MATH 100A Complete Lecture Notes

Brian Chao

Fall 2019

Lecture 9/26/2019 (Week 0 Thursday):

Group theory is about the symmetries of objects. Given an object X, we are looking for a function $X \to X$ that is a bijection and preserves properties of X. Thus, the "symmetries" of X is informally

$$Symm(X) = \{f : X \to X | f \text{ bijection}\}.$$

For example, given a straight-line segment graph $1 - 2 - 3 - 4$, its symmetries are $\{\text{id, flipping}\}$. We can flip it so that it becomes $4 - 3 - 2 - 1$.

We observe that:
(1) $\text{Id}_X \in Symm(X)$.
(2) If $f, g \in Symm(X)$, then $f \circ g \in Symm(X)$.
(3) If $f \in Symm(X)$, then $f^{-1} \in Symm(X)$.

Definition:

We say that $(G, \cdot)$ is a group if the binary operation $\cdot : G \times G \to G$ satisfies :
(a) $\exists e \in G$, such that $\forall g \in G$, $g \cdot e = e \cdot g = g$. (This is the *neutral* element, or the identity element.)
(b) (associtivity of group operation) $\forall g_1, g_2, g_3 \in G$, we have $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.
(c) $\forall g \in G$, $\exists g' \in G$ such that $g \cdot g' = g' \cdot g = e$.

Remark: The professor says that we will do a bunch of things focused on a central purpose rather than just going topic by topic.

Example:

Let $X = \{1, 2, ..., n\}$. Then,

$$Symm(X) = \{f : X \to X | f \text{ is a bijection}\}.$$

It is denoted by S_n, and it is called the *symmetric group*. S_n is a group under composition. It is easy to verify the group properties. The cardinality of S_n is $n!$.

For example, for the set $\{1, 2, 3\}$. We can map 1 to 3. What do we map 2 to? Well, we have only 2 choices now. Continuing this logic, we deduce that $|S_3| = 3!$.

Example:

Consider $(\mathbb{Z}, +)$. This a group with identity element 0. The "inverse" of x is $-x$.

Example:

Is $(\mathbb{Z}, \cdot)$ a group? Well, no, because 0 has no inverse element. Another reason is that $2x = 1$ has no solutions in $\mathbb{Z}$.

Example:

Consider $(\mathbb{Q}, \cdot)$. This isn't a group because 0 has no inverse element. However, $(\mathbb{Q}\backslash\{0\}, \cdot)$ is a group.

Example:

$GL_n(\mathbb{R}) = \{a \in M_n(\mathbb{R}) | \det(a) \neq 0\}$, the set of invertible $n \times n$ matrices with real entries, is a group under matrix multiplication.

Recall: (Well-Ordering Principle) Any nonempty subset of nonnegative integers $A \subset \mathbb{Z}^+$ has a minimal element.

Theorem (Division Algorithm):

For every $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, $\exists!(q, r) \in \mathbb{Z} \times \mathbb{Z}$, such that:

$$a = bq + r$$

with $0 \leq r < b$. This just means that we divide a by b.

Proof. We have to prove both uniqueness and existence. First let

$$A := \{a - bk | k \in \mathbb{Z}, a - bk \geq 0\} = (a + b\mathbb{Z}) \cup \mathbb{Z}^{\geq 0}.$$

The intuition here is we are dividing a by subtracting k copies of b from it. The reason for the minus sign in front of bk is just to make it easier to imagine.

If $a \geq 0$, then $a = a - b \cdot 0 \in A$. Now suppose $a < 0$. Then let $k = -a$. This gives us $a + b(-a) = a(1 - b)$. The sign of a is negative, and, since b is a positive integer, $(1 - b) \leq 0$. Thus $a(1 - b) \geq 0$, and we conclude $a(1 - b) \in A$. So, in either case we know A is nonempty. By the well-ordering principle, let r be the minimal element of A. In particular, $r \in A$. Thus $r \geq 0$, and we get:

$$a - bq = r$$

for some $q \in \mathbb{Z}$. We now show that $r < b$. Suppose to the contrary that $r \geq b$. Then $r - b \geq 0$ and $r - b = a - bq - b = a - b(q + 1)$. This means $r - b \in A$ and $r - b < r$, which contradicts the minimality of r. This finishes the existence proof.

Now we show that (q, r) is unique. Suppose that (q_1, r_1) and (q_2, r_2) both satisfy $a = bq_i + r_i$. We want to show that the two pairs are equal. We know that $bq_1 + r_1 = bq_2 + r_2 \implies b(q_1 - q_2) = r_2 - r_1$. Without loss of generality, assume $q_1 \geq q_2$. Then $r_2 - r_1 \geq 0$, furthermore $0 \leq r_2 - r_1 \leq r_2 < b$. Since $r_2 - r_1$ is a multiple of b, it is only possible that $r_2 - r_1 = 0$, and thus $q_1 = q_2$. ∎

Definition:

We say that $a|b$, or a *divides* b, if $\exists k \in \mathbb{Z}$, such that $b = ak$.

Proposition:

If $a|b$ and $b|c$, then $a|c$.

Proposition:

If $a|b_1$ and $a|b_2$, then $a|b_1 \pm b_2$.

Proposition:

If $a|b$, then $a|bk$, where k can be any integer.

Proposition:

If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

Definition:

A *subgroup* of a group $(G, \cdot)$ is a subset $H \subset G$ such that $(H, \cdot)$ is a group. We denote this with $H \leq G$.

Example:

$(\mathbb{Z}^+, +)$ is not a subgroup of $(\mathbb{Z}, +)$ because positive integers do not have additive inverses in the positive integers.

Example:

Consider $k\mathbb{Z} = \{ka | a \in \mathbb{Z}\}$. Then $(k\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

Theorem:

A subgroup of $\mathbb{Z}$ is of the form $a\mathbb{Z}$ for $a \in \mathbb{Z}$.

Proof. Let H be a subgroup of $\mathbb{Z}$. If $H = \{0\}$, then we are done. Indeed, $0\mathbb{Z} = \{0\}$. Now suppose that H has a nonzero element $h \in H$. We claim that H has a positive element. Indeed, exactly one of $h, -h \in H$ is positive. Thus $H \cap \mathbb{Z}^+ \neq \emptyset$.

By the well-ordering principle, $H \cap \mathbb{Z}^+$ has a minimal element, say $a \in H \cap \mathbb{Z}^+$. We claim that $H = a\mathbb{Z}$.

We have to show that $a\mathbb{Z} \subset H$ and $H \subset a\mathbb{Z}$.

Subclaim 1: For all $k \in \mathbb{Z}^+$, $ak \in H$. We will prove by induction. The base case is $a \cdot 1 \in H$. Assume that $a \cdot k \in H$. Then $a \cdot (k+1) = ak + a \in H$, since we assume that $ak, a \in H$. Thus, $ak \in H$ for $k \in \mathbb{Z}^+$, and moreover $-ak = a(-k) \in H$. We conclude $a\mathbb{Z} \subset H$.

Now suppose $h \in H$. By the division algorithm, $\exists!(q, r)$ integers such that $h = aq + r$, with $0 \leq r < a$. We want to show $r = 0$. We have $r = h - aq$. Since $aq \in H$, we know $-aq \in H$, and finally $h - aq = h + (-aq) \in H$. Since $r \in H$ and $r < a$ and $a = \min(H \cap \mathbb{Z}^+)$, we must have $r \leq 0$, else the existence of a $r > 0$ would contradict the minimality of a. Yet $0 \leq r$. Thus $r = 0 \implies h = aq \in a\mathbb{Z}$, establishing $H \subset a\mathbb{Z}$. ■

Recall: The greatest common divisor of a, b is denoted $\gcd(a, b)$. * We cannot define $\gcd(0, 0)$, since gcd only outputs positive integers.

Proposition:

$\gcd(a, b) \leq \min\{|a|, |b|\}$ if either $a \neq 0$ or $b \neq 0$.

Lecture 10/1/2019 (Week 1 Tuesday):

Definition:

Consider $a, b \in \mathbb{Z}$, where at least one is nonzero, say $b \neq 0$. The *greatest common divisor* of a, b is a number $\gcd(a, b) > 0$ such that:
(1) $\gcd(a, b)|a$ and $\gcd(a, b)|b$;
(2) $\gcd(a, b)$ is the biggest number with property (1).

Notation: Define:

$$a\mathbb{Z} + b\mathbb{Z} = \{ax + by | x, y \in \mathbb{Z}\} \subset \mathbb{Z}.$$

Claim:

$a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Proof. It suffices to prove that if $\alpha, \beta \in X := a\mathbb{Z} + b\mathbb{Z}$, then then $\alpha + \beta \in X$ and $-\alpha \in X$ and $0 \in X$. This is because once we have shown that these hold, then it is clear that we have closure under addition, as well as the identity and inverse elements. Also integer addition is always associative, so we don't need to worry about that.

First, $0 \in X$, because setting $x = y = 0$, $ax + by = 0 \in X$. Second, if $\alpha = ax + by$, then $-\alpha = a(-x) + b(-y) \in X$. Third, if $\alpha = ax_1 + by_1$ and $\beta = ax_2 + by_2$. Then, $\alpha + \beta = a(x_1 + x_2) + b(y_1 + y_2) \in X$. ∎

Recall: All subgroups $X \subset \mathbb{Z}$ are of one of the following forms: $X = \{0\}$ or $X = b\mathbb{Z}$, where b is the smallest positive element in X.

For $a\mathbb{Z}+b\mathbb{Z}$, we can choose $x = 0$ and $y = 1$ in $ax+by$ to show that $b\mathbb{Z} \subset a\mathbb{Z}+b\mathbb{Z}$, and thus, $a\mathbb{Z} + b\mathbb{Z} \neq \{0\}$, since $b\mathbb{Z}$ contains a smallest positive element b.

Conclusion: $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ for $d > 0$.

Theorem:

d is the greatest common divisor of a, b. In particular, $d \in d\mathbb{Z}$, thus, $d = ax + by$ for some $x, y \in \mathbb{Z}$.

