Math 305 Notes

Course Intro

Welcome! The main changes from Math 304 to 305 are:

- More lecture
- Less formal daily work
- A bit more written work

Any questions?

3 Intro to Groups

DEF 1: [1] A *binary operation* on a set G is a function $G \times G \to G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a \circ b$, or ab, in G, called the composition of a and b. A group $(G, \circ)$ is a set G together with a binary operation $(a, b) \mapsto a \circ b$ that satisfies associativity, identity, and inverses. If the operation is commutative, we say G is *abelian*.

RMRK 2: Judson calls these *laws of composition*. I'll stick with binary operations.

EX. 3: $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, any ring R with its addition

NOTATION 4: We typically write ab instead of $a \circ b$; when operations are familiar, we use familiar notation, e.g., $m - n$ instead of $m + (-n)$, etc.

EX. 5: Cayley table for $\mathbb{Z}_5$ under addition.

DEF 6: This is known as a *Cayley table*.

EX. 7: $\mathbb{Z}_n, n > 1$ is never a group under multiplication modulo n. *Why not?*

EX. 8: If $n > 1$ is an integer and $\gcd(k, n) = 1$, then k is invertible modulo n. By $U(n)$ we will denote the group of units modulo n (in Math 304, this was $(\mathbb{Z}_n)^\times$). Let's work out the Cayley table for $U(10)$.

EX. 9: The general linear group, $\mathrm{GL}_2(\mathbb{R})$ is the set of 2×2 invertible matrices with real entries.

EX. 10: Let $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, and $K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, where $i^2 = -1$. Show: $I^2 = J^2 = K^2 = -1$, $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$, and $IK = -J$. The set $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$ is called the *quaternion group*.

DEF 11: A group is *finite*, or has *finite order*, if it contains a finite number of elements; otherwise, the group is said to be *infinite* or to have *infinite order*. We write $|G| = n$ or $|G| = \infty$. We won't worry about the particular size of infinity.

3.1 Basic Properties of Groups

PROP 12: Identities and inverses are unique.

Proof. Standard. □

PROP 13: If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. By definition, $(ab)(ab)^{-1} = e$. But $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$, and the result follows by uniqueness. □

PROP 14: For any $a \in G$, $(a^{-1})^{-1} = a$.

Proof. Multiply $a^{-1}(a^{-1})^{-1} = e$ by a. □

NOTE 15: Groups also have a *right/left cancellation law*: Given $a, b, c \in G$, $ba = ca \Rightarrow b = c$ and $ab = ac \Rightarrow b = c$.

NOTATION 16: [2] We define $g^0 = e$, and for $n \in \mathbb{N}$,

$$g^n = \underbrace{g \cdot g \cdots g}_{n \text{ times}}$$

and

$$g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}$$

THM 17: The usual laws of exponents hold, given $g, h \in G$ and $m, n \in \mathbb{Z}$:

1. $g^m g^n = g^{m+n}$
2. $(g^m)^n = g^{mn}$
3. $(gh)^n = (h^{-1}g^{-1})^{-n}$. If G is abelian, then $(gh)^n = g^n h^n$.

3.3 Subgroups

DEF 18: Let G be a group. A *subgroup* H of G is a subset of G such that when the operation of G is restricted to H, H is a group in its own right. We write $H \leq G$.

RMRK 19: Every group G has at least two subgroups: $\{e\}$ (the *trivial subgroup* and G. A *proper* subgroup H is a proper subset of G.

$\mathbb{Q}^* \leq \mathbb{R}^*$.

$H = \{1, -1, i, -i\} \leq \mathbb{C}^*$.

$\mathrm{SL}_2(\mathbb{R}) \leq \mathrm{GL}_2(\mathbb{R})$; note that if $A \in \mathrm{SL}_2(\mathbb{R})$ that $A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

RMRK 20: It is possible to have groups that are subsets of other groups, but not subgroups. The operations must be the same. So for instance, $\mathrm{GL}_2(\mathbb{R}) \subseteq \mathbb{M}_2(\mathbb{R})$, but the former is a group under matrix multiplication, while the latter is only a group under matrix addition (though in fact, it is a noncommutative ring).

