group is cyclic, generated by 1. It is also generated by -1. Could we choose any other element to generate it?
(3) The additive real numbers: $(\mathbb{R}, +)$. This group contains $\mathbb{Z}$ as a subgroup. How many generators does this group have?
(4) The multiplicative real numbers: $\mathbb{R}^\times := (\mathbb{R}\backslash\{0\}, \cdot)$.
(5) The additive complex numbers: $(\mathbb{C}, +)$. This group contains $\mathbb{R}$ as a subgroup.
(6) The multiplicative complex numbers: $\mathbb{C}^\times := (\mathbb{C}\backslash\{0\}, \cdot)$. This group contains $\mathbb{R}^\times$ as a subgroup.
(7) The group $(\{\pm 1\}, \cdot)$. This group contains two elements, with identity 1, and $(-1) \cdot (-1) = 1$. Note that $(-1)^{-1} = -1$. This is a cyclic subgroup of $\mathbb{R}^\times$ of order 2, generated by -1.
(8) The integers modulo m: $(\mathbb{Z}/m, +)$. The set $\mathbb{Z}/m$ is the set

$$\{[0], [1], [2], \ldots, [m-1]\}$$

of equivalence classes of integers modulo m. This is a cyclic group under addition of order m. The generator is 1.
   (a) Why is addition well defined?
   (b) What are the inverses?
   (c) Suppose that $[k]$ generates $\mathbb{Z}/m$. What is the relationship of k to m?
(9) The symmetric group on n letters: Σ_n. Let $S = \{1, \ldots n\}$ be a set with n elements. The group $\Sigma_n = \mathrm{Aut}(S)$ is the group of bijective set-maps ("automorphisms") of S. An element σ of Σ_n is a permutation

$$\sigma : S \to S.$$

The group multiplication is composition.
   (a) Why does this form a group?
   (b) What is the order of Σ_n?
   (c) Is Σ_n Abelian? Check out $n = 2, 3$ explicitly.

(10) The general linear group: $GL_n(\mathbb{R})$. This is the group of $n \times n$ matrices with real entries and non-zero determinant. The group operation is matrix multiplication. Why do we require the determinant to be non-zero?

(11) The circle: S^1. This is a group under multiplication when viewed as a subset of the complex plane.
$$\begin{aligned} S^1 &= \{z \in \mathbb{C}^\times \;:\; |z| = 1\} \\ &= \{e^{ix} \;:\; x \in \mathbb{R}\} \end{aligned}$$
Naturally, S^1 is a subgroup of $\mathbb{C}^\times$.

(12) The cyclic group of order m: C_m. This is the abstract group with one generator g and elements
$$C_m = \{1, g, g^2, g^3, \ldots, g^{m-1}\}.$$
We impose the *relation* $g^m = 1$, so that $g^k = g^{k+m}$ for any k in $\mathbb{Z}$. This group can be viewed non-abstractly as a subgroup of S^1 generated by $g = e^{2\pi i/m}$.
$$\{e^{2\pi ik/m} \in S^1 \;:\; k \in \mathbb{Z}\}.$$

(13) The infinite cyclic group: C_∞. This is the abstract group with one generator g and distinct elements
$$C_\infty = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, g^3, \ldots\}.$$
This group can be viewed non-abstractly as a subgroup of S^1 generated by $g = e^{2\pi i\xi}$
$$\{e^{2\pi ik\xi} \in S^1 \;:\; k \in \mathbb{Z}\}$$
where ξ is any *irrational* real number (why do we make this restriction?).

3. Homomorphisms

Definition 3.1. Let G, H be groups. A map $f : G \to H$ is a *homomorphism* if it preserves the product:
$$f(g_1g_2) = f(g_1) \cdot f(g_2).$$

Facts about homomorphisms $f : G \to H$ (verify these).

(1) $f(x^{-1}) = f(x)^{-1}$.
(2) $f(e) = e$.
(3) The image $\operatorname{im} f \subset H$ is a subgroup.

The *kernel* of the homomorphism f is the subgroup
$$\ker f = \{g \;:\; f(g) = e\} \leq G.$$
(Verify that this is a subgroup.)

If f is injective, then it is said to be a *monomorphism.* If f is surjective, then it is said to be an *epimorphism.* If f is bijective, then the set-theoretic inverse f^{-1} is necessarily a homomorphism, and we say that f is an *isomorphism.* We then write $G \cong H$.

(Verify that f is a monomorphism if and only if $\ker f = e$.)

Homomorphisms from G to G are called *endomorphisms.* Endomorphisms which are isomorphisms are called *automorphisms.*

Examples of homomorphisms.

(1) $\log : (\mathbb{R}^{\geq 0}, \cdot) \to (\mathbb{R}, +)$. Since this map is a bijection, it has an inverse. It is the homomorphism $\exp : (\mathbb{R}, +) \to (\mathbb{R}^{\geq 0}, \cdot)$.

