Course Notes

Introduction to Abstract Algebra

Alex Rutar

BSM Fall 2018

Contents

Chapter 1

Fundamentals of Groups

1.1 Basics of Groups

Def'n. 1.1.1 *We say that $(G,*)$ with $* : G \times G \to G$ is a* ***group*** *if for all $a,b,c \in G$*

1. $(a*b)*c = a*(b*c)$
2. $\exists e \in G : \quad a*e = a = e*a$
3. $\exists u \in G : \quad a*u = e = u*a$

We have our first basic proposition:

Prop. 1.1.2 *The identity and inverses are unique.*

Proof If e,f are both identities, then $e = e*f = f$. If u,v are both inverses of x, then $u*(x*v) = u*e = u$ and $(u*x)*v = e*v = v$ so $u = v$. □

Def'n. 1.1.3 *If $ab = ba$ for all $a,b \in G$ then we say that G is* ***commutative****.*

Def'n. 1.1.4 *Let G be a group with $G = \{g_1, g_2, \ldots, g_n\}$. Then the* ***Cayley Table*** *for G is the matrix $M \in M_n(G)$ where $M_{ij} = g_i g_j$.*

Prop. 1.1.5 *In each column or row, each element occurs exactly once. Furthermore, if $M_{ij} = e$, then $M_{ji} = e$.*

Proof This follows directly by left or right cancellation, and by commutativity of the elements with their inverse. □

Def'n. 1.1.6 *Let $(G, \blacklozenge)$, $(H, \star)$ be groups. A mapping $f : G \to H$ is called an* ***homomorphism*** *if*

$$f(u \blacklozenge v) = f(u) \star f(v)$$

If f is also a a bijection, then we call f an ***isomorphism****.*

Prop. 1.1.7 *G and H are isomorphic if and only if their Cayley Tables are the same up to permutation of elements.*

Proof Obvious. □

1.1.1 The group $\mathbb{Z}_m$

Def'n. 1.1.8 *Let $\sim$ be an equivalence relation. We then define the **quotient group** $G/\sim$ given by the equivalence classes of elements in G.*

To construct $\mathbb{Z}_m$, we define $\mathbb{Z}_m = \mathbb{Z}/\sim$ where $a \sim b$ if $a \cong b \pmod{m}$. Since we have a division algorithm in $\mathbb{Z}$, for any $d \in \mathbb{Z}$, we can write $d = tm + r$ with $0 \leq r \leq m-1$. Thus $\overline{d} = \overline{r}$, so we can represent $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. As a result we usually do not bother writing $\overline{\cdot}$.

Prop. 1.1.9 *We have $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$.*

Proof Obvious. □

Thm. 1.1.10 $\mathbb{Z}_m^\times = \{\overline{a} \mid \gcd(a, m) = 1\}$.

Proof Assume $\overline{a} \in \mathbb{Z}_m^\times$ so there exists $\overline{x}$ with $\overline{x} \cdot \overline{a} = 1$. Then $\overline{xa} = \overline{1}$ so $xa \cong 1 \pmod{m}$ so $m|xa - 1$. Let $d = \gcd(a, m)$ so $d|a$ and $d|m$. Thus $d|xa - 1$ and $d|xa$ so $d|1$ and $\gcd(a, m) = 1$.

Conversely, suppose $\gcd(a, m) = 1$. Then by Bézout's Lemma, get x, y so that $xa + ym = 1$, so $xa \cong 1 \pmod{1}$ and $\overline{xa} = \overline{1}$ and $\overline{xa} = \overline{1}$ and we have our multiplicative inverse. □

We thus have $|\mathbb{Z}_m^\times| = \phi(m)$.

1.2 Subgroups

Def'n. 1.2.1 *A subset H of a group G is called a **subgroup** if H is also a group with the same operation. We write $H \leq G$.*

For example, $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$. Note that associativity automatically holds since every element of H is an element of G. Furthermore, $1_H = 1_G$ since $1_H 1_G = 1_H = 1_H 1_H$ where the first equality holds since 1_G is an identity, and the second since 1_H is an identity. As a result, inverses in H are inverses in G.

