Algebra Review

1 Finite Groups

The study of algebra is motivated by a desire to abstract away from the familiar notions of arithmetic, numbers, and algebra to develop a theory that is general and applies to different structures which share similar properties. For example, we will study structures called **groups** and prove general results about them that may be applied to the structures we are already familiar with, such as the integers $\{0, 1, \ldots, p-1\}$ under modular arithmetic for p a prime. Texts in Algebra: Abstract Algebra by Herstein, A First Course in Abstract Algebra by Fraleigh,

Definition 1 (Group)**.** *A group $\langle G, *\rangle$ is a set G, closed under a binary operation $*$, such that:*

1. *(associativity) for all $a, b, c \in G$, we have*

$$(a * b) * c = a * (b * c);$$

2. *(identity) there is an element $e \in G$ such that for all $x \in G$,*

$$e * x = x * e = x;$$

3. *(inverse) for every $a \in G$, there is a element $a' \in G$ such that*

$$a * a' = a' * a = e.$$

A group is ***abelian*** *or* ***commutative*** *if for every $a, b \in G$, $a * b = b * a$.*

Example 2 (non-finite)**.** $\mathbb{N}^+$ *(without zero) is not a group under addition–there is no identity element. $\mathbb{N}$ including zero is still not a group under addition, since 3 has no additive inverse. Is $\mathbb{N}$ a group under multiplication? The sets $\mathbb{Q}^+$ and $\mathbb{R}^+$, as well as $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$. are commutative groups under multiplication. The set $M_{m\times n}(\mathbb{R})$ of all $m \times n$ matrices under matrix addition is a commutative group. The set $M_n(\mathbb{R})$ of all $n \times n$ matrices under matrix multiplication is not a group. The $n \times n$ matrix with all entries 0 has no inverse. The set $GL(n, \mathbb{R})$ of all $n \times n$ invertible matrices with matrix multiplication is a non-commutative group!*

Example 3. *The set $GL(2, 3)$ of all 2×2 invertible matrices over a field of 3 elements is a finite, non-commutative group. Example of non-commutativity.*

Example 4. *For a prime p, $\mathbb{Z}_p$ is a group under addition, and $\mathbb{Z}_p^*$ is a group under multiplication.*

Verify that for $p = 7$, both $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$ are groups, and verify for general p a prime.

For $\mathbb{Z}_p^*$ associativity holds, and the identity is 1. Take any $x \in \mathbb{Z}_p^*$. To compute the inverse, note that $gcd(p, x) = 1$, and hence there exist integers x' and b such that

$$x * x' + pb = 1.$$

Then $x * x' - 1 = -pb$, i.e. $p | x * x' - 1$ which implies $x * x' \equiv 1 \pmod{p}$.

There are certain properties that it will be helpful to remember about groups. Let G be a group with binary operation $*$, and $a, b, c \in G$. Then:

1. the left and right cancellation laws hold in G: $a * b = a * c$ implies $b = c$ and $b * a = c * a$ implies $b = c$;
2. $a * x = b$ and $y * a = b$ have unique solutions in G;
3. any group only has one identity;
4. $(ab)^{-1} = b^{-1}a^{-1}$.

2 Subgroups, Cyclic Groups and Generators

We will sometimes abuse notation and refer to a group $\langle G, *\rangle$ as G when the operation is implied or understood. We will also omit the operator between elements of the group, i.e. ab will be used to denote $a * b$. The inverse of a group element a will often be referred to as a^{-1}. The exponent over a group element denotes repeated group operation, so that $a^3 = aaa$. Using this notation, we may add exponents for group operations, i.e. $a^2 * a^3 = a^5$ and $a^2 * a^{-3} = a^{-1}$ and so on.

Definition 5. *A subset H of a group G is a **subgroup** of G, denoted $H \preceq G$, if H is closed under the binary operation of G and H with the induced operation from G is itself a group.*

Thus $\mathbb{Q}^+$ is a subgroup of $\mathbb{R}^+$ under multiplication, and $\mathbb{Z}$ is a subgroup of $\mathbb{R}$ under addition, but $\langle \mathbb{Q}^+, \cdot\rangle$ is not a subgroup of $\langle \mathbb{R}, +\rangle$.

Definition 6. *The **order** of a finite group G, denoted $|G|$, is the size of the set G.*

Consider an element a of G. What if we would like to build a subgroup of G containing a? For closure, we must include aa, aaa, etc. We also need the identity, and an inverse a^{-1} for a. Then we also need $a^{-1}a^{-1}a^{-1}$ and so on.

