Abstract Algebra Notes

Contents

1. Groups

1.1. Group Basics

Definition (group): A *group* is a set G with an operation $\times : G \times G \to G$ which satisfies the following properties:

a) There exists an element $e \in G$ such that $a \times e = e \times a = a$ for all $a \in G$ (if the operation is represented multiplicatively, then often we write it as 1_G, or just 1).
b) For every $a \in G$, there exists $a^{-1} \in G$ such that $a \times a^{-1} = a^{-1} \times a = e$.
c) The operation is associative, i.e. for every $a, b, c \in G$, we have $a \times (b \times c) = (a \times b) \times c$.

From here on out, the operation $\times$ will take a number of forms, such as $+$ or $\cdot$, or it won't make an appearance at all and implicit multiplication (such as ab) will represent the operation.

Example *(standard examples/nonexamples)*:
- Consider $(\mathbb{Z}, +)$. The identity is 0, and the inverse of n is $-n$.
- Consider $(\mathbb{Z}^\times, \cdot)$, where $\mathbb{Z}^\times = \mathbb{Z}\backslash\{0\}$. The identity is 1, but not every element has an inverse. For example, $2 \cdot n \neq 1$ for any integer n.
- Consider $(\mathbb{C}^\times, \cdot)$. The identity is 1, and the inverse of z is z^{-1}.
- Consider $(\mathrm{SL}_n(\mathbb{C}), \times)$, where $\mathrm{SL}_n(\mathbb{C})$ is the set of $n \times n$ matrices with elements in $\mathbb{C}$ that have determinant 1. The identity is I_n, and since every element has nonzero determinant, an inverse exists and is given by the inverse matrix.
- Consider $\{1, 2, \ldots, n\}$ and the set of functions T on it that are bijective. Then S_n denotes the group of all of these functions, and is called the *symmetric group*. The identity permuation is just $f(x) = x$, and the inverse of an element is given by the inverse function.
- The integers mod n form a group under addition, and is what's known as *cyclic*, since a single element (say 1) generates the entire group by repeatedely applying the operation to the element. A group with size n where a single element generates it is often called a *cyclic group*, and is denoted C_n.
- The group G with one element 1 is called the *trivial group*.

Definition (abelian): Suppose $(G, \cdot)$ is a group. If for every $a, b \in G$ we have $ab = ba$, then the group is called *abelian*.

Taking $\mathrm{SO}(n)$ as an example, we see that not every group is abelian.

Proposition (identity and inverse are unique): Let $(G, \cdot)$ be a group. Then the identity is unique. Furthermore, every element has a unique inverse.

Proof: Suppose e_1, e_2 are identities. Then $e_2 = e_1 e_2 = e_1$. Now suppose x, y are inverse of a. Then $x = xe = x(ay) = (xa)y = ey = y$. ∎

Definition (left/right inverse): Suppose $(G, \cdot)$ is a group. An element a has a *left inverse* if there exists $\ell \in G$ such that $\ell a = e$. An element a has a *right inverse* if there exists $r \in G$ such that $ar = e$.

Proposition (left and right inverse imply invertible): Suppose $(G, \cdot)$ is a group, and $a \in G$ has left inverse ℓ and right inverse r. Then $\ell = r$ and a is invertible with inverse ℓ.

Proof: We have

$$\ell = \ell(ar) = (\ell a)r = r.$$

Then we have

$$\ell a = e = ar = a\ell.$$

■

Proposition (cancellation law): Suppose $(G, \cdot)$ is a group. If $a, b, c \in G$ such that $ab = ac$ or $ba = ca$.

Proof: Multiply the first equation by a^{-1} on the left, and second equation by a^{-1} on the right.■

Definition (product group): Let $(G, \star)$ and $(H, *)$ be groups. Then the *product group* $(G \times H, \cdot)$ has operation $\cdot$ defined by

$$(g_1, h_1) \cdot (g_1, h_2) = (g_1 \star g_2, h_1 * h_2) \in G \times H.$$

Definition (subgroup): Suppose $(G, \star)$ is a group. Then a subset H of G is a *subgroup of* G, denote $H \leq G$, if when inheriting the operation $\star$, H is a group. If $H \neq G$, then H is a *proper subgroup of* G, denoted $H < G$.

Example *(subgroup generated by element)*: Let x be an element of a group G. Then the subset

$$\langle x \rangle = \{\ldots, x^{-2}, x^{-1}, 1, x^1, x^2, \ldots\}$$

is a subgroup of G. More generally, given a subset S of a group G, we let $\langle S \rangle$ denote the subgroup given by creating any string of the elements of S and their inverses.

Proposition: If $H \leq G$, then H has the same identity as G, and the inverse of an element in H is the same as the elements' inverse in G.

Proof: Let 1_G denote the identity in G, and let 1_H denote the identity in H. Since $H \subseteq G$, we have $h1_G = 1_G h = h$ for all $h \in H$. Thus 1_G is an identity of H. Since the identity of a group is unique, this implies $1_G = 1_H$.