1.2.1 Subgroup Tests

Prop. 1.2.2 (First Subgroup Test) *A subset H of a group G is a subgroup if and only if*

1. $H \neq \emptyset$
2. $x, y \in H \Rightarrow xy \in H$
3. $x \in H \Rightarrow x^{-1} \in H$

Proof Follows by above discussion. □

Prop. 1.2.3 (Second Subgroup Test) *A subset H of a group G is a subgroup*

1. $H \neq \emptyset$
2. $x, y \in H \Rightarrow xy^{-1} \in H$

That the first subgroup test implies the second is obvious. Coversely, the identity is in H since $xx^{-1} \in H$. Thus get closure under inversion by choosing x as the identity to get inverses. Then if $x, y \in H$, $x, y^{-1} \in H$ so $x(y^{-1})^{-1} = xy \in H$.

Furthermore, if G is finite, it suffices to show closure under multiplication, since inverses can be optained by repeated multiplication.

Prop. 1.2.4 *Arbitrary intersections of subgroups are also subgroups.*

Proof Obvious. □

1.2.2 Cosets of Subgroups

Def'n. 1.2.5 *Let $H \le G$, $g \in G$. Then the **right coset** of H by g is the set $Hg := \{hg : h \in H\}$. Similarly, the **left coset** of H by g is the set $gH := \{gh : h \in H\}$.*

Ex. 1.2.6 Consider $G = \mathbb{Z}_{13}^\times = \{1, 2, \ldots, 12\}$ and $H = \langle 3 \rangle = \{1, 3, 9\}$. Then the cosets of H are given by

$$\begin{aligned} H1 &= \{1,3,9\} & H2 &= \{2,5,6\} \\ H3 &= H1 & H4 &= \{4,10,12\} \\ H5 &= H2 & H6 &= H2 \\ H7 &= \{7,8,11\} & H8 &= H7 \\ H9 &= H1 & H10 &= H4 \\ H11 &= H7 & H12 &= H4 \end{aligned}$$

so there are 4 disjoint cosets of H.

This inspires the following theorem:

Thm. 1.2.7 *Let $H \le G$. Then*

1. $|Hg| = |H|$
2. $Hg = H \Leftrightarrow g \in H$
3. *For any $x, y \in G$, either $Hx = Hy$ or $Hx \cap Hy = \emptyset$*
4. $Hx = Hy \Leftrightarrow xy^{-1} \in H$

Proof

1. The map $\cdot g : H \to Hg$ is bijective since it has an inverse.
2. This is a special case of (4) with $x = g$, $y = 1$.
3. Suppose $Hx \cap Hy \neq \emptyset$. Thus let $z \in Hx \cap Hy$ and write $z = h_1 x = h_2 y$. Then for any $hx \in Hx$, $hx = hh_1^{-1} h_1 x = hh_1^{-1} h_2 y \in Hy$ so $Hx \subseteq Hy$. The identical argument works in reverse, so equality holds.
4. Assume $Hx = Hy$, and if $x \in Hx$, then $x \in Hy$ so $x = hy$ and $xy^{-1} = h$. Conversely, suppose $xy^{-1} \in H$, then $xy^{-1}y \in Hy$ so $x \in Hy$. Also, $x \in Hx$ so $x \in Hx \cap Hy \neq \emptyset$ so by (3), $Hx = Hy$. □

Def'n. 1.2.8 *The* ***index*** *of a subgroup H in a group G is denoted $|G:H|$ and denotes the number of distinct right cosets of H.*

Prop. 1.2.9 *$Hx \mapsto x^{-1}H$ is a one-to-one correspondence between right cosets and left cosets.*

Thus G is a disjoint union of $|G:H|$ right cosets of H, each of size $|H|$. Therefore we have

Cor. 1.2.10 $|G| = |G:H| \cdot |H|$

Thm. 1.2.11 (Lagrange) *Suppose G is a finite group. Then*

1. *For any $H \leq G$, $|H| \mid |G|$.*
2. *For any $g \in G$, $o(g) \| |G|$.*

Proof
1. Since $|G| = |G:H| \cdot |H|$, $|G:H|$ is a positive integer.
2. $o(g) = |\langle g \rangle|$ and it follows by (1). □