QUESTION 21: Given two groups G_1 and G_2, how can you tell if they are "the same" (that is, isomorphic)? One way is by examining their subgroups. Two groups with different subgroup structures can't be the same, even if their orders are. So, e.g., $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are different, as $\mathbb{Z}_4$ has only one subgroup of order 2, while $\mathbb{Z}_2 \times \mathbb{Z}_2$ has three.

QUESTION 22: How can we tell if a given set H is a subgroup of G? It turns out we don't need to check everything.

PROP 23: A subset H of a group G is a subgroup if and only if it satisfies the following conditions.

1. The identity e of G is in H.
2. If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.
3. If $h \in H$, then $h^{-1} \in H$.

Proof. The reverse is clear, so we focus on the forward direction. Since H is a group it has an identity, e_H. We show $e_H = e$ by observing that $e_H e_H = e_H$, and $e e_H = e_H$,

so that $e_H e_H = e e_H$, and right cancellation gives our desired outcome. The second condition holds since H is a group. For the third, if $h \in H$ then h has an inverse h' in H, but also an inverse h^{-1} in G. But by uniqueness of inverses, these are the same. □

PROP 24: A subset H of a group G is a subgroup of G if and only if $H \neq \emptyset$, and whenever $g, h \in H$, then $gh^{-1} \in H$.

Proof. If $H \leq G$, then $gh^{-1} \in H$ whenever g and h are in H, by closure under multiplication and the taking of inverses.

Conversely, suppose $H \subseteq G$ such that $H \neq \emptyset$ and $gh^{-1} \in H$ whenever $g, h \in H$. If $g \in H$, then $gg^{-1} = e \in H$, and $eg^{-1} = g^{-1} \in H$. Further, given $h_1, h_2 \in H$, $h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$, so H is a subgroup by the previous proposition. □

4 Cyclic Subgroups

There is more in Chapter 4 than we're going to cover.

DEF 25: Let G be a group and $a \in G$. The *cyclic subgroup generated by a*, denoted a, is the set $a = \{a^k : k \in \mathbb{Z}\}$. If there is an element $g \in G$ for which $G = g$, we say G is a *cyclic group*.

THM 26: Given a group G and $a \in G$, a is indeed a subgroup.

EX. 27: What examples can we think of?

EX. 28: $\mathbb{Z}_6 = 1 = 5$

EX. 29: $U(9) = 2$

EX. 30: $U(8) = \{1, 3, 5, 7\}$ is not cyclic; each nonidentity element generates a subgroup of order 2.

THM 31: [3] Every cyclic group is abelian.

THM 32: Every subgroup of a cyclic group is cyclic.

Proof. Let $G = a$ and $H \leq G$. If $H = \{e\}$, we are done, so suppose H contains a nonidentity element g. Then $g = a^n$ for some $n \in \mathbb{Z}$. Since H is a subgroup, $g^{-1} = a^{-n} \in H$. Since either $n > 0$ or $-n > 0$, H contains positive powers of a. Let m be the smallest natural number power of a in H; we claim $H = a^m$.

Let $h' \in H$. We know that $h' \in G$ so $h' = a^k$ for some k; by the division algorithm, $k = mq + r$, where $0 \leq r < m$, so $a^k = a^{mq+r} = (a^m)^q a^r$. So, $a^r = a^k (a^m)^{-q}$. But this means $a^r \in H$, which is a contradiction if $r > 0$. Consequently, $k = mq$, and $H = a^m$. □

COR 33: The subgroups of $\mathbb{Z}$ are m where $m \in \mathbb{Z}$.

PROP 34: Let G be cyclic of order n and suppose that a is a generator for G. Then $a^k = e$ if and only if $n|k$.

Proof. First, suppose that $a^k = e$. By the division algorithm, $k = nq + r$; hence $e = a^k = a^{nq+r} = a^{nq} a^r = e a^r = a^r$. Since $n = |a|$, $r = 0$.