Now suppose $h \in H$ has inverse $h_H^{-1} \in H$ and inverse $h_G^{-1} \in G$. Since $h, h_H^{-1} \in G$, this implies that h_H^{-1} is an inverse of h in G. Since inverses are unique, this implies $h_G^{-1} = h_H^{-1}$. ■

Proposition: The intersection of two subgroups $H_1, H_2 \leq G$ is another subgroup of G.

Proof: Clearly $1 \in H_1 \cap H_2$. If $a, b \in H_1 \cap H_2$, then $a, b \in H_1$ and $a, b \in H_2$, so $ab \in H_1 \cap H_2$ by closure. Similar logic shows that $H_1 \cap H_2$ contains inverses. ■

Definition (order of group and element): The *order* of a group G is the number of elements in it. The *order* of an element $x \in G$ is the smallest $n \in \mathbb{N}$ such that $x^n = 1$, and is denoted ord x. If no such n exists, then the order is ∞.

Proposition: Suppose G is a group. If $g^n = 1$, then ord g divides n.

Proof: Suppose otherwise. Thus $n = a \cdot \text{ord } g + b$, where $b < \text{ord } g$ and $a, b \in \mathbb{Z}_{\geq 0}$. Then we have

$$g^n = g^{a \cdot \text{ ord } g} g^b = g^b.$$

Since ord g is the minimal number such that $g^k = 1$, $g^b \neq 1$, so we have a contradiction. ■

Proposition: Suppose G is a finite group. Then ord g is finite for all $g \in G$.

Proof: If not, then the sequence $g, g^2, g^3, \ldots$ would contain pairwise distinct elements, and thus G would not be finite, contradiction. ■

1.2. Isomoprhisms and Homomorphisms

Definition (isomorphism): Let $(G, \times)$ and $(H, \star)$ be groups. A bijection $\varphi : G \to H$ is called an *isomorphism* if

$$\varphi(g_1 \times g_2) = \varphi(g_1) \star \varphi(g_2)$$

for all $g_1, g_2 \in G$. If there exists an isomorphism between G and H, then we say they are *isomorphic*, and denote it $G \cong H$.

Example *(isomorphisms)*:

- The identity map from G to itself is trivially an isomorphism.

- Define the map $\varphi : S_2 \to \mathbb{Z}/2\mathbb{Z}$ by $\varphi(\{1,2\}) = 0$ and $\varphi(\{2,1\}) = 1$. Then it's easy to check that φ is an isomorphism, so $\mathbb{Z}/2\mathbb{Z} \cong S_2$.

Definition (automorphism): If $\varphi : G \to G$ is an isomorphism, then φ is an *automorphism.*

Definition (homomorphism): Let $(G, \times)$ and $(H, \star)$ be groups. A function $\varphi : G \to G$ is called a *homomorphism* if

$$\varphi(g_1 \times g_2) = \varphi(g_1) \star \varphi(g_2)$$

for all $g_1, g_2 \in G$.

Definition (endomorphism): If $\varphi : G \to G$ is a homomorphism, then φ is an *endomorphism.*

Example *(homomorphism)*:
- Every isomorphism is a homomorphism.
- Consider $\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ given by $\varphi(n) = n \pmod 3$. Then it's easy to see this is a homomorphism.

Proposition: Let φ be a homomorphism between G and H. Then $\varphi(1_G) = 1_H$ and $\varphi(a)^{-1} = \varphi(a^{-1})$ for all $a \in G$.

Proof: We have

$$\varphi(1_G) = \varphi(1_G \times 1_G) = \varphi(1_G) \star \varphi(1_G) \Rightarrow 1_H = \varphi(1_G).$$

We also have

$$1_H = \varphi(1_G) = \varphi(a \times a^{-1}) = \varphi(a)\varphi(a^{-1})$$

and

$$1_H = \varphi(1_G) = \varphi(a^{-1} \times a) = \varphi(a^{-1})\varphi(a).$$

■

Proposition: Suppose G, H are groups. Then $G \cong H$ if and only if there exist homomorphisms $\varphi : G \to H$ and $\psi : H \to G$ such that $\varphi \circ \psi = \mathrm{id}_H$ and $\psi \circ \varphi = \mathrm{id}_G$. Now suppose the second statement holds. Then as functions, we see that φ, ψ are bijections, and their inverses are each other. Thus φ is a bijective homomorphism between G and H, and thus an isomorphism.

Proof: Suppose $G \cong H$. Thus there exists a bijection $\xi : G \to H$ that is a homomorphism. Then we can just take $\varphi = \xi$ and $\psi = \xi^{-1}$. ■

Definition (kernel): The *kernel* of a homomorphism $\varphi : G \to H$ is the set of elements in G that map to 1_H under φ. In other words, $\ker \varphi = \varphi^{-1}(\{1_H\})$. When $\ker \varphi = \{1_G\}$, we often call the kernel trivial.

Example *(kernels)*:
- For an isomorphism, the kernel will be $\{1_G\}$, as it's a bijection.
- The kernel of $\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ where $\varphi(n) = n \pmod 3$ is $3\mathbb{Z}$.

Proposition: The kernel of a homomorphism $\varphi : G \to H$ is a subgroup of G, the image of a homomorphism is a subgroup of H, and $\varphi^{-1}(N)$ is a subgroup of G for $N \leq H$. Furthermore, a homomorphism is injective if and only if $\ker \varphi = \{1_H\}$.