1.2.3 Center of a Group

Def'n. 1.2.12 *For any $g \in G$, define*

$$C_G(g) = \{x \in G : gx = xg\}$$

the ***centralizer*** *of g in G. Then define the* ***center*** *of a group G*

$$Z(G) = \bigcap_{g \in G} C_G(g) \leq G$$

Note that the center of a group is the set of elements which commute with everything in the group. These are indeed groups: We certainly have $1 \in C_G(g)$. Also, if $x, y \in G$, then $gx = xg$ and $gy = yg$ so that $gxy = xgy = xyg$. If $x \in C_G(g)$, then $gx = xg$ so $g = xgx^{-1}$ and $x^{-1}g = gx^{-1}$.

This definition inspires the following definition:

Def'n. 1.2.13 *We say that f is a* ***conjugate*** *of g if and only if there exists $x \in G$ such that $x^{-1}gx = f$.*

Denote the binary relation by $\sim$: we will show that this is an equivalence relation:
1. Reflexive: $g \sim g$ by $x = 1$
2. Symmetric: If $g \sim f$, then $x^{-1}gx = f$ so $g = xfx^{-1} = (x^{-1})^{-1}fx^{-1}$
3. Transitive: If $f \sim g$ and $g \sim h$, get x, y so $x^{-1}gx = f$ and $y^{-1}fy = h$ so

$$h = y^{-1}x^{-1}gxy = (xy)^{-1}g(xy)$$

Def'n. 1.2.14 *These equivalence classes are called the* ***conjugacy classes*** *of G.*

We denote the conjugacy class of $g \in G$ by $C_g = \{x^{-1}gx : x \in G\}$. Note that $|C_g| = 1$ if and only if $C_g = \{g\}$ if and only if $x^{-1}gx = g$ for any $x \in G$ if and only if $gx = xg$ and $g \in Z(G)$.

Thm. 1.2.15 *For any $g \in G$, $|C_g| \cdot |C_G(g)| = |G|$.*

1.3 Examples of Finite Groups

1.3.1 Cyclic Groups

Def'n. 1.3.1 *The* ***order of an element*** $g \in G$ *is* $o(g) := \left|\{g^d | d \in \mathbb{Z}\}\right|$. *The* ***order of a group*** G *is* $|G|$.

We certainly have $o(g) \leq |G|$ for any $g \in G$. Equality holds when $o(g) = \infty$ and G is countable, or $G = \{g^d : d \in \mathbb{Z}\}$.

Def'n. 1.3.2 *A collection* $H = \{g_1, g_2, \dots, g_k\}$ ***generates*** G *if we can write any* $g \in G$ *as a product of elements in* H.

Def'n. 1.3.3 *We say that* G *is* ***cyclic*** *if* $G = \{g^d : d \in \mathbb{Z}\}$ *for some* $g \in G$. *Equivalently, it is generated by a set of cardinality one.*

Ex. 1.3.4 Note that $\mathbb{Z}_{13}^\times$ is cyclic with generator 2.

Lemma 1.3.5 *If* $o(g)$ *is finite and* $d \in \mathbb{Z}$, *then*

$$o(g^d) = \frac{o(g)}{\gcd(o(g), d)}$$

Proof Let $o(g) = K$ and $t = \gcd(K, d)$ and write $K = tK_1$ and $d = td_1$ with K_1, d_1 coprime. Thus $o(g^d)$ is the smallest positive integer l with $(g^d)^l = 1$. But then $(g^d)^l = 1 \Leftrightarrow g^{dl} = 1 \Leftrightarrow o(g)|dl$ and $k|dl$, that is $tK_1|td_1l$ and $k_1|d_1l$. Thus $K_1|l$ so the smallest positive intger l is K_1 and $o(g^d) = K_1 = \frac{o(g)}{\gcd(o(g),d)}$ as desired. □