The converse is straightforward. □

THM 35: Let G be cyclic of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then $|b| = n/d$, where $d = \gcd(k, n)$.

Proof. We wish to find the smallest integer m such that $e = b^m = a^{km}$. By the previous proposition, this is the smallest integer m such that $n|km$, or, equivalently, $n/d|m(k/d)$. Since $d = \gcd(k, n)$, $\gcd(n/d, k/d) = 1$. Hence, for n/d to divide $m(k/d)$, $n/d|m$. The smallest such m is n/d. □

COR 36: The generators of $\mathbb{Z}_n$ are the integers r such that $1 \leq r < n$ and $\gcd(r, n) = 1$.

EX. 37: What are the generators of $\mathbb{Z}_{10}$?

5 Permutation Groups

THM 38: The symmetric group on n letters, S_n, is a group with $n!$ elements, where the binary operation is the composition of maps.

Proof. Straightforward. □

EX. 39: Make a subgroup of S_5 consisting of $\sigma = (4\ 5)$, $\tau = (1\ 3)$, and $\mu = (1\ 3)(4\ 5)$ and the identity. Cayley table!

EX. 40: These groups are never abelian for $n \geq 3$: $\sigma = (1\ 4\ 3\ 2)$ and $\tau = (1\ 2)(3\ 4)$ don't commute in S_4, for instance.

DEF 41: Let S_X be the permutation group on the set X. A *cycle of length k* is a permutation σ such that there are k elements $a_1, a_2, \ldots, a_k \in X$ for which $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3, \ldots, \sigma(a_k) = a_1$, and $\sigma(x) = x$ for all $x \neq a_i$. We will write $(a_1\ a_2\ \cdots\ a_k)$ to denote the cycle σ. Every permutation in S_n can be represented this way (in fact, as a product of disjoint permutations!).

EX. 42: Examples of cycles of various lengths.

EX. 43: Not every permutation is a cycle. For instance:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1\ 2\ 4\ 3)(5\ 6)$$

EX. 44: Compute some products of cycles. **Very important**: our book adopts the convention that we multiply right-to-left, as functions are composed. This is not what I am used to, but I will try to follow along!!

DEF 45: Two cycles in S_X, $\sigma = (a_1\ a_2\ \cdots\ a_k)$ and $\tau = (b_1\ b_2\ \cdots\ b_\ell)$ are *disjoint* if $a_i \neq b_j$ for all i, j.

PROP 46: Let $\sigma, \tau \in S_X$ be disjoint cycles. Then $\sigma\tau = \tau\sigma$.

Proof. Let $\sigma = (a_1\ a_2\ \cdots\ a_k)$ and $\tau = (b_1\ b_2\ \cdots\ b_\ell)$ be in S_X. We need to show that $\sigma\tau(x) = \tau\sigma(x)$ for all $x \in X$. If x is not among the elements of X permuted by σ or τ, then $\sigma\tau(x) = x = \tau\sigma(x)$.

On the other hand, suppose $x \in \{a_1, a_2, \ldots, a_k\}$. By definition $\sigma(a_i) =$

$a_{(i \mod k)+1}$ and $\tau(a_i) = a_i$. Therefore:

$$\begin{aligned}\sigma\tau(a_i) &= \sigma(\tau(a_i)) \\ &= \sigma(a_i) \\ &= a_{(i \mod k)+1} \\ &= \tau(a_{(i \mod k)+1}) \\ &= \tau(\sigma(a_i)) \\ &- \tau\sigma(a_i).\end{aligned}$$

Similarly, if $x \in \{b_1, b_2, \dots, b_\ell\}$, σ and τ also commute. □

THM 47: Every permutation in S_n can be written as the product of disjoint cycles.