Proof: Suppose $a, b \in \ker \varphi$. Then $\varphi(ab) = \varphi(a)\varphi(b) = 1_H$, so $ab \in \ker \varphi$. We already know that $1_G \in \ker \varphi$, and so is an identity for it. For any $a \in \ker \varphi$, we also have $1_H = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) = \varphi(a^{-1})$, and thus $a^{-1} \in \ker \varphi$. Thus $\ker \varphi \leq G$.

Suppose $h_1, h_2 \in \varphi(G)$. Thus there exists $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1, \varphi(g_2) = h_2$. We then have $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = h_1 h_2$. Thus $h_1 h_2 \in \varphi(G)$. Note that $1_H \in \varphi(G)$ and so it has an identity. If $h \in \varphi(G)$ with $\varphi(g) = h$, then $1_H = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) = h\varphi(g^{-1})$. Similarly, we find $1_H = \varphi(g^{-1})h$. Thus $h^{-1} \in \varphi(G)$.

Since $1_H \in N$, we have $1_G \in \varphi^{-1}(N)$. If $g \in \varphi^{-1}(N)$, then $\varphi(g) \in N$. Then $\varphi(g)^{-1} \in N$. Since φ is a homomorphism, $\varphi(g)^{-1} = \varphi(g^{-1})$. Thus $g^{-1} \in \varphi^{-1}(N)$, so it contains inverses. If $a, b \in \varphi^{-1}(N)$, then $\varphi(ab) = \varphi(a)\varphi(b) \in N$, which implies $ab \in \varphi^{-1}(N)$, and so is closed. Thus $\varphi^{-1}(N)$ is a subgroup of G.

Now suppose φ is injective. We already know that $\varphi(1_G) = 1_H$, so by injectivity no other element of G can map to 1_H. Thus $\ker \varphi = \{1_G\}$. Now suppose the kernel is trivial, and suppose $\varphi(a) = \varphi(b)$. Then $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = 1_H$. Thus $ab^{-1} \in \ker \varphi$, which implies $ab^{-1} = 1_G \Rightarrow a = b$. Thus φ is injective. ■

1.3. Quotient Groups

Definition (left/right coset, index): Let H be a subgroup of H. Then for any $g \in G$ the set

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

is called a *left coset of* H. Similarly, the set

$$Hg = \{hg : h \in H\}$$

is called a *right coset of* H. The *index* of H in G, denoted $[G : H]$, is the number of left cosets of H in G.

Almost all statements we prove for left cosets will hold for right cosets, and vice versa. Note that $x \mapsto g_2 g_1^{-1} x$ is a bijection from $g_1 H$ and $g_2 H$, so the cosets of H have the same cardinality, in particular, $|H|$.

Proposition: Suppose $H \leq G$ and $g_1, g_2 \in G$. Then $g_1H = g_2H$ if and only if $g_1^{-1}g_2 \in H$.

Equivalently, the second condition can be $g_2^{-1}g_1$. The inverse element just has to be on the left.

Proof: Suppose $g_1H = g_2H$. Then $g_2 = g_2e = g_1h$ for some $h \in H$. Thus $g_1^{-1}g_2 = h \in H$. Now suppose $g_1^{-1}g_2 \in H$. Thus it's inverse $g_2^{-1}g_1 \in H$. Given $g_1h \in g_1H$, we have $g_1H = g_2(g_2^{-1}g_1)h \in g_2H$, so $g_1H \subseteq g_2H$. Given $g_2h \in g_2H$, we have $g_1(g_1^{-1}g_2)h \in g_1H$, so $g_2H \subseteq g_1H$. ■

Note this implies that cosets are disjoint or equal, since if they has nonempty intersection, then $g_1h_1 = g_2h_2 \Rightarrow g_2^{-1}g_1 = h_2h_1^{-1} \in H$ for some $h_1, h_2 \in H$, and by the above the two cosets are equal.

Theorem (Lagrange's theorem): Let G be a finite group and H a subgroup. Then $|H|$ divides $|G|$.

Proof: From the above, we know that distinct cosets are disjoint. Thus the distinct cosets of H partition G. Let k be the number of distinct cosets. Since cosets have the same size, this implies $k|H| = |G|$. ■

Corollary: If $x \in G$, where G is a finite group, then $x^{|G|} = 1$.

Proof: Let $H = \langle x \rangle \leq G$. By finiteness, ord $x = |H|$. Since $|H|$ divides $|G|$ by Lagrange's theorem, we have $x^{|G|} = \left(x^{|H|}\right)^{|G|/|H|} = 1$, as desired. ■

Proposition (only prime order group is cyclic): Let p be a prime. Every order p group is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof: Suppose $|G| = p$. Note that every element can either have order 1 or p by the above corollary. If an element has order 1, then by definition it's the identity. Thus every other element in G has order p. Thus we can pick $g \in G$ (namely any element other than the identity) such that $\{g^0, g, g^2, g^3, ..., g^{p-1}\} = G$. Now define $\varphi : G \to \mathbb{Z}/p\mathbb{Z}$ by $\varphi(g^k) = k \pmod p$. Thus φ is a bijection, and

$$\varphi(g^a g^b) = \varphi(g^{a+b}) = a + b \pmod p = \varphi(g^a) + \varphi(g^b) \pmod p.$$

Thus φ is an isomorphism, so G and $\mathbb{Z}/\ p\mathbb{Z}$ are isomorphic. ■

To motivate quotient groups, suppose $\varphi : G \to Q$ is a surjective homomorphism, and suppose $h \in \ker \varphi$. Then note for any $g \in G$, we have $\varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)$. Thus φ basically ignores elements of $\ker \varphi$. Roughly speaking, this means Q is isomorphic to G when we "mod out" by $\ker \varphi$.