Definition 7. *The set $H = \{a^n : n \in \mathbb{Z}\}$ with the induced operation of G is the smallest subgroup of G containing a. We say that H is the **cyclic** subgroup of G generated by a, and is denoted $\langle a\rangle$. We say that an element a of a group G generates G if $\langle a\rangle = G$. A group is cyclic if $G = \langle a\rangle$ for some $a \in G$, i.e. some element generates it.*

Example 8. *The groups $\mathbb{Z}$ and $\mathbb{Z}_n$ under addition are cyclic.*

Example 9. *The group $\mathbb{Z}_p^*$ (for p a prime) under multiplication is cyclic. A generator of $\mathbb{Z}_p^*$ is also called a primitive element mod p. Show this for $p = 7$.*

Fact 10. *Any cyclic group of order n is isomorphic to $\mathbb{Z}_n$.*

Definition 11. *If the the cyclic subgroup $\langle a\rangle$ is finite, then the **order** of a is the order $|\langle a\rangle|$ of this cyclic subgroup. Otherwise, a is of infinite order.*

If G is finite, cyclic, and a generates G, then the order of $a \in G$ is the smallest positive integer n such that $a^n = e$. To see this, note that if G is finite and cyclic, then $a^j = a^k$ for some $j, k \in \mathbb{Z}$ with $j > k$. Let n be the smallest positive integer such that $a^n = e$. Then $\langle a\rangle = \{e, a^1, a^2, \ldots, a^{n-1}\}$ has order n. Thus a has order n, the smallest $n > 0$ such that $a^n = e$.

3 The Theorem of Lagrange

We are now going to prove an elegant and powerful theorem that has a very simple proof. We will then look at some of its applications, such as the proof of Fermat's little theorem.

Definition 12. *Let H be a subgroup of a group G. The subset $aH = \{ah | h \in H\}$ of G is the* ***left coset*** *of H containing a, while the subset $Ha = \{ha | h \in H\}$ is the* ***right coset*** *of H containing a.*

Theorem 13 (Theorem of Lagrange)**.** *Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.*

Proof. We prove this in two steps. First, we show that G can be partitioned into left cosets of H. Then we show that every left coset of H has size $|H|$. The theorem clearly follows.

To prove the first part, we show that every element $g \in G$ can be placed in exactly one coset. Since $H \preceq G$, it must contain the identity of G, so we know that g is in the coset gH. Thus it suffices to show that if g is in a coset aH then $gH = aH$. First observe that for any coset aH, $g \in aH \iff a^{-1}g \in H$. Assuming $g \in aH$, we have that $a^{-1}g \in H$. We need to show that for any $x \in G$,

$$x \in aH \iff x \in gH,$$

in other words,

$$a^{-1}x \in H \iff g^{-1}x \in H.$$

We show the first direction; the opposite direction is similar. Using the fact that H is a group we have $a^{-1}x \in H$ implies $x^{-1}a \in H$, since every element of H has an inverse. Since H is closed and $a^{-1}g \in H$, we then have $x^{-1}aa^{-1}g = x^{-1}g$ is in H as well. Finally the inverse of this is in H, so $g^{-1}x \in H$.

Now it remains to show that every coset of H contains $|H|$ elements. To see this, for any coset aH, consider the map $\phi : H \to aH$ defined as $\phi(h) = ah$. By definition the mapping is onto. Now if $\phi(h_1) = \phi(h_2)$ then $ah_1 = ah_2$ and $h_1 = h_2$, so the mapping is one-to-one as well. ■

Now we can easily prove Fermat's little theorem:

Theorem 14. *If p is a prime, for any integer a relatively prime to p:*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. Consider $\mathbb{Z}_p^*$ which has order $p-1$. By Lagrange's theorem, the order of the cyclic group generated by a must divide $p-1$, i.e. if a has order m then there exists an integer k such that $mk = p-1$. Then $a^{mk} = (a^m)^k = 1^k \pmod{p}$. ■

Another easy consequence of Lagrange's theorem is that every group of prime order is cyclic, and furthermore that every element (except the identity) of such a group is a generator. To see this, take any $a \neq e \in G$. Again, the order of a must divide p. Since $a \neq e$ $\langle a \rangle$ contains at least two elements, so the order of a must be p.

Example 15 (groups of prime order)**.** *Sophie Germain primes are primes p such that $2p+1$ is also prime. For example $p = 5$ is a Germain prime since $2p+1 = 11$ is also a prime. The largest known Germain prime is $48047305725 \cdot 2^{172403} - 1$, though it is conjectured that there are infinitely many such primes. Anyways, recall that the set of quadratic residues in $\mathbb{Z}_{2p+1}$, $H = \{a^2 : a \in \mathbb{Z}_{2p+1}\}$, has size $\frac{(2p+1)-1}{2} = p$. One can verify that H forms a subgroup; since H has order p a prime, it is cyclic.*