Subgroups of Cyclic Groups

Thm. 1.3.6 *Any subgroup of a cyclic group is also cyclic.*

Proof Let $G = \langle g \rangle$ be a cyclic group, $H \leq G$. If $H = \{1\}$, then $H = \langle 1 \rangle$ is cyclic. Otherwise, there exists some $0 \neq m \in \mathbb{Z}$ with $g^m \in H$. Now, there exists a smallest positive integer k with $g^k \in H$. We see that $H = \langle g^k \rangle$. The reverse inclusion is obvious since $(g^k)^t \in H$ for all $t \in \mathbb{Z}$. For the forward inclusion, pick $x \in H$ so $x = g^d$ for some d. Then division with remainder yields $d = tk + r$ with $0 \leq r \leq k-1$ so that $g^d = g^{tk+r}$ and $x = (g^k)^t g^r$ so $g^r = x(g^k)^{-t} \in H$. Minimality of k forces $r = 0$, so $d = tk$, $x = g^d = (g^k)^t \in \langle g^k \rangle$. □

If $|G| = o(g) = n$ finite, write $n = tk + r$, for $0 \leq r \leq k-1$. Then $g^r = g^n(g^k)^{-t} = (g^k)^{-t} \in H$, and again $r = 0$, $n = tk$, $k|n$.

Now suppose $G = \langle g \rangle$ with finite order n. Then $G = \{1, g, g^2, \dots, g^{n-1}\}$, and subgroups of G correspond to positive diviors of n. Then $k|n \leftrightarrow \langle g^k \rangle = \{1, g^k, g^{2k}, \dots, g^{n-k}\}$ Now suppose $G = \langle g \rangle$ is infinite, and $G = \{\dots, g^{-1}, 1, g, g^2, \dots\}$. Then subgroups of G correspond to nonnegative integers, and $k \geq 0 \leftrightarrow \langle g^k \rangle = \{\dots, g^{-k}, 1, g^k, g^{2k}, \dots\}$.

Ex. 1.3.7 Consider $G = \mathbb{Z}_{13}^\times = \langle 2 \rangle$, $|\mathbb{Z}_{13}^\times| = 12 = o(2)$.

Divisor of 12	Subgroup of $\mathbb{Z}_{13}^\times$
1	$\langle 2^1 \rangle = \langle 2 \rangle = \mathbb{Z}_{13}^\times$
1	$\langle 2^2 \rangle = \langle 4 \rangle = \{1, 4, 3, 12, 9, 10\}$
1	$\langle 2^3 \rangle = \langle 8 \rangle = \{1, 8, 12, 5\}$
1	$\langle 2^4 \rangle = \langle 3 \rangle = \{1, 3, 9\}$
1	$\langle 2^6 \rangle = \langle 12 \rangle = \{1, 12\}$
1	$\langle 2^{12} \rangle = \langle 1 \rangle = \{1\}$

1.3.2 Permutation Groups

Recall that S_n is the symmetric group of degree n, consisting of all permutations of $[n]$. Thus $|S_n| = n!$. Instead of using the matrix form, we can write the permutation group using the cycle form.

Ex. 1.3.8 Write

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 3 & 1 & 2 & 9 & 8 & 5 & 6 \end{pmatrix} = (14)(2785)(3)(69)$$

We can also write (14)(2785)(69), in other words excluding elements which map to themselves.

In general, a cycle $(a_1 a_2 \ldots a_k)$ indicates that $a_1 f = a_2$, $a_2 f = a_3, \ldots, a_k f = a_1$. In S_n, each permutation can be expressed in a cycle form (using disjoint cycles). The cycle form is unique up to ordering within the cycles, and ordering among the cycles.

Ex. 1.3.9 In S_5, the possible cycle structures are

$$I, (ab), (abc), (abcd), (abcde), (ab)(cd), (ab)(cde)$$

We then have

$$\begin{aligned} o(I) &= 1 \\ o((ab)) &= 2 \\ o((abc)) &= 3 \\ o((abcd)) &= 4 \\ o((abcde)) &= 5 \\ o((ab)(cd)) &= 2 \\ o((ab)(cde)) &= 6 \end{aligned}$$

For $f = (abc)$, $f^2 = (abc)(abc) = (acb)$, $f^3 = (abc)(acb) = abc$. For $f = (abcd)$, $f^2 = (ac)(bd)$, $f^3 = (abdc)(ac)(bd)(adcb)$, and $f^4 = (abcd)(adcb) = (abcd)$.