Proof. We know that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ for some $d > 0$, but we can't say that

$d = \gcd(a, b)$ yet. By setting $x = 1$ and $y = 0$ in $ax + by$, we have $a \in a\mathbb{Z} + b\mathbb{Z}$. Hence $a \in d\mathbb{Z}$ too, so $d|a$. Similarly, setting $x = 0$ and $y = 1$, we get that $b \in a\mathbb{Z} + b\mathbb{Z}$, so that $b \in d\mathbb{Z}$, and $d|b$. Thus d divides both a and b.

It remains to show that d is the greatest divisor. Notice that $d = ax + by$ for some $x, y \in \mathbb{Z}$. Let d' be a common divisor of a, b, so that $d'|a$ and $d'|b$, so that $d'|(ax + by)$. In particular, $d'|d$ as well, which implies $d' \leq d$. Thus this finishes the proof. ■

Example:

Since $\gcd(2, 5) = 1$, we have $2\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$, so any integer may be written as a sum of a multiple of 2 and a multiple of 5.

Corollary:

If $c|a$ and $c|b$, then $c| \gcd(a, b)$.

Proof. Essentially the last proof, but with d' replaced with c. ■

Corollary:

$\gcd(a, b) = 1$ if and only if $1 = ax + by$ for some $x, y \in \mathbb{Z}$. In this case, a, b are said to be *coprime*.

Proof. The forward direction of the proof is given by the theorem we just proved. Now suppose that $1 = ax + by$ for some $x, y \in \mathbb{Z}$. Write $d = \gcd(a, b)$. This means that $d|a$ and $d|b$, so it must divide $ax + by = 1$. So, $d|1$, so $d = \pm 1$. But we have defined the gcd to be a positive number, so $d = 1$. ■

Corollary:

If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$. $\star$

For example, $6|2 \cdot 3$, but $\gcd(6, 2) \neq 1$, so won't work.

Proof. Write $1 = ax+by$. Multiplying the equation by c, we have $c = acx+bcy = a(cx)+(bc)y$, which is a sum of multple of a's. Thus $a|c$. ■

Prime Numbers

Definition:

p is prime if $p > 1$ and its only divisors are $\pm 1, \pm p$. In other words $d|p \implies d = \pm 1, \pm p$.

Lemma:

Let p be a prime and $n \in \mathbb{Z}$. Then either:
(1) $p|n$ or (2) $\gcd(p, n) = 1$. $\star\star$

Proof. Let $d = \gcd(p, n)$. Then $d|p$, but since $d > 0$, we know that $d = 1$ or $d = p$. If $d = 1$, then the second situation occurs, then we are done. Else if $d = p$, then $d|n$, which implies that $p|n$. ■

Lemma:

If p is a prime and $p|ab$, then either $p|a$ or $p|b$.

Proof. If $\gcd(p, a) = 1$ and $p|ab$, then a previous corollary ($\star$) guarantees that $p|b$. Else, by lemma ($\star\star$), if $\gcd(p, a) \neq 1$, then $p|a$. ■

Corollary:

If p is a prime and $p|a_1 \cdots a_n$ then at least $p|a_i$ for some $i \in \{1, ..., n\}$.

Proof. By induction on n. ■

Example:

How can we list all prime numbers ≤ 40?

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \\ 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \end{pmatrix}$$

The key technique here is that if n is not prime, then $n = ab$. If $a, b > \sqrt{n}$, then $ab > \sqrt{n}\sqrt{n} = n$. So a number that is not prime should have at least one divisor $\leq \sqrt{n}$. So we do this: circle 2 as a prime number, and then cross out all other even numbers on the board. Then circle 3, and then cross out out numbers that are multiples of 3 on the board. Then circle 5 and continue doing the same thing. We only need to do this for up to $n = 6 < \sqrt{40}$, and all the numbers that remain on the board will be primes.

Fundamental Theorem of Arithmetic (FTA):

Any integer $n > 1$ can be factored uniquely into product of primes:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

provided that the primes are ordered: $p_1 < p_2 < \cdots < p_k$.

Proof. We first prove existence. Assume for contradiction that FTA fails to hold. Let X denote the set of integers $n > 1$ that cannot be factored into primes. X cannot be empty else there is nothing to contradict. X has a smallest element n by the well-ordering principle. If $n \in X$ is prime, then n is a prime factorization of itself, so $n \notin X$, contradiction.

Otherwise if n is composite, then $n = ab$ for $1 < a, b < n$. By minimality of n, we have $a, b \notin X$. This means that both a, b can be factored into primes, so their product $ab = n$ can also be factored into a product of primes. Contradiction.

Now we prove uniqueness. Let X denote the set of integers $n > 1$ which can be factored in two ways. Let n be the minimal element of X. Let $n = p_1^{a_1} \cdots p_k^{a_k} = q_1^{b_1} \cdots q_l^{b_l}$ be two prime factorizations of n. We know:

$$p_1 | n \implies p_1 | q_1^{b_1} \cdots q_l^{b_l}$$

By Euclid's lemma, $p_1 | q_i$ for some q_i. Since q_i is prime, $p_1 = q_i$ for some i.

Similarly, with parallel logic, $q_1 = p_j$ for some j. Continuing this logic, all the p_i on the LHS are some q_j on the RHS, and vice versa. In particular $p_1 = q_1$, because the smallest prime number for each factorization must be the same. Then:

$$\frac{n}{p_1} = \frac{n}{q_1} = p_1^{a_1 - 1} \cdots p_k^{a_k} = q_1^{b_1 - 1} \cdots q_l^{b_l}.$$

But $n/p_1 < n$, contradicting that n is the smallest element of X with two different factorizations. ■

Lecture 10/3/2019 (Week 1 Thursday):

Fundamental Theorem of Arithmetic: Any $n \in \mathbb{Z}^{\geq 2}$ can be written as a product of primes in a unique way.

Theorem (Euclid):

There are infinitely many primes.

Proof. By contradiction. Suppose that $2 = p_1 < p_2 < ... < p_n$ are the only primes. Consider the number $N := p_1 p_2 \cdots p_n + 1$. Since $N > 1$, N has a prime factor p. Since the remainder of N divided by any p_i is 1, we must have $p_i \neq p$ for all $1 \leq i \leq n$. So p is a new prime that is not any of the p_i. Contradiction. ■

Example:

(Not on test) Consider a function $\mu(n) = 0$ if $p^2 | n$ for some p prime, $\mu(n) = 1$ if $n = 1$, else $\mu(n) = (-1)^m$ if $n = p_1 \cdots p_m$ where $p_i \neq p_j$. If you can show that:

$$\frac{\mu(1) + ... + \mu(M)}{\sqrt{M}}$$

is bounded, then you get a million dollars. This is equivalent to the Riemann Hypothesis.

Definition:

For all $n \in \mathbb{Z}^{+}$, $n = 2^{\square} 3^{\square} 5^{\square} \cdots p^{\square} \cdots$, where each box can contain a number that could be 0. We write:

$$n = 2^{v_2(n)} 3^{v_3(n)} \cdots p^{v_p(n)}.$$

$v_p : \mathbb{Z}^{+} \to \mathbb{Z}^{\geq 0}$ is called the *p-valuation* of n.

Example:

What is $v_p(mn)$? First, write

$$m = \prod_{p \text{ prime}} p^{v_p(m)}$$

For example, if $m = 10$, then $v_2(10) = 1$, $v_3(10) = 0$, $v_5(10) = 1$, and $v_p(10) = 0$ for all $p > 5$. Going back to the question,

$$mn = \left(\prod_{p\in\mathcal{P}} p^{v_p(m)}\right)\left(\prod_{p\in\mathcal{P}} p^{v_p(n)}\right) = \prod_{p\in\mathcal{P}} p^{v_p(m)+v_p(n)}.$$

Thus, $\boxed{v_p(mn) = v_p(m) + v_p(n)}$. In particular, if $d|n$ and $n \in \mathbb{Z}^+$, then $v_p(d) \leq v_p(n)$. To be more specific, if $d|n$, then $n = dk$ for some $k \in \mathbb{Z}^+$. Hence $v_p(n) = v_p(dk) = v_p(d) + v_p(k) \geq v_p(d)$.

Lemma:

$d|n$ if and only if $\forall p \in \mathcal{P}$, $v_p(d) \leq v_p(n)$.

Proof. We have already proven the forward direction. Now for the other direction, consider, $k = \prod_{p\in\mathcal{P}} p^{v_p(n)-v_p(d)} \in \mathbb{Z}^+$. (Since k cannot be infinite, $v_p(n)$ has to be eventually zero for some p. This forces $v_p(d) = 0$ eventually as well.)

Then

$$d \cdot k = \prod_{p\in\mathcal{P}} p^{v_p(d)} \prod_{p\in\mathcal{P}} p^{v_p(n)-v_p(d)}$$

$$\prod_{p\in\mathcal{P}} p^{v_p(n)} = n.$$

This shows that $d|n$ as desired. ■

Lemma:

Let $d(n) :=$ number positive divisors of n. Then,

$$d(n) = \prod_{p\in\mathcal{P}} (v_p(n) + 1).$$

This product exists, since $v_p(n)$ is eventually zero as p increases.

Proof: We know that $d|n$ if and only if for all $p \in \mathcal{P}$, $v_p(d) \leq v_p(n)$. Hence, $v_p(d) \in \{0, 1, 2, ..., v_p(n)\}$. So for any prime $p \in \mathcal{P}$, there are exactly $v_p(n) + 1$ possibilities for $v_p(d)$, and they can be chosen independently for each $p \in \mathcal{P}$. Therefore there are

$$\prod_{p \in \mathcal{P}} (v_p(n) + 1)$$

choices for d. ■

Remark: We have:

$$v_p(k^2) = v_p(k \cdot k) = v_p(k) + v_p(k) = 2v_p(k).$$

Lemma: By the remark above, $v_p(k^2)$ is even for any $p \in \mathcal{P}$.

Example:

$\sqrt{2}$ is irrational. Indeed, suppose to the contrary that $\sqrt{2}$ is rational. Then write $\sqrt{2} = m/n$ for $m, n > 0$. Then, $2 = m^2/n^2$, and $2n^2 = m^2$. Taking 2-valuations of both sides,

$$v_2(2n^2) = v_2(m^2)$$

$$\implies v_2(2) + 2v_2(n) = 2v_2(m)$$

$$\implies 1 = 2v_2(m) - 2v_2(n)$$

but the RHS is even. Contradiction. ■

Proposition:

$n \in \mathbb{Z}^+$ is a perfect square $\iff$ $d(n)$ is odd.