(2) det : $GL_n(\mathbb{R}) \to \mathbb{R}^\times$. The kernel is the subgroup of matrices with determinant 1. This subgroup is called the *special linear group* and denoted $SL_n(\mathbb{R})$.
(3) Let n be any integer. The map $\lambda_n : \mathbb{Z} \to \mathbb{Z}$ given by $\lambda_n(m) = nm$ is a monomorphism if $n \neq 0$.
(4) The map $f : \mathbb{Z} \to C_\infty$ given by $f(n) = g^n$ is an isomorphism.
(5) Similarly, there is an isomorphism $\mathbb{Z}/n \cong C_n$.
(6) There is a monomorphism $\iota : \mathbb{Z}/n \to \mathbb{Z}/(nm)$ given by $\iota([k]) = [mk]$. (What is wrong with just defining $\iota([k]) = [k]$?).
(7) There is an epimorphism $\nu : \mathbb{Z}/(nm) \to \mathbb{Z}/n$ given by $\nu([k]) = [k]$.
(8) If H is a subgroup of G, the inclusion $\iota : H \hookrightarrow G$ is a monomorphism.
(9) Given an element $g \in G$, we can form an associated automorphism of G via the assignment $h \mapsto ghg^{-1}$ (verify this is an automorphism). This mapping is sometimes referred to as *conjugation by g*.

4. Cosets

A subgroup H naturally partitions a group into equal pieces. These partitions are called *cosets*.

Definition 4.1. Let H be a subgroup of a group G, and let $g \in G$. The (right) *coset* gH is the subset of G given by

$$gH = \{gh \, : \, h \in H\}.$$

You can similarly talk about left cosets Hg, and the discussion that follows is equally valid for left cosets. Left cosets and right cosets generally differ unless G is abelian.

Facts about cosets (which you should verify):

(1) A coset gH is *not* a subgroup unless $g \in H$.
(2) The set-map $H \to gH$ given by $h \mapsto gh$ is a bijection. Therefore, the H cosets all have the same cardinality as H.
(3) $g_1H = g_2H$ if and only if $g_1 = g_2h$ for some $h \in H$. Otherwise g_1H and g_2H are distinct.
(4) Define an equivalence relation $\sim$ on G by declaring that $g_1 \sim g_2$ if and only if there exists an $h \in H$ so that $g_1h = g_2$. Then the equivalence classes of this equivalence relation are in one to one correspondence with the cosets of G.

Let G/H denote the set of cosets. We see that for a collection of representatives g_λ of the equivalence classes of (4) above, the group G breaks up into the *disjoint* union

$$G = \bigcup_\lambda g_\lambda H.$$

The following proposition is immediate.

Proposition 4.2. Suppose G is finite. Then we have

$$|G| = |H| \cdot |G/H|.$$

Consequently, the order of any subgroup of G must divide the order of G.

For abelian groups G for which we are using additive notation, it is typical to write H cosets as $g + H$ instead of gH. For instance, for the subgroup

$$m\mathbb{Z} = \{mk \,:\, k \in \mathbb{Z}\} \leq \mathbb{Z}$$

($m \neq 0$) we write the cosets as $n + m\mathbb{Z}$. Look familiar? The elements of the group $\mathbb{Z}/m$ of integers modulo m correspond to the cosets $\mathbb{Z}/m\mathbb{Z}$.

5. Normal subgroups

We would like to make G/H a group. How would we do this? The most natural multiplication on cosets would be

$$(g_1H) \cdot (g_2H) = (g_1g_2)H. \tag{5.1}$$

However there is a problem in that this is not well defined in general (convince yourself that this is so). If G is abelian, then this multiplication is well defined, and G/H is a group. We have already seen an example of this: the cosets $\mathbb{Z}/m\mathbb{Z}$ form a group.

If G is non-abelian, there is a criterion on H that suffices to make G/H a group.

Definition 5.2. A subgroup N of G is said to be *normal* if any of the following equivalent conditions hold (verify that these are equivalent).

(1) For all $g \in G$, we have $gN = Ng$ (left cosets are the same as right cosets).
(2) For all $g \in G$ and $h \in N$, we have $ghg^{-1} \in N$ (N is invariant under conjugation).
(3) The multiplication formula of Equation (5.1) is well defined and gives G/N the structure of a group.

If N is a normal subgroup of G, one sometimes writes $N \trianglelefteq G$. The resulting group of cosets G/N is called the *quotient group*. There is a natural quotient homomorphism

$$q : G \to G/N$$
$$g \mapsto gN$$

which is surjective. The kernel of q is N (why?).

It turns out that every epimorphism is essentially given as a quotient homomorphism. Prove the following theorem.

Theorem 5.3 (First Isomorphism Theorem)**.** Let $f : G \to H$ be a homomorphism. Then the subgroup $\ker f$ is normal, and there is a natural isomorphism $G/\ker f \cong \operatorname{im} f$ making the following diagram commute.