If $f = (a_1 a_2 \ldots a_k)$, $o(f) = k$.

Prop. 1.3.10 *Suppose $f = \gamma_1 \gamma_2 \ldots \gamma_i$ for disjoint cycles. Then $o(f) = lcm(o(\gamma_1), o(\gamma_2), \ldots, o(\gamma_i))$.*

Proof Note that the γ_i commute, so that

$$\begin{aligned} f^d = I &\Leftrightarrow (\gamma_1 \gamma_2 \ldots \gamma_i)^d = I \\ &\Leftrightarrow \gamma_1^d \gamma_2^d \ldots \gamma_i^d = I \\ &\Leftrightarrow \gamma_i^d = I \quad \forall i \end{aligned}$$

The last line holds since the γ_i^d operates on disjoint sets. Thus we have our formula, as desired. □

Note that any finite permutation of $f \in S_n$ can be expressed as a composition of 2-cycles. For example, $(abc) = (ab)(ac)$ and in general $(a_1 a_2 \dots a_k) = (a_1 a_2)(a_1 a_3)\dots(a_1 a_k)$. In general, any k−cycle can be replaced by a composition of $(k-1)$ 2-cycles. This motivates the following definition:

Def'n. 1.3.11 *A permutation $f \in S_n$ is* ***even*** *if it can be expressed as a composition of an even number of 2-cycles. Then $f \in S_n$ is* ***odd*** *if it can be expressed as a composition of an odd number of 2-cycles.*

For example, $(15362)(4798) = (15)(13)(16)(12)(47)(49)(48)$ can be written as a composition of 7 2-cycles. This is certainly not unique: for example $(26) = (21)(16)(21)$.

Lemma 1.3.12 *The identity permutation is not odd.*

Proof For contradiction, assume

$$I = \alpha_1 \alpha_2 \dots \alpha_k$$

and assume that such an odd k is a minimal counterxample. We certainly have $k \geq 3$. Say $\alpha_1 = (cd)$, so c must be involved in another α_i, or d is mapped to c. Let α_r be the last 2-cycle involving c, say $\alpha_r = (cx)$. Now we rewrite α_{r-1} without changing $\alpha_{r-1}\alpha_r$.

1. If $\alpha_{r-1} = (yz)$ disjoint from $\alpha_r = (cx)$, then $(yz)(cx) = (cx)(yz)$.
2. If $\alpha_{r-1} = (cy)$ with $y \neq x$, then $(cy)(cx) = (xc)(xy)$.
3. If $\alpha_{r-1} = (xy)$, $y \neq c$, then $(xy)(cx) = (yc)(yx)$.
4. $\alpha_{r-1} = \alpha_r$ so $(cx)(cx) = I$, contradicting minimality.

We can repeat this process until the last 2-cycle involving c is α_1, a contradiction. □

Prop. 1.3.13 *A permutation cannot be both even and odd.*

Proof Suppose f can be written as an even and odd permutation:

$$f = \alpha_1 \alpha_2 \dots \alpha_m$$
$$f = \beta_1 \beta_2 \dots \beta_n$$

but then

$$I = \alpha_1 \alpha_2 \dots \alpha_m \alpha_m \dots \alpha_2 \alpha_1 = \beta_1 \beta_2 \dots \beta_n \alpha_m \alpha_{m-1} \dots \alpha_1$$

so I is odd, a contradiction. □

Def'n. 1.3.14 *We define the* ***signature*** $\operatorname{sgn}(f)$ *to be* 1 *of* f *is even, and* -1 *if* f *is odd.*

Prop. 1.3.15 *1.* $\operatorname{sgn}(f^{-1}) = \operatorname{sgn}(f)$
2. $\operatorname{sgn}(fg) = \operatorname{sgn}(f)\operatorname{sgn}(g)$

Proof Follows directly from the 2-cycle decomposition. □

Def'n. 1.3.16 *The* ***alternating group*** *of degree n is the group $A_n = \{f \in S_n : \operatorname{sgn}(f) = 1\} \leq S_n$.*

Thm. 1.3.17 $|A_n| = \frac{n!}{2}$.