Proof. Left as HW. Recall that $d(n) = \prod_{p \in \mathcal{P}} (v_p(n) + 1)$. Do some even/odd analysis.

Definition:

We say $a \equiv b \pmod{n}$, or a is *congruent to b modulo n* if $n|(a - b)$.

Example:

If $n = 5$, then $0 \equiv 5$, $1 \equiv 6$, ... modulo 5. Intuitively, this just means that we only care about the point we are at on a pentagon instead of what label we give to our location.

Remark: We have:
(1) $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$.
(2) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$.
(3) $a \equiv a \pmod{n}$.

Thus congruence modulo n is an equivalence relation on integers. Let's actually verify (2). Suppose that $a \equiv b$ and $b \equiv c$ modulo n. This means that $n|(a-b)$ and $n|(b-c)$. Hence $n|(a+b)+(b-c)$, which was what was needed to show that $n|(a-c)$.

Proposition:

$a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$ implies:
(1) $a_1 + b_1 \overset{n}{\equiv} a_2 + b_2$
(2) $a_1 b_1 \overset{n}{\equiv} a_2 b_2$

All this means is that when carrying out addition and multiplication, you get to replace a (bigger) number with another (smaller) number that is the same as the original (bigger) number mod n.

Proof. For the first one, we have $n|(a_1-a_2)+(b_1-b_2)$, so $n|(a_1+b_1)-(a_2+b_2)$. For the second claim, we know that $n|(a_1-a_2)$ and $n|(b_1-b_2)$. We have:

$$n|(a_1b_1 - a_2b_2)$$

$$\iff n|(a_1b_1 - a_2b_1 + a_2b_1 - a_2b_2)$$

$$\iff n|b_1(a_1 - a_2) + a_2(b_1 - b_2)$$

$$\impliedby n|(a_1 - a_2) \text{ and } n|(b_1 - b_2)$$

as desired. ■

Example:

What is the remainder when 20192018 is divided by 9?

Solution. We have

$$20192018 = 8+1\times10+0\times10^2+2\times10^3+9\times10^4+1\times10^5+0\times10^6+2\times10^7.$$

What is this modulo 9? We know that $10 \overset{9}{\equiv} 1$, hence $10^n \overset{9}{\equiv} 1^n = 1$. Hence, our number is equivalent to $8+1+0+2+9+1+0+2 \overset{9}{\equiv} 5$. Thus $9|(n-5)$. If r is the remainder, then $9|(n-r)$. This means that $9|(5-n)+(n-r)$, so that $9|5-r$. Also, since $0 < r \leq 8$, we deduce that $-3 \leq 5-r < 5$. The fact that $9|(5-r)$ and $-3 \leq 5-r < 5$ together imply that $5-r = 0$, and thus $r = 5$.

Lecture 10/8/2019 (Week 2 Thursday):

Recall: $a \equiv b \pmod{n}$ is an equivalence relation. Furthermore, if $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ and $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

Example:

Find the remainder when $n = 140100109200$ is divided by 9.

Solution. Because $10 \equiv 1 \pmod{9}$, $10^k \equiv 1 \pmod{9}$. Thus, we conclude that

$$n \equiv 1 + 4 + 1 + 1 + 9 + 2 \pmod{9}$$
$$\equiv 0 \pmod{9}.$$

Example:

Find the remainder of n divided by 11, where n is as above.

Solution. What is $10 \pmod{11}$? It equals -1. Hence $10^k \equiv (-1)^k \pmod{11}$. Hence

$$n = 140100109200 \pmod{11}$$

$$\equiv -1 + 4 - 0 + 1 - 0 + 0 - 1 + 0 - 9 + 2 - 0 + 0 \pmod{11}$$
$$\equiv -4 \pmod{11}.$$

Notice that if r is the remainder of n divided by 11, then $11 | n - r$, equivalently $n \equiv r \pmod{11}$. We have also shown $n \equiv 7 \pmod{11}$. Combining the two facts, $r \equiv 7 \pmod{11}$, which means that $11 | r - 7$. Since $-7 \leq r - 7 < 4$, we conclude that $r - 7 = 0$, so $r = 7$. (Review this logic!)

Lemma:

r is the remainder of a divided by n if and only if $0 \leq r < n$ and $a \equiv r \pmod{n}$.

Proof. ($\implies$) If r is the remainder and q is the quotient of a divided by n, then we know that

$$a = nq + r, \ 0 \leq r < n.$$

This tells us that $a - r = nq \implies n|a - r \implies a \equiv r \pmod{n}$.

($\Longleftarrow$) Suppose that r' is the remainder of a divided by n. So by ($\implies$) we know that $a \equiv r' \pmod{n}$. By assumption we have that $a \equiv r \pmod{n}$. Thus by properties of modulo n as an equivalence relation, $r \equiv r' \pmod{n}$. Hence $r \equiv r' \pmod{n}$. Hence $n|r - r'$. We have:

$$-n < -r' \leq r - r' \leq r < n.$$

Hence, $r - r'$ is a multiple of n that is between $-n$ and n. We conclude that $r - r' = 0$, so $r = r'$ is the remainder. ■

Remark: The general setting of an equivalence relation is as follows. Let X be a non-empty set. We have a "relation" $x_1 \sim x_2$ for some pairs $(x_1, x_2) \in X^2$. We say that $\sim$ is an equivalance relation if:

(1) $a \sim a$;
(2) $a \sim b \implies b \sim a$;
(3) $a \sim b$ and $b \sim c \implies a \sim c$.

Fact:

Let $[a] := \{x \in X | a \sim x\}$. This is a subset of X, called an *equivalence class*.

Lemma:

$x \sim a$ if, and only if $[x] = [a]$.

Proof. ($\implies$) We need to show that $[x] \subset [a]$ and $[a] \subset [x]$. Suppose $y \in [x]$; then $x \sim y$. By assumption, $x \sim a \implies a \sim x$. Hence $a \sim y$, and $y \in [a]$. This shows that $[x] \subset [a]$. By symmetry, $[a] \subset [x]$, and the claim follows.

($\Longleftarrow$) Suppose now $[x] = [a]$. Notice that $x \sim x$, thus $x \in [x] = [a]$ by assumption. This implies that $a \sim x$, and thus $x \sim a$. ■

Theorem:

Suppose $\sim$ is an equivalence relation on X (has to be nonempty), and $[a]$ is the equivalence class of a. Then $\{[a]|a \in X\}$ is a partition of X; that means

(1) $\bigcup_{a\in X}[a] = X$.
(2) $[a] \cap [a'] \neq \emptyset \implies [a] = [a']$.

Proof. $\forall x \in X, x \sim x$. This implies that $x \in [x]$, which further implies that $x \in \bigcup_{a\in X}[a]$. Now for the second part, suppose that $x \in [a] \cap [a']$. This means $a \sim x$ and $a' \sim x$, implying that $[a] = [x]$ and $[a'] = [x]$. Hence, $[a] = [x] = [a']$. ■

Example:

Let $[a]_n$ be the equivalence class of a with respect to $a \equiv b \pmod n$. For example, $[0]_2 = 2\mathbb{Z}$. Another example: what is $[1]_3$ (the residue class of modulo n)? This is just $3\mathbb{Z} + 1$.

Remark: Intuitively, $[a]_n$ just means: all the numbers equal to a when $\pmod n$.

Proposition:

⋆ $[a]_n = [b]_n \iff a \equiv b \pmod n$. Thus, $[1]_5 = [6]_5$, for example.

Remark: $\mathbb{Z}_n = \{[a]_n|a \in \mathbb{Z}\}$ is a partition of $\mathbb{Z}$. Notice that if r is the remainder of a divided by n, then $[a]_n = [r]_n$. So, $\mathbb{Z}_n = \{[0]_n, [1]_n, ..., [n-1]_n\}$. Notice that $[i]_n \neq [j]_n$ if $0 \leq i \neq j < n$, so $|\mathbb{Z}_n| = n$. (Important)

Remark (continued): Let $[a]_n + [b]_n := [a+b]_n$, and $[a]_n \cdot [b]_n := [ab]_n$. We must show that these operations are independent from the choice of a, b. That is, we have to show that these operations are well-defined. That is, if $[a_1]_n = [a_2]_n$ and $[b_1]_n = [b_2]_n$, then we have to show $[a_1+b_1]_n = [a_2+b_2]_n$ and $[a_1b_1]_n = [a_2b_2]_n$.
We know that:

$$[a_1]_n = [a_2]_n, \;\; [b_1]_n = [b_2]_n$$

$$\iff a_1 \equiv a_2 \pmod n, \;\; b_1 \equiv b_2 \pmod n$$

$$\implies a_1 + b_1 \equiv a_2 + b_2 \pmod n, \;\; a_1b_1 \equiv a_2b_2 \pmod n$$

$$\implies [a_1+b_1]_n = [a_2+b_2]_n, \ \ [a_1b_1]_n = [a_2b_2]_n.$$

Example:

Let us draw a multiplication table with $\mathbb{Z}_6$:

*	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

All of the $[\cdot]$ should implicitly have a "6" subscript, but I didn't include that.

Remark: $(\mathbb{Z}_n, +, \cdot)$ has: distribution, associativity for $+$, identity element for addition $[0]$, inverse element for addition $[-a]$, and $[1][a] = [a][1] = [a]$. Thus, $(\mathbb{Z}_n, +)$ is a group. The function $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(a) = [a]_n$ is a group homomorphism. That means, $f(ab) = f(a) \cdot f(b)$.

Question:

What elements of $\mathbb{Z}_n$ do have multiplicative inverse? That is, we want to find the $[a]_n$ such that for some x, $[x]_n$ is such that $[a]_n[x]_n = [1]_n$.

This is the case if and only if $[ax]_n = [1]_n \iff ax \equiv 1 \pmod{n} \iff ax - 1 = ny$ for some $y \in \mathbb{Z} \iff ax - ny = 1$ for some x and y in $\mathbb{Z}$. The integer solutions (x, y) are possible if and only if $\gcd(a, n) = 1$. That is, a and n need to be relatively prime.

So for example, in the $\mathbb{Z}_6$ multiplication table above, only $[1]_6$ and $[5]_6$ have multiplicative inverses.