As an example, take $\varphi : \mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ where $\varphi(n) = n \pmod{10}$. Then when we "mod out" but multiples of 10 in $\mathbb{Z}$, we get all the elements of $\mathbb{Z}/10\mathbb{Z}$, i.e. $\{..., -20, -10, 0, 10, 20, ...\} \to 0, \{..., -19, -9, 1, 11, 21, ...\} \to 1$, etc. Thus we can think of Q as the quotient of G and $\ker \varphi$, with the elements of it being cosets of $\ker \varphi$. We now make all of this precise.

Definition (normal): A subgroup N of G is called *normal* if it is the kernel of some homomorphism. We write $N \trianglelefteq G$.

Definition (quotient group): Let $N \trianglelefteq G$. Then the *quotient group*, denote G/N, is group with elements being left cosets of N. The operation is given by taking an elements $C_1, C_2 \in G/N$, picking $g_1 \in C_1, g_2 \in C_2$, and letting C_1C_2 being the coset containing g_1g_2.

Note that the operation is equivalent to declaring $(g_1N) \cdot (g_2N) = (g_1g_2)N$, which is often how we'll treat the operation.

We need to check that this operation is well-defined, and that it actually forms a group. First suppose $a \in g_1N$ and $b \in g_2N$. Thus $a = g_1h_1, b = g_2h_2$ for some $h_1, h_2 \in N$. We need to show that $abN = g_1g_2N$, which is equivalent to showing $g_2^{-1}g_1^{-1}ab \in N$. Since N is normal, there exists some homomorphism φ into some group such that $\ker \varphi = N$. Then we have

$$\varphi(g_2^{-1}g_1^{-1}ab) = \varphi(g_2^{-1})\varphi(g_1^{-1})\varphi(g_1)\varphi(h_1)\varphi(g_2)\varphi(h_2) = \varphi(g_2^{-1})\varphi(g_1^{-1})\varphi(g_1)\varphi(g_2) = 1.$$

Thus $g_2^{-1}g_1^{-2}ab \in N$, so this operation is well-defined. It's easy to see that 1_GN is the identity, and that $g^{-1}N$ is the inverse of gN. Thus G/N is indeed a group.

Now we'd like a way to identify normal subgroups without having to to reference a homorphism. It turns out this is the condition we'd like:

Proposition (normality condition): Let $H \leq G$. Then $H \trianglelefteq G$ if and only if for all $g \in G$ and $h \in G$, $ghg^{-1} \in H$. We often write the second part as $gHg^{-1} = H$ for all $g \in G$.

Proof: First suppose $H \trianglelefteq G$. Thus there exists some group K and homomorphism $\varphi : G \to K$ such that $\ker \varphi = H$. Then for any $g \in G, h \in H$, we have $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = 1_K$, so $ghg^{-1} \in H$.

Now suppose $gHg^{-1} = H$ for all $g \in G$. Let $[G/H]$ contain all cosets of H, and define the operation as $(g_1H)(g_2H) = (g_1g_2)H$. To show this is well defined, suppose $a = g_1h_1$ and $b = g_2h_2$ for some $h_1, h_2 \in H$. We need to show that $(ab)H = (g_1g_2)H$, which means we just need to show that $g_2^{-1}g_1^{-1}ab \in H$. To do this, note that

$$g_2^{-1}g_1^{-1}ab = g_2^{-1}g_1^{-1}g_1h_1g_2h_2 = g_2^{-1}h_1g_2h_2.$$

Then by the condition, there exists $h_3 \in H$ such that $g_2^{-1}h_2g_2 = h_3$. Thus

$$g_2^{-1}g_1^{-1}ab = h_3h_2 \in H$$

Thus the cosets are the same, and the multiplication is well-defined. The identity is 1_GH, and the inverse of gH is $g^{-1}H$.

Now let $\varphi : G \to [G/H]$ be defined by $\varphi(g) = gH$. We have $\varphi(g_1g_2) = (g_1g_2)H = (g_1H)(g_2H) = \varphi(g_1)\varphi(g_2)$, so φ is a homorphism. If $h \in H$, then $\varphi(h) = hH = H$, so $H \subseteq$

$\ker\varphi$. If $g \in \ker\varphi$, then $gH = H$, which implies that $g \in H$. Thus $\ker\varphi \subseteq H$. Since we've constructed a homomorphism with kernel H, it is indeed a normal subgroup. ■

Finally, we have another formal way of saying that G/N "acts" like the group a surjective homomorphism with kernel N sends G to.