Proof We see two separate proofs.

1. Consider $\phi : A_n \to S_n \setminus A_n$ by $f \mapsto f(12)$. This is injective since if $\phi(f) = \phi(g)$, then $f(12) = g(12)$ and $f = g$. It is surjective: if g is odd, then $g(12)$ is even that $\phi(g(12)) = g$. Thus ϕ is bijective and $|A_n| = |S \setminus A_n| = |A| - |A_n|$ so $|A_n| = |S_n|/2 = n!/2$.
2. We claim that $|S_n : A_n| = 2$. For $f \in S_n$ even, $f \in A_n$ so $A_n f = A_n$. For $f \in S_n$ odd, f^{-1} is odd and $(12)f^{-1}$ is even and $(12)f^{-1} \in A_n$. Thus $A_n(12) = A_n f$, so there are only two cosets of A_n: A_n and $A_n(12)$, and the result follows by Lagrange's Theorem. □

Centralizers of Permutation Groups

Ex. 1.3.18 Consider $g = (12)(34) \in S_4$. Then $C_{S_4}(g) = \{x \in S_4 \mid gx = xg\} = \{I, (12)(34), (12), (34), (14)(23), (1$

The key idea is to observe that $x^{-1}gx = g$, which is called the conjugate of g by x.

Ex. 1.3.19 Consider $f = (34)(1572)(86)(9)$, $g = (194)(368)(257)$.

$$\begin{aligned} g^{-1}fg &= (752)(863)(491)(34)(1572)(86)(194)(368)(257) \\ &= (16)(2597)(38)(4) \\ &= (3g)(4g)(1g5g7g2g)(8g6g)(9g) \end{aligned}$$

In general, if $f, g \in S_n$ and $(a_1 a_2, \ldots, a_k)$ is a cycle in the cycle form of f, then $(a_1 z a_2 z \ldots a_k z)$ is a cycle in the cycle form of $z^{-1}fz$. To see this, $a_1 z(z^{-1}fz) = a_1 f z = a_2 z$, so $a_1 z$ maps to $a_2 z$, and similarly for all the pairs of elements in the cycle.

If we now return to $(12)(34)x = x(12)(34)$, we have $x^{-1}(12)(34)x = (12)(34)$ so

$$(1x\,2x)(3x\,4x) = (12)(34)$$

Since the cycle form is unique up to rearranging within cycles, we have

LHS	$1x$	$2x$	$3x$	$4x$	x
(12)(34)	1	2	3	4	I
(21)(34)	2	1	3	4	(12)
(12)(43)	1	2	4	3	(34)
(21)(43)	2	1	4	3	(12)(34)
(34)(12)	3	4	1	2	(13)(24)
(34)(21)	3	4	2	1	(1324)
(43)(12)	4	3	1	2	(1423)
(43)(21)	4	3	2	1	(14)(23)

Let's now compute the conjugacy classes of S_n. Let's do S_3 first: The conjugacy classes are given by

$$\{1\}, \{(12), (13), (23)\}, \{(123)\}$$

In general, the conjugacy classes in S_n correspond to the possible cycle structures in S_n.None

1.3.3 Dihedral Groups

Fix a regular polygon with n vertices. Let D_n be the collection of rigid motions with map the regular n–polygon to itself. Since $r^n = 1$ and $s^2 = 1$, we have

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

Thus $|D_n| = 2n$. We can compute the oprations on D_n:

$$\begin{aligned} r^a \cdot r^b &= r^{a+b} \\ sr^a \cdot r^b &= sr^{a+b} \\ r^a \cdot sr^b &= sr^{b-a} \\ sr^a \cdot sr^b &= r^{b-a} \end{aligned}$$

Thus $o(sr^a) = 2$ and $o(r^a)$ is given by the usual formula.