Proposition:

$[a]_n$ has a multiplicative inverse if, and only if $\gcd(a, n) = 1$.

Corollary:

All $[a]_p \in \mathbb{Z}_p \backslash \{[0]_p\}$ have a multiplicative inverse if p is prime.

Example:

Find $[7]_{11}^{-1}$.

Solution. We have $[7x]_{11} = [1]_{11} \iff 7x \equiv 1 \pmod{11} \implies 11 | 7x - 1$. This means that for some (x, y), $11y = 7x - 1 \implies 7x - 11y = 1$. We can take $x = 8, y = 5$. Hence, $[7]_{11}^{-1} = [8]_{11} = [-3]_{11}$.

Lecture 10/10/2019 (Week 2 Thursday):

Recall: $[a]_n$ has a multiplicative inverse $\iff$ $\gcd(a, n) = 1$.

Corollary:

p prime $\iff$ any non-zero element of $\mathbb{Z}_p$ has a multiplicative inverse.

Proof. ($\Longrightarrow$) We have proved this in the previous lecture.

($\Longleftarrow$) For all $1 \leq a \leq p-1$, $[a]_p$ has a multiplicative inverse $\Longrightarrow$ for all $1 \leq a \leq p-1$, $\gcd(a, p) = 1 \Longrightarrow p$ is prime. ■

Definition:

We say $[a]_n$ is *invertible* if it has a multiplicative inverse.

Let $\mathbb{Z}_n^\times$ be the set of invertible elements. Let

$$\mathbb{Z}_n^\times = \{[a]_n | 1 \leq a \leq n-1, \gcd(a, n) = 1\}.$$

Lemma:

$(\mathbb{Z}_n^\times, \cdot)$ is a group.

Proof. We have already discussed that $\cdot$ has associativity and that $[1]_n \cdot [a]_n = [a]_n \cdot [1]_n = [a]_n$. (Hence $[1]_n$ is the neutral element.) We need to check that $\mathbb{Z}_n^\times$ is closed under multiplication. That means if $[a]_n$ and $[b]_n$ are invertible, then their product $[a]_n \cdot [b]_n$ is invertible.

Since $[a]_n$ is invertible, $[a]_n[a^*]_n = [1]_n$ for some a^*. Similarly, $[b]_n[b^*]_n = [1]_n$ for some b^*. Observe that:

$$([a]_n \cdot [b]_n)([b^*]_n \cdot [a^*]_n) = [1]_n$$

This shows that $[a]_n \cdot [b]_n \in \mathbb{Z}_n^\times$. The last thing we check is that $\forall [a]_n \in \mathbb{Z}_n^\times$, there exists $[a^*]_n \in \mathbb{Z}_n^\times$ as the inverse of $[a]_n$ (i.e. inverse has to be in the group). Since $[a]_n \in \mathbb{Z}_n^\times$, we know that there is $[a^*]_n$ such that $[a]_n[a^*]_n = [1]_n$, but this means that $[a^*]_n$ is invertible, so the claim follows. ■

Example:

$[a]_n[x]_n = [1]_n$ for some x if and only if $ax \equiv 1 \pmod{n}$, if and only if $ax - 1 = ny$ for some $y \in \mathbb{Z}$. This happens if and only if there exists $x, y \in \mathbb{Z}$ such that $ax - ny = 1$.

Example:

Find $[13]_{29}^{-1}$.

Solution. $29 = 13 \times 2 + 3$, $13 = 3 \times 4 + 1$, and $3 = 1 \times 3 + 0$. Going backwards, we get that

$$\begin{aligned} 1 = 13 - 3 \times 4 &= 13 - (29 - 13 \times 2) \times 4 \\ &= (29)(-4) + (13)(1 + 8) \\ &= 29 \times (-4) + 13 \times 9. \end{aligned}$$

This implies that $[13]_{29}^{-1} = [9]_{29}$.

Definition:

Suppose $(G, \cdot)$ and $(H, \star)$ are two groups. A map $f : G \to H$ is called a *group homomorphism* if

$$f(g_1 \cdot g_2) = f(g_1) \star f(g_2).$$

Example:

Consider $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(a) = [a]_n$, both groups with the addition operation. f is a surjective group homomorphism.

Definition:

Let $f : G \to H$ be a group homomorphism. We define

$$\ker(f) = \{g \in G | f(g) = \text{neutral element of } H\}.$$

Example:

In the previous example, $a \in \ker(f) \iff [a]_n = [0]_n \iff n|a$. So $\ker(f) = n\mathbb{Z}$.

Example:

Suppose $(G, \cdot)$, $(H, \star)$ are groups. Then $(G \times H, \circ)$ is a group where

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 \cdot g_2, h_1 \star h_2).$$

It is easy to check that $G \times H$ is a group.

Example:

Consider $f : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m$, $f(a) = ([a]_n, [a]_m)$. We claim that this is a group homomorphism. We check that

$$f(a_1 + a_2) = ([a_1 + a_2]_n, [a_1 + a_2]_m)$$

$$f(a_1) + f(a_2) = ([a_1]_n, [a_1]_m) + ([a_2]_n, [a_2]_m) = ([a_1 + a_2]_n, [a_1 + a_2]_m)$$

as needed. Now notice that $a \in \ker(f) \in ([a]_n, [a]_m) = ([0]_n, [0]_m) \iff [a]_n = [0]_n$ and $[a]_m = [0]_m \iff n|a, m|a \iff \operatorname{lcm}(m, n)|a$. Hence $\ker(f) = \operatorname{lcm}(m, n)\mathbb{Z}$.

Example:

If $f : \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}_4$, $f(a) = ([a]_2, [a]_4)$, then f is not surjective as $([0]_2, [1]_4)$ cannot be in the image. (Since otherwise, we would have a both even and odd.)

Chinese Remainder Theorem:

$f : \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m$, $f(a) = ([a]_n, [a]_m)$ is surjective if $\gcd(n, m) = 1$. In other words, for all $b, c \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$, such that $x \equiv b \pmod{n}$ and $x \equiv c \pmod{m}$.

Proof. We borrow an idea from linear algebra. If a linear mapping $T : \mathbb{R} \to \mathbb{R}^2$ has both standard basis vectors in its image, then it is onto. (Of course such a linear map doesn't exist, else $\mathbb{R}^2$ would be spanned by $v = [T]$, and would have dimenision 1.) Why is $([1]_n, [0]_m)$ in the image? We are looking for $x \in \mathbb{Z}$

such that $x \equiv 1 \pmod{n}$ and $x \equiv 0 \pmod{m}$. This means that $x = my$ for some $y \in \mathbb{Z}$. Thus, we want to find y such that $my \equiv 1 \pmod{n}$. Since $\gcd(m, n) = 1$, there exists m^* such that $mm^* \equiv 1 \pmod{n}$. We then have $f(mm^*) = ([mm^*]_n, [mm^*]_m) = ([1]_n, [0]_m)$.

To make the last part a bit clearer, let me put it this way. Since $\gcd(m, n) = 1$, there exists $x', y' \in \mathbb{Z}$ such that $nx' + my' = 1$. Then $my' - 1 = -nx'$, so choosing $x = my'$ will ensure that $x \equiv 0 \pmod{m}$ and $x \equiv 1 \pmod{n}$ as we needed. So in the last paragraph we are setting $y' = m^*$.

Similarly, if $x \equiv 0 \pmod{n}$ and $x \equiv 1 \pmod{m}$, then we write $x = ny \equiv 1 \pmod{m}$. And again since $\gcd(m, n) = 1$ means that there is n^* such that $nn^* \equiv 1 \pmod{m}$. So $f(nn^*) = ([nn^*]_n, [nn^*]_m) = ([0]_n, [1]_m)$.

To clarify again, since $\gcd(m, n) = 1$, there exists $x', y' \in \mathbb{Z}$ such that $nx' + my' = 1$. Then $nx' = -my' + 1$. Hence, choosing $x = nx'$ will ensure that $x \equiv 0 \pmod{n}$ and $x \equiv 1 \pmod{m}$. So in the last paragraph we are setting $x' = n^*$.

Now given any $b, c \in \mathbb{Z}$, we have

$$f(b(mm^*) + c(nn^*))$$

$$= f(b(mm^*)) + f(c(nn^*)) \text{ (because } f \text{ is a group homomorphism)}$$

$$([bmm^*]_n, [bmm^*]_m) + ([cnn^*]_n, [cnn^*]_m)$$

$$= ([b]_n, [0]_m) + ([0]_n, [c]_m) = ([b]_n, [c]_m)$$

as desired. ■

Proposition:

If n, m are relatively prime, then an explicit solution to $x = [b]_n$, $x = [c]_m$ is given by

$$x = npc + mqb$$

where p, q are integers so that $np + mq = 1$.

Lemma:

In a group $(G, \cdot)$ any $g \in G$ has a unique inverse that we denote by g^{-1} (or by $-g$ in the additive case).

Proof. Suppose that $g \cdot g' = 1_G$ and also suppose that $g'' \cdot g = 1_G$. Notice that we are only assuming that g' is a right inverse and g'' is a left inverse. Then

$$g'' \cdot (g \cdot g') = g'' \cdot 1_G = g''$$

$$(g'' \cdot g) \cdot g' = 1_G \cdot g' = g'.$$

Hence $g' = g''$ because the two expressions we started with are equal by associativity. ∎

Wilson's Theorem:

Suppose that p is prime. Then $(p-1)! \equiv -1 \pmod{p}$.

Proof. For $(1)(2)\cdots(p-1)$, we may pair any $[a]_p$ with its inverse. This way we are left with product of numbers that are their own inverses. The only numbers remaining in the product is x such that $x^2 \equiv 1 \pmod{p}$. This happens iff $p | x^2 - 1$ iff $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$ iff $x = 1$ or $x = p-1$ as $1 \leq x \leq p-1$. This implies that $(p-1)! \equiv (1)(p-1) \pmod{p}$. ∎

Fermat's Little Theorem:

p prime $\implies a^p \equiv a \pmod{p}$.