Theorem (first isomorphism theorem): Let $\varphi : G \to H$ be a homomorphism. Then $G/\ker\varphi \cong \varphi(G)$.

Proof: Let $N = \ker\varphi$. Define $\psi : G/N \to \varphi(G)$ by $\psi(gN) = \varphi(g)$. Note this is well defined since if a, b represent the same coset, then they must have the same φ value (as $a^{-1}b \in H \Rightarrow \varphi(a^{-1}b) = 1_H$). We have $\psi((g_1g_2)N) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1N)\psi(g_2N)$. Thus ψ is a homomorphism. Note if that $\psi(gN) = \varphi(g) = 1_H$, then $g \in N$. Thus $\ker\psi = \{1_GN\}$, so ψ is injective. Surjectivity is easy, since $\varphi(g) = \varphi(gN)$ for all $g \in G$. ■

Theorem (correspondence theorem): Let $\varphi : G \to G'$ be a surjective homomorphism. There exists a natural bijection between

$$\{\text{subgroups of } G \text{ containing } \ker\varphi\} \longleftrightarrow \{\text{subgroups of } G'\}.$$

Given a subgroup $H \leq G$ with contains $\ker\varphi$, it maps to $\varphi(H) \leq G'$.

Proof: Given a subgroup $H \leq G$ containing $\ker\varphi$, we show that $\varphi^{-1}(\varphi(H)) = H$, and given $H' \leq G'$, we show that $\varphi(\varphi^{-1}(H')) = H'$.

First suppose $H' \leq G'$. From basic set theory, we have $\varphi(\varphi^{-1}(H')) \subseteq H'$. Now suppose $h' \in H'$. Thus there exists $g \in G$ such that $\varphi(g) = h'$. Thus $g \in \varphi^{-1}(H')$, which implies $h' \in \varphi(\varphi^{-1}(H'))$, so we have the other inclusion.

Now suppose $H \leq G$ contaning $\ker\varphi$. Again from basic set theory, $\varphi^{-1}(\varphi(H)) \supseteq H$. Now suppose $g \in \varphi^{-1}(\varphi(H))$. Thus there exists $f \in H$ such that $\varphi(g) = \varphi(f) \Rightarrow \varphi(gf^{-1}) = 1$. Thus $gf^{-1} \in \ker\varphi \leq H$. Since $f \in H$, this implies $g \in H$, so $\varphi^{-1}(\varphi(H)) \subseteq H$. ■

1.4. Group Actions

Definition (group action): Let X be a set and G be a group. A *group action* is a binary operation $\cdot : G \times X \to X$, which lets g send x to $g \cdot x$. This operation satisfies the following:
- $(g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $g_1, g_2 \in G, x \in X$.
- $1_G \cdot x = x$ for all $x \in X$.

Example: Consider $G = D_8$, and let it act on the set of colorings of the vertices of a square. If a square x has tl and br red and tr and bl blue, then $r^2 \cdot x = x$.

Definition (orbit): Given a group action G on X, we define an *orbit* to be an equivalence class on X, where $x \sim y$ if there exists $g \in G$ such that $y = g \cdot x$.

It's easy to see that the orbits partition G.

Definition (stabilizer): The *stabilizer* of a point $x \in X$, denote $\text{Stab}_G(x)$, is the set of $g \in G$ such that $g \cdot x = x$.

It's easy to see that $\text{Stab}_G(x)$ is a subgroup of G.

Theorem (orbit-stabilizer theorem): Let $\mathcal{O}$ be an orbit, and pick any $x \in \mathcal{O}$. Let $S = \text{Stab}_G(x)$. Then

$$|\mathcal{O}||S| = |G|.$$

Proof: Let C be the set of cosets of S (which by Lagrange's theorem we know has size $|G|/|S|$), and define $f : C \to \mathcal{O}$ given by $f(gS) = g \cdot x$. This is well defined, since if $g_1 S = g_2 S$, we have $g_1^{-1} g_2 \in S$, so $g_1^{-1} g_2 \cdot x = x \Rightarrow g_2 \cdot x = g_1 \cdot x$. Reversing this logic also shows that f is injective. Surjectivity follows since every element of $\mathcal{O}$ takes the form $g \times x$. Thus f is a bijection, implying

$$|\mathcal{O}| = |C| = |G|/|S|,$$

as desired. ■

In particular, this result implies that the stabilizers of elements in an orbit have the same size.

Definition (fixed points): Let G act on X. Then for $g \in G$, let

$$\text{FixPt } g = \{x \in X : g \cdot x = x\}.$$

Lemma (Burnside's lemma): Let G act on X. Let B be the set of orbits in X. Then

$$|B| = \frac{1}{|G|} \sum_{g \in G} |\text{FixPt } g|.$$

Proof: We double count the number of pairs $(g, x) \in G \times X$ such that $g \cdot x = x$. Let N be that number. If we fix g, then the number of x that work is $|\text{FixPt } g|$. Thus

$$N = \sum_{g \in G} |\text{FixPt } g|.$$

If we fix x instead, the number of g that work is $|\text{Stab}_G(x)|$, so

$$\begin{aligned} N = \sum_{g \in G} |\text{FixPt } g| &= \sum_{x \in X} |\text{Stab}_G(x)| \\ &= \sum_{\mathcal{O} \in B} \sum_{x \in \mathcal{O}} |G|/|\mathcal{O}| \\ &= \sum_{\mathcal{O} \in B} |G| \\ &= |G||B|, \end{aligned}$$

where the third equality follows from the orbit-stabilizer theorem. Dividing by $|G|$ yields the desired conclusion. ■

One particular type of group action is important.