Proof. We can assume that $X = \{1, 2, \dots, n\}$. If $\sigma \in S_n$ and we define $X_1 = \{\sigma(1), \sigma^2(1), \dots\}$, Then X_1 is finite and X is finite. Now let $i \in X$ be the first integer not in X_1, and define $X_2 = \{\sigma(i), \sigma^2(i), \dots\}$. Again, X_2 is finite.

Continuing in this manner, we can define disjoint sets $X_3, X_4, \dots$. Since X is a finite set, this process will end and there will be only a finite number of these sets, say r. If σ_i is the cycle defined by

$$\sigma_i(x) = \begin{cases}\sigma(x) & x \in X \\ x & x \notin X\end{cases},$$

then $\sigma = \sigma_1\sigma_2\cdots\sigma_r$. Since the sets $X_1, X_2, \dots, X_r$ are disjoint, the cycles $\sigma_1, \sigma_2, \dots, \sigma_r$ must also be disjoint. □

EX. 48: Let $\sigma = (1\ 6\ 2\ 4)$ and $\tau = (1\ 3)(4\ 5\ 6)$. Calculate $\tau\sigma$ and $\sigma\tau$.

DEF 49: A permutation of length 2 is called a *transposition*.

PROP 50: Any permutation of a finite set containing at least two elements can be written as the product of transpositions.

Proof. Write $(a_1\ a_2\ \cdots\ a_n) = (a_1\ a_n)(a_1\ a_{n-1})\cdots(a_1\ a_3)(a_1\ a_2)$. □

EX. 51: Observe that $(1\ 4\ 3)(2\ 5\ 6) = (1\ 4)(1\ 3)(2\ 5)(2\ 6)$. But also note that we could throw some other transpositions in there, too.

RMRK 52: It turns out there is no unique way to represent a permutation as a product of transpositions. However, the *parity* of the number of transpositions turns out to be unique. To prove that, we need a lemma.

LEM 53: [4] If the identity is written as the product of r transpositions,

$$\mathrm{id} = \tau_1\tau_2\cdots\tau_r,$$

then r is an even number.

Proof. Induction on r. If $r = 1$, it can't be the identity, hence $r > 1$. If $r = 2$, we are done.

Suppose that $r > 2$. In this case, the product of the last two transpositions, $\tau_{r-1}\tau_r$, must be one of the following cases:

$$\begin{aligned}(a\ b)(a\ b) &= \mathrm{id} \\ (b\ c)(a\ b) &= (a\ c)(b\ c) \\ (c\ d)(a\ b) &= (a\ b)(c\ d) \\ (a\ c)(a\ b) &= (a\ b)(b\ c),\end{aligned}$$

where a, b, c, d are distinct.

The first equation says that a transposition is its own inverse. If this occurs, delete $\tau_{r-1}\tau_r$ from the product to obtain

$$\mathrm{id} = \tau_1\tau_2\cdots\tau_{r-3}\tau_{r-2}.$$

In each of the other three cases, we can replace $\tau_{r-1}\tau_r$ with the right-hand side of the corresponding equation to obtain a new product of r transpositions for the identity.

In this new product, the next-to-last transposition will be the last occurence of a.

We can continue this process with $\tau_{r-2}\tau_{r-1}$ to obtain either a product of $r-2$ transpositions or a new product of r transpositions, in which the last occurrence of a has moved to τ_{r-2}. If the identity is the product of $r-2$ transpositions, then again we are done by induction; otherwise, we repeat with $\tau_{r-3}\tau_{r-2}$.

At some point we will either have two adjacent, identical transpositions canceling each other out, or a will be shuffled so that it will appear in only the first transposition. However, the latter case cannot occur, because the identity would not fix a in this instance.

Therefore, the identity permutation must be the product of $r-2$ transpositions and, again by our induction hypothesis, we are done. □

THM 54: If a permutation σ can be expressed as an even number of transpositions, then any other product of transpositions equaling σ must also contain an even number of transpositions. Similarly, if σ can be expressed as the product of an odd number of transpositions, then any other product of transpositions equaling σ must also contain an odd number of transpositions.