In particular, if $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. If $[a]_p = 0$, then $a^p \equiv a \equiv 0 \pmod{p}$. So we can and will assume that $[a]_p \neq [0]_p$. For now let us introduce a trick. Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$, $f([x]_p) = [a]_p[x]_p$. Since p is prime and $[a]_p \neq [0]_p$, there exists a^* such that $[a]_p[a^*]_p = [1]_p$. Define $g([x]_p) = [a^*]_p[x]_p$. Notice that $f(g([x])) = [a]_p([a^*]_p[x]_p) = [x]_p$ by associativity. Also $g \circ f = \text{id}$ by a similar argument. Hence f is a bijection, and $f([0]_p) = [0]_p$. So $f(\mathbb{Z}_p \backslash \{[0]_p\}) = \mathbb{Z}_p \backslash \{[0]_p\}$.

Thus f is just a permutation, so we certainly have

$$f([1]_p) \cdots f([p-1]_p) = [1]_p[2]_p \cdots [p-1]_p.$$

But the above expression is also equal to

$$([a]_p[1]_p) \cdots ([a]_p[p-1]_p)$$

$$= [a]_p^{p-1}[(p-1)!]_p = [(p-1)!]_p$$

By Wilson's Theorem,

$$[a]_p^{p-1}[-1]_p = [-1]_p$$
$$\implies [a]_p^{p-1} = [1]_p$$
$$\iff a^{p-1} = 1 \pmod p$$

as desired. ■

Lecture 10/15/2019 (Week 3 Tuesday):

Recall: Fermat's little theorem says that $a^p = a \pmod p$ if p is prime.

Example:

Find the remainder of 2^{50} divided by 7.

Solution. By Fermat's little theorem, $a^{49} = (a^7)^7 \equiv a^7 \equiv a \pmod 7$, where $a = 2$. Hence

$$2^{50} = 2^{49} \cdot 2 \equiv 2 \cdot 2 \equiv 4 \pmod 7.$$

Since $0 \leq 4 \leq 6$, the remainder of 2^{50} divided by 7 is 4.

Definition:

Let $S_n := \{f : \{1, ..., n\} \to \{1, ..., n\} | f \text{ is a bijection}\}$. Think about S_n as the set of symmetries of the complete graph with n vertices (A complete graph is a graph where all the vertices are connected).

S_n is called the *symmetric group*. Indeed, f, g are bijections, then $f \circ g$ is also a bijection.

Recall: f is a bijection if and only if it has an inverse function f^{-1}. Hence, to show that the composition of bijections $f \circ g$ is also a bijection, it suffices to show that it has an inverse function. It is easy to check that $(f \circ g) \circ (g^{-1} \circ f^{-1}) = \text{id}$.

Lemma:

$(S_n, \circ)$ is a group.

Proof. We have already discussed that $\circ$ defines an operation on S_n. We have:
(1) $f \circ \text{id} = \text{id} \circ f = f$
(2) $f \circ f^{-1} = f^{-1} \circ f = \text{id}$
(3) Associativity of function composition. ∎

Example:

Consider

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

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

We then have

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ (f \circ g)(1) = 4 & (f \circ g)(2) = 2 & (f \circ g)(3) = 1 & (f \circ g)(4) = 3 \end{pmatrix}$$

We can calculate $g \circ f$ similarly, and we observe that $f \circ g \neq g \circ f$. Hence $(S_4, \circ)$ is not an Abelian group.

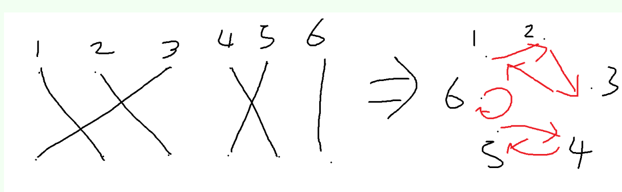
Remark: The professor drew arrow diagrams, which is probably more informative than what I drew.

Definition:

A group $(G, \cdot)$ is called *Abelian* if

$$\forall g_1, g_2 \in G, g_1 \cdot g_2 = g_2 \cdot g_1.$$

Example:



Definition:

A permutation $\sigma \in S_n$ is called a *cycle* if for some $i_1, i_2, ..., i_m$ we have

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, ..., \sigma(i_m) = i_1$$

and other values fixed. We denote this cycle by $(i_1 \ \ i_2 \cdots i_m)$. m is called the *length* of this cycle.

Remark: So the permutation in the last picture is not a cycle, because it has multiple "loops".

Remark: It is not clear if $(1, 2) \in S_2$ or S_n for some $n \geq 2$. To address this issue, we view

$$S_m \subset S_n$$

if $m \leq n$. S_m, by this kind of embedding, is a subgroup of S_n if $m \leq n$.

Example:

$(1 \ \ 2)(2 \ \ 3) = (1 \ \ 2 \ \ 3)$. You read $(2, 3)$ as "2 goes to 3, and 3 goes to 2".

Example:

$\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}2 & 1\end{pmatrix} = \mathrm{id}$.

Lemma (Linking):

$\begin{pmatrix}a_1 & a_2 \cdots a_n\end{pmatrix}\begin{pmatrix}a_n & a_{n+1} \cdots a_{n+m}\end{pmatrix}$ where $a_i \neq a_j$ if $i \neq j$, is equal to

$$\begin{pmatrix}a_1 & a_2 \cdots a_{n+m}\end{pmatrix}$$

Proof. Without loss of generality compute

$$\begin{pmatrix}1 & 2 \cdots n\end{pmatrix}\begin{pmatrix}n \cdots n+m\end{pmatrix}$$

$$= \begin{pmatrix}1 & 2 \cdots n-1 & n & n+1 \cdots n+m\end{pmatrix}$$

by just thinking about what is going on. ■

Example:

$\begin{pmatrix}1 & 2 & 3\end{pmatrix}^2 = \begin{pmatrix}3 & 2 & 1\end{pmatrix} = \begin{pmatrix}1 & 3 & 2\end{pmatrix}.$

Proposition:

$\sigma^m = \text{id}$ if σ is a cycle of length m. Subsequently, $\sigma^{mk} = \text{id}$. In this case, $\sigma^{m-1} = \sigma^{-1}$.

Remark: The only cycle of length 1 is the identity. We could write $(1), (2), (3)$ etc.

Definition:

For $\sigma \in S_n$, let $M_\sigma := \{i \in [1 \cdots n] | \sigma(i) \neq i\}$. We say that σ, τ are disjoint if $M_\sigma \cap M_\tau = \emptyset$. That is for every i, either $\sigma(i) \neq i$ or $\tau(i) \neq i$, but not both.

Lemma:

$\sigma(M_\sigma) = M_\sigma$. That is, if $i \in M_\sigma \implies \sigma(i) \in M_\sigma$. Also, $\forall j \in M_\sigma,\ \exists i \in M_\sigma$, such that $\sigma(i) = j$.

Proof. Suppose to the contrary that we have $i \in M_\sigma$ yet $\sigma(i) \notin M_\sigma$. Since $i \in M_\sigma$, $\sigma(i) \neq i$. On the other hand, since $\sigma(i) \notin M_\sigma$, $\sigma(\sigma(i)) = \sigma(i)$. Since σ is an injection, $\sigma(i) = i$, which is a contradiction. This implies that $\sigma(M_\sigma) \subset M_\sigma$. Since σ is a bijection, $|\sigma(M_\sigma)| = |M_\sigma|$. Hence $\sigma(M_\sigma) = M_\sigma$. ■
(Here we have used the fact that for two finite sets A, B, if $A \subset B$ and $|A| = |B|$, then $A = B$.)

Lemma:

If σ and τ are two disjoint permutations, then $\sigma\tau = \tau\sigma$.

Proof. We want to show that for any i we have

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

Case 1: if $i \notin M_\sigma \cup M_\tau$, then both τ and σ fixes i, so there is nothing to prove.
Case 2: if $i \in M_\sigma$, then $\sigma(i) \in M_\sigma$ by the lemma. Then,

$$i \in M_\sigma \implies i \notin M_\tau \implies \tau(i) = i$$

$$\sigma(i) \in M_\sigma \implies \sigma(i) \notin M_\tau \implies \tau(\sigma(i)) = \sigma(i)$$

Hence

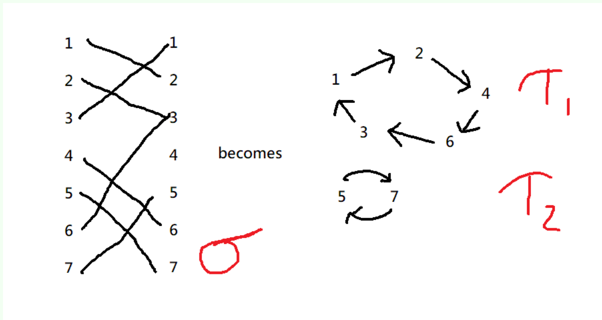
$$\sigma(\tau(i)) = \sigma(i)$$

$$\tau(\sigma(i)) = \sigma(i)$$

so $\tau(\sigma(i)) = \sigma(\tau(i))$. Case 3 is similar to case 2. ■

Lecture 10/17/2019 (Week 3 Thursday):

Example:



(Yes, I know that 2 is supposed to be connected to 4, I made a mistake.) The point of this picture is that $\sigma = \tau_1\tau_2$, so σ can be written as a composition of disjoint cycles.

Theorem:

Any $\sigma \in S_n \backslash \{\mathrm{id}\}$ can be written as a product of disjoint cycles. And such a product is unique up to reordering.

Proof. (Existence) We proceed by induction. If $\sigma(n) = n$ (i.e. the last number is fixed), then $\sigma \in S_{n-1}$ (if we view $S_{n-1} \leq S_n$). So by the induction hypothesis, σ can be written as a product of disjoint cycles.

Suppose $\sigma(n) = m \neq n$. Let $\tau = (m\ \ n)$. Then $(\tau\sigma)(n) = \tau(\sigma(n)) = \tau(m) = n$. Hence, $\tau\sigma \in S_{n-1}$. So by the induction hypothesis, $\tau\sigma$ can be written as a product of disjoint cycles, say $\tau\sigma = \gamma$. Multiplying both sides by τ, $\sigma = \tau\gamma$. We have to make sure that $\tau = (m\ \ n)$ and γ are disjoint.

Claim: n does not appear in (the, we don't have uniqueness yet) cycle decomposition of γ. Indeed, if we write $\gamma = \tau_1\tau_2\cdots\tau_k$, then observe that

$$M_{\tau_1\tau_2\cdots\tau_k} = \bigcup_{i=1}^{k} M_{\tau_i}$$

and since $\gamma(n) = n$, $n \notin M_{\tau_1\cdots\tau_k}$. Hence, $n \notin M_{\tau_i}$ for all i. Next, we consider two cases for m.