Definition (conjugation): Let G act on itself as follows:

$$g : h \mapsto ghg^{-1}.$$

This is called *conjugation*. The *conjugacy classes* of a group G are the orbits of G under the conjugacy action.

Definition (center): The *center* of a group G, denoted $Z(G)$, is the set of elements $x \in G$ such that $xg = gx$ for all $g \in G$.

It's easy to see that $Z(G)$ is normal, and that each element in $Z(G)$ is its own conjugacy class.

We can also define conjugation naturally on subgroups, by letting g act on $H \leq G$ by $H \mapsto gHg^{-1}$. Thus two subgroups $H, K \leq G$ are *conjugate subgroups* if there exists $g \in G$ such that $K = gHg^{-1}$. Note that conjugation is an isomorphism, so conjugate subgroups are isomorphic. Also note that normal subgroups are fixed by all $g \in G$.

Definition (normalizer): For $H \leq G$, the *normalizer* of H is

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

This is just the stabilizer of H under the conjugation action.

1.5. Sylow Theorems

Theorem (Sylow theorems): Let G be a group of order $p^n m$, where $\gcd(p, m) = 1$ and p is prime. A *Sylow p-subgroup* is a subgroup of order p^n. Let n_p be the number of Sylow p-subgroups.
a) $n_p \equiv 1 \pmod{p}$. In particular, $n_p \neq 0$ and a Sylow p-subgroup exists.
b) $n_p \mid m$.
c) Any two Sylow p-subgroups are conjugate subgroups, and thus isomorphic.

Proof: First we show that a Sylow p-subgroup exists. Let X be the set of all size p^n subsets of G, and let G act on X by left multiplication: $g \cdot S = \{gs : s \in S\}$. We claim there exists an orbit $\mathcal{O}$ under this action with size not divisible by p. To show this, note that

$$\begin{aligned}
\nu_p\left(\binom{p^n m}{p^n}\right) &= \nu_p\left(\frac{(p^n m)!}{(p^n)!(p^n(m-1))!}\right) \\
&= \nu_p((p^n m)!) - \nu_p((p^n)!) - \nu_p((p^n(m-1))!) \\
&= \frac{p^n - 1}{p-1}(m - 1 - (m-1)) \\
&= 0.
\end{aligned}$$

Thus $|X| = \binom{p^n m}{p^n} \neq 0 \pmod{p}$. Since the orbits partition X, this implies there exists an orbit not divisible by p, as desired.

Now pick $S \in \mathcal{O}$ and let $H = \mathrm{Stab}_G(S)$. By the orbit-stabilizer theorem, we have $|\mathcal{O}||H| = |G| = p^n m$. Since p^n doesn't divide $|\mathcal{O}|$, it must divide $|H|$. Now consider a second action where we let H act on S by left multiplication (which we can do since $H = \mathrm{Stab}_G(S)$, so $hs \in S$). Now pick $s \in S$, and consider $\mathrm{Stab}_H(s)$. If $h \in \mathrm{Stab}_H(s)$, then $hs = s \Rightarrow h = 1_H$. Thus $\mathrm{Stab}_H(s) = \{1_H\}$. Thus by the orbit-stabilizer theorem, all orbits of this action have size $|H|$. Thus $|H|$ divides $|S| = p^n$. Thus $|H| = p^n$, so we have a Sylow p-subgroup.

Next we show that any two Sylow p-subgroups are conjugate. Let $Q \leq G$ have order a power of p, and let P be a Sylow p-subgroup. Let Q act on the left cosets of P by left multiplication. Since Q has order power of p, by the orbit-stabilizer theorem, every has size divisible by p or is 1. There are m left cosets of P and m is not divisible by p. Since the orbits partition the cosets, there must exist some orbit with size 1. Thus there exists some g for which $qgP = gP$ for all $q \in Q$. Thus $qg \in gP$ for all $q \in Q$, which implies $q \in gPg^{-1}$ in for all $q \in Q$. Thus $Q \subseteq gPg^{-1}$. Then if Q is a Sylow p-subgroup, it has size p^n, and so the sets must be equal. Thus any two Sylow p-subgroups are conjugate.

Now we show that $n_p \equiv 1 \pmod{p}$. Let $\mathcal{S}$ be the set of all Sylow p subgroups, which by definition has size n_p. From the above, $\mathcal{S}$ is nonempty with some element P. Let P act on $\mathcal{S}$ by conjugation. Again since P has order power of p, the orbits have size power of p or 1. Thus the number of fixed points equivalent to n_p modulo p.