Proof. Suppose that

$$\sigma = \sigma_1\sigma_2\cdots\sigma_m = \tau_1\tau_2\cdots\tau_n,$$

where m is even. We must show that n is also an even number. The inverse of σ is $\sigma_m\cdots\sigma_1$. Since

$$\mathrm{id} = \sigma\sigma_m\cdots\sigma_1 = \tau_1\cdots\tau_n\sigma_m\cdots\sigma_1,$$

n must be even by the lemma. The proof in the case that σ can be expressed as an odd number of transpositions is an exercise. □

DEF 55: We say that σ is an *even* (resp., *odd*) permutation if it can be expressed as en even (resp., odd) number of transpositions.

DEF 56: Let $A_n = \{\sigma \in S_n \ : \ \sigma \text{ is even}\}$. We call A_n the *alternating group on n letters*.

THM 57: $A_n \leq S_n$.

Proof. By Lemma 53, $\mathrm{id} \in A_n$. Now let $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ and $\tau = \tau_1\tau_2\cdots\tau_s$ be in A_n. Observe that $\tau^{-1} = \tau_s\tau_{s-1}\cdots\tau_2\tau_1$. Then $\sigma\tau^{-1} = \sigma_1\sigma_2\cdots\sigma_r\tau_s\tau_{s-1}\cdots\tau_2\tau_1 \in A_n$ as it consists of an even number of transpositions. □

PROP 58: The number of even permutations in S_n, $n \geq 2$, is equal to the num-

ber of odd permutations; hence, the order of A_n is $n!/2$.

Proof. Let A_n be the set of even permutations in S_n and B_n be the set of odd permutations. If we can show that there is a bijection between these sets, they must contain the same number of elements, and since every permutation is even or odd, that number is $n!/2$.

Fix a transposition $\sigma \in S_n$. Since $n \geq 2$, such a σ exists. Define

$$\lambda_\sigma : A_n \to B_n$$

by

$$\lambda_\sigma(\tau) = \sigma\tau.$$

Suppose that $\lambda_\sigma(\tau) = \lambda_\sigma(\mu)$. Then $\sigma\tau = \sigma\mu$ and so

$$\tau = \sigma^{-1}\sigma\tau = \sigma^{-1}\sigma\mu = \mu.$$

Therefore, λ_σ is one-to-one.

To see that λ_σ is onto, let $\mu \in B_n$; observe that $\sigma\mu$ is even, so $\lambda_\sigma(\sigma\mu) = \sigma\sigma\mu = \mu$. □

5.2 Dihedral Groups

DEF 59: Let $n \geq 3$. The *nth dihedral group* is the set of rigid motions of a regular n-sided polygon, or n-gon, and denoted by D_n.

THM 60: The dihedral group, D_n, is a subgroup of S_n of order $2n$.

Proof. We can number the vertices of a regular n-gon $1, 2, \ldots, n$. Notice that there are exactly n choices to replace the first vertex. If we replace the first vertex by k, the second vertex must be replaced by either $k+1$ or $k-1$. Thus, there are $2n$ possible rigid motions of the n-gon. □

THM 61: The group $D_n, n \geq 3$, consists of all products of the two elements r and s, where r has order n and s has order 2, and these two elements satisfy the relation $srs = r^{-1}$.

Proof. The possible motions of a regular n-gon are either reflections or rotations. There are exactly n possible rotations:

$$\text{id}, \frac{360°}{n}, 2 \cdot \frac{360°}{n}, \ldots, (n-1) \cdot \frac{360°}{n}.$$

Let $r = \frac{360°}{n}$. The rotation r generates all other rotations: $r^k = k \cdot \frac{360°}{n}$.

Label the n reflections $s_1, s_2, \ldots, s_n$, where s_k is the reflection that leaves vertex k fixed. There are two cases of reflections, depending on whether n is even or odd. If n is even, then two vertices are left fixed by a reflection, and $s_1 = s_{n/2+1}$, $s_2 = s_{n/2+2}, \ldots, s_{n/2} = s_n$. If there are an odd number of vertices, then a single vertex is fixed by each reflection; in either case, the order of each s_k is two.