First, suppose $\gamma = \tau_1 \cdots \tau_k$ where τ_i are disjoint cycles. If $m \notin \bigcup_{i=1}^{k} M_{\tau_i}$, then $(m\ \ n)$ and τ_i are disjoint. Then we are done, since

$$\sigma = (m\ \ n)\tau_1 \cdots \tau_k$$

is written as a product of disjoint cycles.

Second, suppose that $m \in \bigcup_{i=1}^{k} M_{\tau_i}$, then since the τ_i are disjoint, we have m in exactly one M_{τ_i}. And since τ_i commute, we can assume WLOG $m \in M_{\tau_1}$. Then

$$\tau_1 = \begin{pmatrix} m & a_1 \cdots a_l \end{pmatrix}.$$

So

$$\begin{aligned} \sigma &= \begin{pmatrix} n & m \end{pmatrix} \tau_1 \cdots \tau_k \\ &= \begin{pmatrix} n & m \end{pmatrix} \begin{pmatrix} m & a_1 \cdots a_l \end{pmatrix} \tau_2 \cdots \tau_k \\ &= \begin{pmatrix} n & m & a_1 \cdots a_k \end{pmatrix} \tau_2 \cdots \tau_k \end{aligned}$$

as desired.

(Uniqueness) Suppose now that

$$\tau_1 \cdots \tau_k = \sigma_1 \cdots \sigma_l$$

where τ_i are disjoint cycles and σ_i are also disjoint cycles. For all $i \in M_\alpha = M_{\tau_1 \cdots \tau_k} = M_{\sigma_1 \cdots \sigma_l} = \bigcup M_{\tau_j} = \bigcup M_{\sigma_j}$. Because the cycles are disjoint, we must have i moved by exactly one M_{τ_j} and exactly one M_{σ_j}. Hence, after reordering, we can assume that $i \in M_{\tau_k}$. Similarly, we can assume that $i \in M_{\sigma_l}$. Write

$$\tau_k = \begin{pmatrix} i & a_1 \cdots a_r \end{pmatrix}$$

$$\sigma_l = \begin{pmatrix} i & b_1 \cdots b_s \end{pmatrix}.$$

Then $\alpha(i) = \tau_1 \cdots \tau_k(i) = \tau_k(i) = a_1$ because τ_i are disjoint. Repeating this argument, we get that $\alpha^t(i) = \tau_k^t(i)$. By a similar argument, we have that

$$\alpha^t(i) = \sigma_l^t(i).$$

This implies that $\tau_k = \sigma_l$, so we can "cancel" out both of those in the two decompositions to get

$$\tau_1 \cdots \tau_{k-1} = \sigma_1 \cdots \sigma_{l-1}.$$

By the induction hypothesis we get uniqueness. ■

Remark: A key idea is that if two permutations both change the same value, then the two permutations can be combined into one permutation. Also this proof won't be on the test.

Recall: $M_\tau = \{i \in [1, ..., n] | \tau(i) \neq i\}$. If $M_{\tau_1} \cap M_{\tau_2} = \emptyset$, then $\tau_1\tau_2 = \tau_2\tau_1$.

Proposition:

$M_{\tau_1\tau_2} = M_{\tau_1} \cup M_{\tau_2}$.

Proof. $i \notin M_{\tau_1} \cup M_{\tau_2} \implies \tau_1(i) = \tau_2(i) = i \implies \tau_1\tau_2(i) = i \implies i \notin M_{\tau_1\tau_2}$. For the other direction, suppose that $i \in M_{\tau_1} \cup M_{\tau_2}$. Then in the first case, suppose $i \in M_{\tau_1}$ and $i \notin M_{\tau_2}$. Hence $\tau_2(i) = i$ and $\tau_1(i) \neq i$, which implies $\tau_1\tau_2(i) = \tau_1(i) \neq i$. Case 2 is similar. ■

Example:

If $\tau = (a_1 \;\; a_2 \cdots a_m)$ and $m \geq 2$, then

$$M_\tau = \{a_1, ..., a_m\}.$$

Definition:

A cycle of length 2 is called a *transposition*. It looks something like $\begin{pmatrix} i & j \end{pmatrix}$ with $i \neq j$.

Proposition:

Any permutation $\sigma \in S_n$ can be written as a product of transpositions.

Proof. We have already shown that any permutation can be written as a product of cycles, so it suffices to show that every cycle can be written as a product of transpositions. Notice that given a cycle $\begin{pmatrix} a_1 & a_2 \cdots a_n \end{pmatrix}$, we can use linking and induction to show that it equals

$$\begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_2 & a_3 \end{pmatrix} \cdots \begin{pmatrix} a_{n-1}, a_n \end{pmatrix}$$

as desired. ■ The product is certainly not unique, but the *parity* of the number of flips is unique.

Theorem:

If τ_i and σ_i are transpositions and $\tau_1 \cdots \tau_m = \sigma_1 \cdots \sigma_l$, then $m \equiv l \pmod 2$.

Proof. Notice that

$$(\sigma_1 \cdots \sigma_l)(\sigma_l \cdots \sigma_1) = \text{id}.$$

Hence

$$\tau_1 \cdots \tau_m \sigma_l \cdots \sigma_1 = \text{id}.$$

So it is enough to show that if

$$\text{id} = \gamma_1 \cdots \gamma_k$$

and γ_i's are transpositions, then k is even. (So in particular if we can show that this is true, then $m + l$ is even, and we are done.) Consider the following steps.

Step 1: Bring all a's to the left.
Step 2: Reduce the number of a's.
Step 3: There is no a at the end of this process.

For steps 1 and 2, we do something like $(y\ x)(a\ x) = (a\ x)(y\ z)$. Or do something like $(x\ y)(a\ x) = (y\ x)(x\ a) = (a\ y)(y\ x)$. Or, we could even have $(a\ x)(a\ x) = \text{id}$. Another possible scenario is $(a\ x)(a\ y) = (a\ y\ x) = (a\ y)(y\ x)$.

The point is, we can bring a to the left without changing the number of transpositions, while even being able to reduce the number of transpositions. Notice that we cannot have only one a in the transposition, else a will not be fixed under $\gamma_1 \cdots \gamma_k(a)$.

In this process, we are not changing the parity of the number of transpositions. And, at the end there are 0 transpositions. ■

Midterm: Cutoff is at section 1.4.

Lecture 10/22/2019 (Week 4 Tuesday):

Example:

Groups include $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n^\times, \times)$, $(\mathbb{Q}^\times, \times)$. These are the abelian groups. Groups that are not abelian include $(GL(n), \times)$, $(S_n, \circ)$ (for $n \geq 3$).

Example (continued):

To show that S_n is not abelian, it is enough to argue that S_3 is non-abelian. Indeed, consider $(1\ 2)$ and $(3\ 1)$.

$$(1\ 2)(3\ 1) = (1\ 3\ 2)$$

$$(3\ 1)(1\ 2) = (3\ 1\ 2).$$

Example:

Consider

$$S^1 = \{z \in \mathbb{C} | |z| = 1\}.$$

Then $(S^1, \cdot)$ is a group, because $1 \in S^1$, and $z \in S^1 \implies z \cdot \overline{z} = |z|^2 = 1$, and $|\overline{z}| = 1$. So $z^{-1} = \overline{z} \in S^1$. Multiplication is associative.

Now consider the roots of unity

$$\mu_n := \{z \in \mathbb{C} | z^n = 1\}$$

$$= \{e^{\frac{2k\pi i}{n}} | 0 \leq k < n\}.$$

Intuitively, this just means $2k\pi/n$ angles on the complex unit circle. Indeed, $z^n = 1 \implies |z|^n = 1$. Since $|z| \geq 0$, we conclude that $|z| = 1$. This further implies that $z = e^{i\theta}$. Combining this with the fact that $z^n = 1$, we have $z^n = e^{in\theta} = 1$, so $n\theta \in \mathbb{Z}2\pi$, so $\theta = 2k\pi/n$ for some $k \in \mathbb{Z}$.

This is a subgroup of S^1. Indeed, notice that $z_1^n, z_2^n = 1 \implies (z_1 z_2)^n = z_1^n z_2^n = 1$. Also $z^n = 1 \implies (z^{-1})^n = (z^n)^{-1} = 1$. Also $1^n = 1$. Hence μ_n is indeed a subgroup of S^1.

Subgroup criterion:

Suppose $(G, \cdot)$ is a group, and $H \subset G$. Then H is a subgroup of G if and only if
(1) $e \in H$, where e is the neutral element of G.
(2) $g_1, g_2 \in H \implies g_1 \cdot g_2 \in H$ (we say that H is closed under multiplication).
(3) $g \in H \implies g^{-1} \in H$ (we say H is *symmetric*, or H is closed under inversion).

Suppose $(G, \cdot)$ is a group. $\forall g \in G$, $\underbrace{g \cdot g \cdots g}_{n \text{ times}} = g^n$ for $n \in \mathbb{Z}^+$. We define g^0 to be the neutral element. We also define $g^{-n} = (g^n)^{-1} = (\underbrace{g \cdot g \cdots g}_{n \text{ times}})^{-1}$. This equals $(g)^{-1} \cdots (g)^{-1} = (g^{-1})^n$.

Exponential laws:

(1) $\forall m, n \in \mathbb{Z}$, $\forall g \in G$, $(g^m)(g^n) = g^{m+n}$.
(2) $(g^m)^n = g^{mn}$.

Proof. If $m, n \in \mathbb{Z}^+$, then

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

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

Hence conclusion obvious by associativity. Also,

$$(g^m)^n = \underbrace{g^m \cdots g^m}_{n \text{ times}} = (g \cdots g) \cdots (g \cdots g) = g^{mn}.$$

Now if $m > 0$ and $n < 0$, and additionally $m + n > 0$, then

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

$$= g^{m+n}$$

by cancellation. The other case may be checked similarly. For example, if $m > 0$ and $n < 0$, then $mn < 0$, and

$$(g^m)^n = ((g^m)^{-n})^{-1} = (g^{m(-n)}) = (g^{-mn})^{-1} = g^{mn}.$$

Recall: Suppose $(G, \cdot)$ and $(H, \star)$ are groups. A map $f : G \to H$ is a *group homomorphism* if

$$f(g_1 \cdot g_2) = f(g_1) \star f(g_2).$$

Definition:

$f : G \to H$ is called an *isomorphism* if f is a homomorphism and bijection.