Clearly P is a fixed point, but we show that it's the only fixed point. To do so, suppose Q is a fixed point, meaning $xQx^{-1} = Q$ for all $x \in P$. Let $N_G(Q)$ be the normalizer of Q. It obviously contains Q, and since Q is a fixed point of P under it's action, the normalizer also contains P. Since $N_G(Q) \leq G$, it has order that divides $p^n m$. Since it contains P, it must have size at least p^n. Thus P, Q are Sylow p-subgroups of $N_G(Q)$. Then by c) of the theorem, we see that P and

Q are conjugate subgroups of $N_G(Q)$. Thus there exists $g \in N_G(Q)$ for which $gQg^{-1} = P$. But by definition of being in the normalizer, we see that $gQg^{-1} = Q$. Thus $Q = P$, as desired.

Finally, we show that $n_p \mid m$. Since we showed that $p \nmid n_p$, we can just show that n_p divides $|G|$. Let G act on the set of all Sylow p-subgrous by conjugation. By c), we see that there's only one orbit under this action, so the conclusion follows from the orbit-stabilizer theorem. ■

Proposition (some consequences of Sylow theorems):
a) A Sylow p-subgroup is normal if and only if $n_p = 1$.
b) If G has order pq with $p < q$, then it has normal subgroup of order q.
c) If p is prime and divides the order of an abelian group, then there is exactly one Sylow p-subgroup.
d) (Cauchy's theorem) If p divides the order of a group, then there exists an element with order p.

Proof:
a) If H is a Sylow p-subgroup of G and $H \trianglelefteq G$. Then for all $g \in G$, we have $gHg^{-1} = H$. However, any two Sylow p-subgroups are conjugate, so the only Sylow p-subgroup is H. Thus $n_p = 1$. If $n_p = 1$, then since any two Sylow p-subgroups are conjugate, we must have $gHg^{-1} = H$ for all $g \in G$, and thus $H \trianglelefteq G$.
b) From the Sylow theorems, we see that $n_q \mid p$. Since $n_q = kq + 1$ for some integer k, we see that n_q must be 1. Then by a), we have the desired conclusion.
c) Conjugation is the identity map in an abelian group, so again there can only be one Sylow p -subgroup.
d) By the Sylow theorems, there exists a subgroup H of order p^n. Pick some nonidentity element $g \in H$. Then by Lagrange's theorem, the group $\langle g \rangle$ has order p^t with $1 \leq t \leq n$. If $t = 1$, we're done. Otherwise take the element $g^{p^{t-1}}$. It's easy to see this has order p.

■

1.6. Problems

Problem: Let G be a finite group. Show that there exists n such that G is isomorphic to some subgroup of S_n.

Solution: Let $G = \{g_1, g_2, ..., g_n\}$ be the elements, with g_1 being the identity. Given an element $g \in G$, let $\text{ind}(g)$ denote the index of it's place in G by the order in the set set given above. Thus $\text{ind}(g_i) = i$. Now define $\varphi : G \to S_n$ as

$$\varphi(g_i) = \{\text{ind}(g_i g_1), ..., \text{ind}(g_i g_n)\}.$$

Now we verify that φ is a homomorphism. Then we know that $\varphi(G) \leq S_n$, and then by definition G and the image are isomorphic.

We have that

$$\varphi(g_i g_j) = \{\text{ind}(g_i g_j g_1), ..., \text{ind}(g_i g_j g_n)\}.$$

Pick $k \in \{1, ..., n\}$. Then

$$(\varphi(g_i)\varphi(g_j))(k) = \varphi(g_i)(\text{ind}(g_j g_k)) = \text{ind}\Big(g_i g_{\text{ind}(g_j g_k)}\Big) = \text{ind}(g_i g_j g_k) = \varphi(g_i g_j)(k).$$

Thus $\varphi(g_i g_j) = \varphi(g_i)\varphi(g_j)$, as desired.

Remark: This result is known as *Cayley's theorem.*

Problem: Let G be a finite abelian group. Prove that for all $x \in G$, we have $x^{|G|} = 1$ without appealing to Lagrange's theorem.

Solution: Fix $x \in G$, and let $G = \{g_1, g_2, ..., g_n\}$. Then by the cancellation law, $\{xg_1, xg_2, ..., xg_n\} = G$. Thus

$$\prod_{i=1}^{n} xg_i = \prod_{i=1}^{n} g_i \Rightarrow x^n = 1,$$

as desired.

Problem: Find all groups G such that $\varphi : G \to G$ defined by $\varphi(g) = g^2$ is a homomorphism.

Solution: Suppose G is abelian. Then $\varphi(ab) = (ab)^2 = a^2b^2 = \varphi(a)\varphi(b)$. Now suppose φ is a homorphism. Then $\varphi(ab) = abab = a^2b^2 = \varphi(a)\varphi(b) \Rightarrow ba = ab$, and thus φ is abelian.

Problem: Let G and H be finite groups, where $|G| = 1000$ and $|H| = 999$. Show that a homomorphism $G \to H$ must be trivial.

Solution: Suppose $\varphi : G \to H$ is a homomorphism. By the first isomorphism, $G/\ker\varphi \cong \varphi(G)$. Note that $|G/\ker\varphi| = |G|/|\ker\varphi|$, as the number of cosets of $\ker\varphi$ is the number of elements in $G/\ker\varphi$, and from the proof of Lagrange's theorem, we know that a subgroup N produces $|G|/|N|$ cosets. Thus

$$|G|/|\ker\varphi| = |\varphi(G)|.$$

Since $\varphi(G) \leq H$, by Lagrange's theorem, $|\varphi(G)|$ divides $|H|$. Now if $|\ker\varphi| \neq |G|$, then the left side above contains a factor of 2 or 5, while the right side contains contains factors of 3 or 37. Thus we must have $|\ker\varphi| = |G|$, which implies the homomorphism is trivial.