Let $s = s_1$. Then $s^2 = 1$ and $r^n = 1$. Since any rigid motion t of the n-gon replaces the first vertex by the vertex k, the second vertex must be replaced by either $k+1$ or $k-1$. If the second vertex is replaced by $k+1$, then $t = r^k$. If the second vertex is replaced by $k-1$, then $t = r^k s$. Hence, r and s generated D_n. That is, D_n

consists of all finite products of r and s,

$$D_n = \{1, rr^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}$$

The proof that $srs = r^{-1}$ is left as an exercise. □

Ex. 62: Let's explore D_4. With the vertices numbered 1, 2, 3, 4, the rotations are

$$\begin{aligned} r &= (1\ 2\ 3\ 4) \\ r^2 &= (1\ 3)(2\ 4) \\ r^3 &= (1\ 4\ 3\ 2) \\ r^4 &= (1) \end{aligned}$$

and the reflections are

$$\begin{aligned} s_1 &= (2\,4) \\ s_2 &= (1, 3) \end{aligned}$$

We note $|D_4| = 8$; the two remaining elements are $rs_1 = (1\ 2)(3\ 4)$ and $r^3s_1 = (1\ 4)(2\ 3)$.

6 Cosets and Langrange's Theorem

6.1 Cosets

Def 63: Let G be a group and H a subgroup of G. Define a *left coset of H with representative $g \in G$* to be the set

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

Right cosets are defined similarly by

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

If left and right cosets coincide or if it is clear from the context to which type of coset that we are referring, we will use the word coset without specifying left or right.

Cosets in $\mathbb{Z}_5$, written additively.

Let $K = \{(1), (1\ 2)\} \leq S_3$. Then the left cosets of K are

$$\begin{aligned} (1)K = (1\ 2)K &= K \\ (1\ 3)K = (1\ 2\ 3)K &= \{(1\ 3), (1\ 2\ 3)\} \\ (2\ 3)K = (1\ 3\ 2)K &= \{(2\ 3), (1\ 3\ 2)\}. \end{aligned}$$

The right cosets are

$$\begin{aligned} K(1) = K(1\ 2) &= K \\ K(1\ 3) = K(1\ 3\ 2) &= \{(1\ 3), (1\ 3\ 2)\} \\ K(2\ 3) = K(1\ 2\ 3) &= \{(2\ 3), (1\ 2\ 3)\}. \end{aligned}$$

Rmrk 64: Observe that a coset is not a subgroup!

Lem 65: Let $H \leq G$ and suppose that $g_1, g_2 \in G$. Then the following are equivalent:

1. $g_1H = g_2H$
2. $Hg_1^{-1} = Hg_2^{-1}$
3. $g_1H \subseteq g_2H$
4. $g_2 \in g_1H$
5. $g_1^{-1}g_2 \in H$

Proof. Let's try proving these in a cycle.

(1) ⇒ (2): Consider $hg_1^{-1} \in Hg_1^{-1}$. Observe that $g_2 = g_1h'$ for some $h' \in H$ so $e = g_1h'g_2^{-1}$, and hence $g_1^{-1} = h'g_2^{-1}$. Thus, $hg_1^{-1} = h(h'g_2^{-1}) = (hh')g_2^{-1} \in Hg_2^{-1}$. The reverse containment is proved symmetrically.

(2) ⇒ (3): Given $h \in H$, we wish to show that $g_1h = g_2h'$ for some $h' \in H$.

Note that $g_1 = g_1 e \in g_2 H$, so there is some h' for which $g_1 = g_2 h'$. Write $g_1 h = (g_2 h')h = g_2(h'h) \in g_2 H$.

(3) $\Rightarrow$ (4): We wish to show that there is some $h' \in H$ for which $g_2 = g_1 h'$. By statement (3), we have $g_1 = g_2 h$ for some $h \in H$, which means $g_2 = g_1 h^{-1}$.