Example:

Suppose $(G, \cdot)$ is a group and $g \in G$. Then $f : \mathbb{Z} \to G$, $f(n) = g^n$, is a group homomorphism.

Proof. We have to check that $f(n+m) = f(n) \cdot f(m)$. We have $f(n+m) = g^{n+m}$ and $f(n) \cdot f(m) = g^n \cdot g^m = g^{n+m}$, where the last equality is justified by the exponential laws. ■

Example:

If $a^n = b^n$ and $a^m = b^m$ for some coprime integers m, n, then $a = b$.

Indeed, since $\gcd(m, n) = 1$, we write $rm + sn = 1$ for $r, s \in \mathbb{Z}$. Hence

$$a = a^1 = a^{rm+sn} = a^{rm}a^{sn} = (a^m)^r(a^n)^s = (b^m)^r(b^n)^s$$
$$= b^{mr}b^{ns} = b^{mr+ns} = b.$$

Example:

If $g \in G$, let

$$c_g : G \to G, \;\; c_g(x) = gxg^{-1}.$$

We say that gxg^{-1} is a *conjugate* of x. We claim that c_g is an isomorphism. (An isomorphism from G to itself is called an *automorphism*).

Proof. Need to show that

$$c_g(xx') = c_g(x)c_g(x').$$

For the LHS,

$$c_g(xx') = gxx'g^{-1}.$$

Also

$$c_g(x)c_g(x') = gxg^{-1}gx'g^{-1} = gxx'g^{-1}.$$

Hence c_g is a homomorphism. Next, we claim that $c_{g^{-1}} \circ c_g = c_g \circ c_{g^{-1}} = \mathrm{id}_G$, which shows that c_g is a bijection. Indeed,

$$c_{g^{-1}}(c_g(x)) = c_{g^{-1}}(gxg^{-1}) = g^{-1}(gxg^{-1})(g^{-1})^{-1} = x.$$

We call c_g an *inner automorphism*. We also remark that if G is Abelian, then $c_g(x) = x$.

Proposition:

$c_{g_1}c_{g_2} = c_{g_1g_2}$.

Proof: Direct computation.

Remark: $c : G \to \mathrm{Aut}(G)$, where $C(g) := c_g$ is a group homomorphism.

Example:

Suppose that $aba^{-1} = b^2$ and $a^3 = e$. Show that $b^7 = e$.

Solution. Notice that $c_a(b) = b^2$, so $c_a(c_a(b)) = c_a(b^2) = c_a(b)c_a(b) = b^4$, where the second-to-last equality follows from the fact that c_a is a group homomorphism. So we obtain

$$c_{a^2}(b) = c_a(c_a(b)) = b^4.$$

Hence

$$c_a(c_{a^2}(b)) = c_a(b^4) = c_a(b)^4 = (b^2)^4$$

But we also have

$$c_a(c_{a^2}(b)) = c_{a^3}(b) = b^8$$

$$\implies c_e(b) = b^8 \implies b = b^8 \implies e = b^8 \cdot b^{-1}$$

as desired.

Lecture 10/24/2019 (Thursday):

Two-Step Subgroup Test

Let $(G, \cdot)$ be a group. A set $H \subset G$ is a subgroup of G if the following conditions are satisfied:
(1) $e_G \in H$
(2) $h_1, h_2 \in H \implies h_1 \cdot h_2 \in H$
(3) $h \in H \implies h^{-1} \in H$.

Example:

Let $\phi : G_1 \to G_2$ be a group homomorphism. Then

$$\mathrm{Im}(\phi) := \{\phi(g) | g \in G_1\}$$

is a subgroup of G_2. We check this using the two-step subgroup test.

(1) We claim that $\phi(e_{G_1}) = e_{G_2}$. Indeed,

$$\phi(e_{G_1}) = \phi(e_{G_1} \cdot e_{G_1}) = \phi(e_{G_1}) \cdot \phi(e_{G_1}).$$

Since the neutral element is unique, we have $\phi(e_{G_1}) = e_{G_2}$.

(2) Let $g, g' \in \mathrm{Im}(\phi)$. Then we can write $g = \phi(h)$ and $g' = \phi(h')$ for $h, h' \in G_1$. Then

$$g \cdot g' = \phi(h) \cdot \phi(h') = \phi(hh').$$

Hence $g \cdot g' \in \mathrm{Im}(\phi)$.

(3) Let $g \in \mathrm{Im}(\phi)$. Then we can write $g = \phi(h)$ for $h \in G_1$. Then we claim that $g^{-1} = \phi(h^{-1})$. Indeed,

$$g \cdot \phi(h^{-1}) = \phi(h) \cdot \phi(h^{-1}) = \phi(h \cdot h^{-1}) = \phi(e_{G_1}) = e_{G_2}$$

$$\phi(h^{-1}) \cdot g = \phi(h^{-1}) \cdot \phi(h) = \phi(h^{-1}h) = e_{G_2}.$$

Example:

Recall that we have defined the *kernel* of a group homomorphism $f : G_1 \to G_2$ to be

$$\ker(\phi) := \{g \in G_1 | \phi(g) = e_{G_2}\}.$$

This is a subgroup of G. Indeed,

(1) $\phi(e_{G_1}) = e_{G_2} \implies e_{G_1} \in \ker(\phi)$
(2) Suppose $g, g' \in \ker(\phi)$. Then $\phi(g \cdot g') = \phi(g) \cdot \phi(g') = e_{G_2} \cdot e_{G_2} = e_{G_2}$.
(3) Suppose $g \in \ker(\phi)$. Then $\phi(g^{-1}) = \phi(g)^{-1} = e_{G_2}^{-1} = e_{G_2}$.

Definition:

Let G be a group and let g be an element of G. We define the *centralizer* of g to be

$$C_G(g) := \{g' \in G | g \cdot g' = g' \cdot g\}.$$

Lecture 10/29/2019 (Tuesday):

Remark: Midterm: median 39, average 37.9, (1/4)th of students ≥ 45, (3/4)th of students ≥ 28. There are 12 students ≤ 27, which is C range. There are 17 students ≥ 44, which is A range.

Recall: If $\phi : G \to H$ is a group homomorphism, then $\text{Im}(\phi) \leq H$ is a subgroup, and $\ker(\phi) \leq G$ is a subgroup.

Definition:

Let $(G, \cdot)$ be a group and for $g \in G$ define

$$C_G(g) := \{h \in G | gh = hg\}.$$

This is called the centralizer of g in G.

Proposition:

$C_G(g)$ is a subgroup of G.

Proof. $e \cdot g = g \cdot e = g$, where e is the neutral element. This shows that $e \in C_G(g)$. Next, let $h \in C_G(g)$. This means that $gh = hg$. Multiplying both sides by h^{-1} repeatedly, we get

$$h^{-1}g = gh^{-1}.$$

Hence $h^{-1} \in C_G(g)$. Lastly if $h_1, h_2 \in C_G(g)$, then

$$(h_1h_2)g = h_1(h_2g) = h_1(gh_2)$$

$$(h_1g)h_2 = (gh_1)h_2.$$

This shows that $h_1h_2 \in C_G(g)$. ■

Proposition:

Let $H_1, H_2 \leq G$. Then $H_1 \cap H_2 \leq G$. More generally, $\{H_i\}_{i \in I}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Proof. $\forall i \in I$, since $H_i \leq G$, $e \in H_i$. This means that $e \in \bigcap_{i \in I} H_i$. Now let $g \in \bigcap_{i \in I} H_i$. Then since H_i is a subgroup, $g^{-1} \in H_i$ for every i, and hence

$g^{-1} \in \bigcap_{i\in I} H_i$. Finally let $h_1, h_2 \in \bigcap_{i\in I} H_i$. Since for all $i \in I$, H_i is a subgroup, $h_1h_2 \in H_i$ for all $i \in I$. Hence $h_1h_2 \in \bigcap_{i\in I} H_i$. ■

Example:

Suppose that $H_1, H_2 \leq G$. If $H_1 \cup H_2 \leq G$, then either $H_1 \subset H_2$ or $H_2 \subset H_1$.

Proof. Suppose to the contrary that this is not the case. Then there exists $h_1 \in H_1 \backslash H_2$ and $h_2 \in H_2 \backslash H_1$. Since $H_1 \cup H_2 \leq G$, $h_1h_2 \in H_1 \cup H_2$. In particular

$$\begin{gathered} h_1h_2 \in H_1 \text{ or } h_1h_2 \in H_2 \\ \implies h_1^{-1}h_1h_2 \in H_1 \text{ or } h_1h_2h_2^{-1} \in H_2 \\ h_2 \in H_1 \text{ or } h_1 \in H_2. \end{gathered}$$

Contradiction.

Definition:

Define

$$Z(G) := \{g \in G | \forall h \in G, gh = hg\}.$$

This is called the *center* of G. Observe that

$$Z(G) = \bigcap_{h\in G} C_G(h).$$

This is a subgroup of G.

Indeed, if $g \in \bigcap_{h\in G} C_G(h)$, then for all $h \in G$, $g \in C_G(h) \iff \forall h \in G, gh = hg \iff g \in Z(G)$.

Example:

Since S_2 is Abelian, $Z(S_2) = S_2$.