Problem: Show that two elements in the same conjugacy class have the same order.

Solution: Suppose $a, b \in G$ are conjugate. Thus there exists $g \in G$ such taht $gag^{-1} = b$. Then

$$b^n = (gag^{-1})^n = \underbrace{gag^{-1} \cdots gag^{-1}}_{n \text{ times}} = ga^n g^{-1}.$$

Thus if ord $a = n$, then $b^n = ga^n g^{-1} = gg^{-1} = 1$. If ord $b = n$, then $b^n = 1 = ga^n g^{-1} \Rightarrow g = ga^n \Rightarrow a^n = 1$. Thus they have the same order, so we're done.

Problem: Assume G is a finite group of order $n \geq 2$ and p is the smallest prime dividing n. Let H be a subgroup of G with $|G|/|H| = p$. Show that H is normal in G.

Solution: Let H act on the left cosets of H by left multiplication. Pick some left coset gH and let $\mathcal{O}$ be it's orbit. By the orbit-stabilizer theorem, $|\mathcal{O}|$ divides $|H|$, which divides n. However, $|\mathcal{O}| \leq p$, since there are p cosets of H by $|G|/|H| = p$. Since p is the smallest prime dividing $|G|$, this forces either $|\mathcal{O}| = 1, p$.

First suppose $|\mathcal{O}| = p$. Then by the orbit-stabilizer theorem, $|\mathcal{O}||\text{Stab}_H(H)| = |H|$ (as $\mathcal{O}$ contains all cosets). However, since $\text{Stab}_H(H) = H$, it has size at $|H|$, which implies $|\mathcal{O}| = 1$, contradiction.

Thus $\mathcal{O} = \{gH\}$. We can do this for all cosets and see each is a fixed point. Thus for any $h \in H$, we have $hgH = gH$, which implies $g^{-1}hg \in H$. Thus $H \trianglelefteq G$.

1.7. Classifying Groups of Order n

This section will be dedicated to classifying all groups of a certain order (up to isomorphism), for reasonable n.

1.7.1. Order 1

Let $G = \{e\}$. Any operation $\times : G \times G \to G$ will just be $e \times e = e$, so only one group exists.

1.7.2. Order 2

Since 2 is prime, the only group is C_2.

1.7.3. Order 3

Since 3 is prime, the only group is C_3.

1.7.4. Order 4

Let $G = \{e, a, b, c\}$, where e is the identity. Note that among a, b, c, at least one must be its own inverse. Suppose $a = a^{-1}$ and $c^{-1} = b$. Then we must have $ac = ca = b$, $bb = cc = a$, and $ba = ab = c$. Letting $\varphi(e) = 0, \varphi(b) = 1, \varphi(a) = 2, \varphi(c) = 3$, we see that $G \cong \mathbb{Z}/4\mathbb{Z}$.

Now suppose each element is its own inverse. Then we must have $ab = ba = c, bc = cb = a, ac = ca = b$. Letting $\varphi(e) = (0,0), \varphi(a) = (0,1), \varphi(b) = (1,0), \varphi(c) = (1,1)$, we see that $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

We've exhausted all possibilities, so the only order 4 groups are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

1.7.5. Order 5

Since 5 is prime, the only group is C_5.

1.7.6. Order 6

Obviously there's $\mathbb{Z}\backslash 6\mathbb{Z}$, so we'll look for non-cylic groups. Thus we can only have elements of order 2 and 3.

By the Sylow theorems and consequences, since $6 = 2 \cdot 3$, there must exist a unique normal subgroup of order 3, which must be isomorphic to $\mathbb{Z}/3\mathbb{Z}$. We let the elements of this subgroup H be e, g, g^2. We let the other three elements be a, b, c.

Since there's only one subgroup of order 3, all of the other elements must have order 2. Since $H \trianglelefteq G$, we have $aHa = aHa^{-1} = H$. Thus $\{aa, aga, ag^2a\} = \{e, aga, ag^2a\}$ is equal to $\{e, g, g^2\}$. If $aga = g$, then $ag = ga$, and then $ag^2 = g^2a$.

$\times$	e	g	g^2	a	b	c
e	e	g	g^2	a	b	c
g	g	g^2	e	b	c	a

2. Rings

Definition (ring): A *ring* is a triple $(R, +, \times)$ such that the following hold:
- $(R, +)$ is an abelian group, with identity 0_R, often denoted just 0.
- $\times$ is an associative, binary operation on R with some identity 1_R, often denoted just 1.
- Multiiplication distributes over addition.

The ring R is *commutative* if $\times$ is commutative.

We will assume a ring is commutative unless otherwise stated.

Example *(integers)*: $\mathbb{Z}$ is basically the canonical example of a ring, as it has many desirable properties we will defined soon, and its the easiest to understand.

3. Fields