(4) $\Rightarrow$ (5): Since $g_2 \in g_1 H$, $g_2 = g_1 h$, so $g_1^{-1} g_2 = h \in H$.

(5) $\Rightarrow$ (1): Let $g_1 h \in g_1 H$. We wish to find an $h' \in H$ for which $g_1 h = g_2 h'$. Observe that since $g_1^{-1} g_2 = h' \in H$, $g_2 = g_1 h'$, and $g_1 = g_2 (h')^{-1}$. So, $g_1 h = (g_2 (h')^{-1})h = g_2((h')^{-1} h) \in g_2 H$. Similarly, given $g_2 h \in g_2 H$, $g_2 h = (g_1 h')h = g_1(hh') \in g_1 H$, so $g_1 H = g_2 H$. □

RMRK 66: This lemma will be super useful in establishing properties of cosets, including the following.

THM 67: Let $H \leq G$. Then the left (resp. right) cosets of H in G partition G. That is, G is the disjoint union of the left (resp. right) cosets of H in G.

Proof. Let $g_1 H$ and $g_2 H$ be two cosets of H in G. We must show either $g_1 H \cap g_2 H = \emptyset$ or $g_1 H = g_2 H$.

If $g_1 H \cap g_2 H \neq emptyset$ and $a \in g_1 H \cap g_2 H$, then $a = g_1 h_1 = g_2 h_2$. Thus $g_1 = g_2 h_2 h_1^{-1}$, or $g_1 \in g_2 H$. By the lemma, $g_1 H = g_2 H$. □

RMRK 68: Let G be a group and H a subgroup of G. The *index* of H in G is the number of left cosets of H in G. We denote the index by $[G : H]$.

Let $G = \mathbb{Z}_6$ and $H = \{0, 3\}$. Then $[G : H] = 3$. If $K = \{0, 2, 4\}$, then $[G : K] = 2$.

If $G = S_3$ and $H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$, then $[G : H] = 2$.

THM 69: Let $H \leq G$. The number of left cosets of H in G is the same as the number of right cosets of H in G.

Proof. Let $\mathcal{L}_H$ and $\mathcal{R}_H$ denote the sets of left and right cosets of H in G, respectively. We seek a bijection $\varphi : \mathcal{L}_H \to \mathcal{R}_H$. If $gH \in \mathcal{L}_H$, let $\varphi(gH) = Hg^{-1}$. By the Lemma, this is well-defined, since if $g_1 H = g_2 H$, then $H g_1^{-1} = H g_2^{-1}$.

To show that φ is one-to-one, suppose that $H g_1^{-1} = \varphi(g_1 H) = \varphi(g_2 H) = H g_2^{-1}$.

Again, by the lemma, $g_1 H = g_2 H$. The map φ is onto since $\varphi(g^{-1} H) = Hg$. □

6.2 Lagrange's Theorem

PROP 70: Let $H \leq G$ with $g \in G$ and define a map $\varphi : H \to gH$ by $\varphi(h) = gh$. Then φ is bijective, and so $|H| = |gH|$.

Proof. Suppose $\varphi(h_1) = \varphi(h_2)$; we wish to show that $h_1 = h_2$. But this is immediate, since $gh_1 = gh_2$, so $h_1 = h_2$. Then, given $gh \in gH$, $\varphi(h) = gh$, so φ is onto. □

THM 71: (Lagrange) Let G be a *finite* group and $H \leq G$. Then $|G|/|H| = [G : H]$ is the number of distinct left cosets of H in G. In particular, $|H|$ divides $|G|$.

Proof. The group G is partitioned into $[G : H]$ distinct left cosets, each of order $|H|$. Therefore, $|G| = [G : H]|H|$. □

COR 72: If G is finite and $g \in G$, then $|g|$ divides $|G|$.

Proof. Recall that $|g| = |g|$ and apply Lagrange's Theorem. □

COR 73: If $|G| = p$, where p is prime, then G is cyclic and is generated by any nonidentity element.

Proof. Let $g \in G$, $g \neq e$. By the corollary, $|g|$ divides $|G|$, which is prime. Since $|g| \neq 1$, $|g| = |g| = p$, so $G = g$. □

COR 74: Let $H, K \leq G$, G finite, such that $K \subseteq H \subseteq G$. Then $[G : K] = [G : H][H : K]$.

Proof. Observe that

$$\begin{aligned}[G : K] &= \frac{|G|}{|K|} \\ &= \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} \\ &= [G : H][H : K].\end{aligned}$$

□

RMRK 75: The converse of Lagrange's theorem is false. That is, $d||G|$ does not imply that G has a subgroup of order d.

FACT 76: A_4 contains 8 three-cycles. There are $4 \cdot 3 \cdot 2$ ways to make a 3-cycle, but it doesn't matter which of the 3 numbers comes first, so there are $4 \cdot 3 \cdot 2/3 = 8$ three-cycles.

PROP 77: The group A_4 has no subgroup of order 6.

Proof. Suppose A_4 has a subgroup H of order 6. Then $[A_4 : H] = 2$. One of the cosets is H itself, so left and right cosets must coincide (they both partition A_4, and one of the two parts of the partition is set). That is, $gH = Hg$, or $gHg^{-1} = H$ for every $g \in A_4$.

Since there are 8 three-cycles in A_4, at least one 3-cycle must be in H. Without loss of generality assume $(1\ 2\ 3) \in H$. Then $(1\ 2\ 3)^{-1} = (1\ 3\ 2) \in h$ as well.

Since $ghg^{-1} \in H$ for all $g \in A_4$ and $h \in H$, and

$$(1\ 2\ 4)(1\ 2\ 3)(1\ 2\ 4)^{-1} = (2\ 4\ 3), (2\ 3\ 4) \in H$$
$$(2\ 4\ 3)(1\ 2\ 3)(2\ 4\ 3)^{-1} = (1\ 4\ 2), (1\ 2\ 4) \in H.$$

Thus, H contains at least seven elements: the identity and these six three-cycles. This is a contradiction. □

THM 78: Two cycles τ and μ in S_n have the same length if and only if there exists $\sigma \in S_n$ such that $\mu = \sigma\tau\sigma^{-1}$.

Proof. Suppose $\tau = (a_1\ a_2 \cdots\ a_k)$ and $\mu = (b_1\ b_2 \cdots b_k)$. Define σ to be the permutation for which $a_i \mapsto b_i$ and everything else is fixed. Then $\mu = \sigma\tau\sigma^{-1}$.

Conversely, suppose $\tau = (a_1\ a_2\ \cdots\ a_k)$ is a k-cycle and $\sigma \in S_n$. If $\sigma(a_i) = b$ and $\sigma(a_{(i \mod k)+1}) = b'$, then $\mu(b) = b'$. Hence,

$$\mu = (\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k)).$$

Since σ is one-to-one and onto, μ is a cycle of the same length as τ. □

6.3 Fermat's and Euler's Theorems

RMRK 79: Recall that the *Euler ϕ-function* is the map $\phi : \mathbb{N} \to \mathbb{N}$ defined by $\phi(n) = 1$ for $n = 1$ and, for $n > 1$, $\phi(n)$ is the number of positive integers m with $1 \leq m < n$ and $\gcd(m, n) = 1$. By a proposition from Chapter 3, we know $|U(n)| = \phi(n)$. Furthermore, for any prime p, $\phi(p) = p - 1$. These facts lead to the following familiar theorems.

THM 80: Let $U(n)$ be the group of units in $\mathbb{Z}_n$. Then $|U(n)| = \phi(n)$.

THM 81: (Euler) Let a and n be integers with $n > 0$ and $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \mod n$.

THM 82: (Fermat) Let p be a prime and $p \nmid a$. Then $a^{p-1} \equiv 1 \mod p$, and for any $b \in \mathbb{Z}$, $b^p \equiv b \mod p$.

Math 305 Notes

Notes

Dr. Mike Janssen