Example:

What about S_n for $n \geq 3$? If $\sigma \in Z(S_n)$, then $\forall \tau \in S_n$, $\tau\sigma\tau^{-1} = \sigma$. If $\sigma \neq \text{Id}$, then $\sigma = \begin{pmatrix} a & b & \cdots \end{pmatrix} (...) (...)$. Observe that

$$\tau\sigma\tau^{-1} = \tau(a \;\; b \;\; ...)\tau^{-1}\tau(...)\tau^{-1}...\tau(\cdots)\tau^{-1}$$

$$= (\tau(a) \;\; \tau(b) \;\; ...)(...)(...).$$

This follows by result from midterm 1. Since the initial cycles were disjoint, after applying τ, we get disjoint cycles again. If $\tau(a) = a$ and $\tau(b) = c \notin \{a, b\}$ (notice that this requires $n \geq 3$). Then

$$\tau\sigma\tau^{-1}(a) = \tau\sigma(a) = \tau(b) = c$$

while

$$\sigma(a) = b \neq c.$$

So $\tau\sigma\tau^{-1} \neq \sigma$. From all of this work we conclude that $\sigma \notin Z(S_n)$. So

$$Z(S_n) = \{\text{id}\}.$$

Example:

We have

$$Z(GL_n(\mathbb{R})) = \left\{ \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} | c \in \mathbb{R}^\times \right\} = \mathbb{R}^\times I.$$

This conclusion should follow by observing that

$$g \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} g$$

$$g \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} g$$

if $g \in Z(GL_n(\mathbb{R}))$.

Example:

$Z(\mathbb{Z}_n) = \mathbb{Z}_n$ since $\mathbb{Z}_n$ is Abelian.

What is the smallest subgroup that contains $g \in G$? Certainly such a subgroup should contain $\{e, g, g^{-1}, g^{-2}, ..., g^2, g^3, ...\}$. We have discussed that $\phi : \mathbb{Z} \to G$, $\phi(n) = g^n$ is a group homomorphism. Thus, the image of ϕ is a subgroup, which is exactly the subgroup form we have above.

Definition:

This is called the subgroup *generated* by g, and it is denoted by $\langle g \rangle$. This is the smallest subgroup of G that contains g.

Example:

$< 2 >$ in $\mathbb{Z}$ is $2\mathbb{Z}$.

Example:

$< 2 >$ in $\mathbb{Z}_5$ is $\mathbb{Z}_5$. Indeed,

$$< 2 >= \{2n | n \in \mathbb{Z}\}.$$

For what integers m do we have

$$[2n]_5 = [m]_5$$

for some $n \in \mathbb{Z}$? Alternatively we need to find out if

$$2n \equiv m \pmod 5$$

has a solution. Since $\gcd(2, 5) = 1$, it has a solution for any m. So any element of $\mathbb{Z}_5$ is in $< 2 >$.

Definition:

Suppose $(G, \cdot)$ is a group and $g \in G$. Then the smallest positive integer n such that $g^n = e$ (if it exists) is called the *order* of g. It is denoted by $o(g)$ or $|g|$.

If there is no such n, we say that $o(g) = \infty$; g is of infinite order.

Lemma:

If $(G, \cdot)$ is a finite group, then any element has finite order.

Proof. Suppose $|G| = n$. Consider $\{e, g, g^2, ..., g^n\} \subset G$. By pigeonhole, for some $0 \leq i < j \leq n$ we have $g^i = g^j$. But this implies

$$g^i g^{-i} = g^j g^{-i} \implies e = g^{j-i}.$$

Hence g is of finite order. ■

Lemma:

Suppose that $(G, \cdot)$ is a finite abelian group, then for all $g \in G$,

$$g^{|G|} = e.$$

Proof. Consider $l_g : G \to G$, $l_g(h) = gh$. Then we claim that l is a bijection. Indeed,

$$l_{g^{-1}} \circ l_g(h) = l_{g^{-1}}(l_g(h)) = h$$
$$l_g \circ l_{g^{-1}}(h) = h.$$

Notice that we have not used that fact that G is a finite abelian group. Next, using the fact that l_g is a bijection on a finite set, if $G = \{g_1, ..., g_n\}$, then $\{gg_1, gg_2, ..., gg_n\}$ is also G. Since G is Abelian, we deduce that

$$(g_1 \cdots g_n) = (gg_1)(gg_2)\cdots(gg_n)$$
$$= g^n(g_1 g_2 \cdots g_n)$$
$$\implies g^n = e.$$

This completes the proof. ■

Remark: $l_g : G \to G$, $l_g(h) = gh$ is a bijection for any group G.

Recall: $\phi : \mathbb{Z} \to G$, $\phi(n) = g^n$ is a group homomorphism. This implies that $\ker(\phi) \leq \mathbb{Z}$. This means that $\ker(\phi) = m\mathbb{Z}$ for some $m \geq 0$. By the definition of order of G, we have $\ker(\phi) = 0$ if $o(g) = \infty$ and $o(g)\mathbb{Z}$ if $o(g) < \infty$. Indeed,

$$\ker(\phi) = \{n \in \mathbb{Z} | g^n = e\}.$$

This m is precisely the order of g, unless if g has infinite order.

Lemma:

Suppose that $(G, \cdot)$ is a finite group. Then for every $g \in G$,

$$o(g) \mid |G|.$$

Lecture 10/31/2019 (Week 5 Thursday):

Recall: $f : \mathbb{Z} \to G$, $f(n) = g^n$ is a group homomorphism. We have $\ker(f) = \{0\}$ if and only if $o(g) = \infty$. When $o(g) < \infty$, we have

$$\ker(f) = o(g)\mathbb{Z}.$$

Lemma:

Suppose that $o(g) < \infty$. Then

$$g^n = g^m \iff n \equiv m \pmod{o(g)}.$$

Proof. $g^n = g^m \iff g^n \cdot g^{-m} = e \iff g^{n-m} = e \iff f(n-m) = e$. This implies that $n - m \in \ker(f)$. From this we conclude that $n - m \in o(g)\mathbb{Z}$, and finally $n \equiv m \pmod{o(g)}$. ■

Proposition:

Suppose $G = \langle g_0 \rangle$ is a group with n elements. Then $G \cong \mathbb{Z}_n$; this means there is a group isomorphism $\overline{f} : \mathbb{Z}_n \to G$.

Proof. Let $\overline{f}([k]_n) = g_0^k$. We need to show that $\overline{f}$ is well-defined. If $[k_1]_n = [k_2]_n$, must we have $g_0^{k_1} = g_0^{k_2}$? Now,

$$\begin{aligned} [k_1]_n = [k_2]_n &\implies k_1 \equiv k_2 \pmod{n} \\ &\implies g_0^{k_1} = g_0^{k_2} \end{aligned}$$

if $o(g_0) = n$, by the previous lemma.

Claim: $o(g_0) = |\langle g_0 \rangle| = n$.

Proof of claim. Let $o(g_0) = m$. We want to show $m = n$. Notice that none of $g_0, g_0^2, ..., g_0^{m-1}$ equals e. This implies that $g_0^i \neq g_0^j$ if $0 \leq i < j \leq m-1$. If not, then $g^i = g^j \implies g^{j-i} = e$, for $0 < j - i \leq m - 1$. Hence we have found m distinct elements in the group, so it must be that $m \leq n$.

On the other hand, for every $g \in G = \langle g_0 \rangle$, we have $g = g_0^k$ for some integer $k \in \mathbb{Z}$. Suppose q is the quotient and r is the remainder of k divided by m. That is, $k = mq + r$, and $0 \leq r < m$. This implies that $k \equiv r \pmod{m}$, and furthermore $g_0^k = g_0^r$. Hence $g \in \{g_0^0, g_0^1, ..., g_0^{m-1}\}$. Since $g \in G$ was arbitrary, the order of G cannot be greater than m. So $n \leq m$. ■

We now show that $\overline{f}$ is surjective. We know that $\forall g \in G$, $g = g_0^k$ for $k \in \mathbb{Z}$. But this means that $g = \overline{f}([k]_n)$. This shows that $\overline{f}$ is surjective.

$\overline{f}$ is also injective. Assume that

$$\overline{f}([k_1]_n) = \overline{f}([k_2]_n).$$

Then

$$\begin{aligned} g_0^{k_1} = g_0^{k_2} &\implies k_1 \equiv k_2 \pmod{o(g)} \\ &\implies k_1 \equiv k_2 \pmod{n} \\ &\implies [k_1]_n = [k_2]_n. \end{aligned}$$

It remains to show that $\overline{f}$ is a homomorphism. Notice that

$$\overline{f}([k_1]_n + [k_2]_n) = \overline{f}([k_1 + k_2]_n) = g_0^{k_1+k_2}$$

$$g_0^{k_1} \cdot g_0^{k_2} = \overline{f}([k_1]_n)\overline{f}([k_2]_n).$$

This finishes the proof. ■

Corollary:

(1) If G is generated by g, then the order of g must be the order of G.
(2) Also

$$G = \{e, g, ..., g^{o(g)-1}\}.$$

(3) $G \cong \mathbb{Z}_{o(g)}$.

Proposition:

Suppose $o(g) = n < \infty$. Then $o(g^m) = \frac{n}{\gcd(n,m)}$.

Proof. $(g^m)^k = e \iff g^{mk} = g^0 \iff mk \equiv 0 \pmod{n}$. This happens iff

$$n|mk \iff \frac{n}{\gcd(n,m)} \Bigg| \frac{m}{\gcd(n,m)} \cdot k.$$

Notice that also

$$\gcd\left(\frac{n}{\gcd(n,m)}, \frac{m}{\gcd(n,m)}\right) = 1.$$

Combining the above observations, $[n/\gcd(n,m)]|k$. So the smallest positive k such that $(g^m)^k = e$ is $\frac{n}{\gcd(n,m)}$. ■

Corollary:

Suppose $G = \langle g_0 \rangle$ has n elements. Then

$$G =< g_0^m > \iff \gcd(n,m) = 1.$$

Proof. $G =< g_0^m > \iff |G| = | < g_0^m > | \iff n = o(g_0^m) = \frac{o(g_0)}{\gcd(n,m)}$. Since $o(g_0) = n$, for the above to hold we must have $\gcd(n,m) = 1$. ■

Example:

$\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic, because the order of any element is at most 2 (check). Because, if this group were to be cyclic, then at least one element must have order 4.

Example:

Symmetries of the real line with function composition form a group. Notice that the composition of two reflections (say reflections about 0 and 1) is a translation. The conclusion is, even though both of these symmetries are of finite order 2, the composition has infinite order.

Lemma:

Let $a, b \in G$ with $ab = ba$. Assume that $o(a) = n < \infty$, and $o(b) = m < \infty$. Then

$$o(ab) = \operatorname{lcm}(m,n).$$

Proof. We need to find the smallest positive k such that $(ab)^k = e \iff a^k b^k = e \iff a^k = b^{-k}$. This implies that $a^{nk} = b^{-nk} \implies e = b^{-nk}$. Hence $m|nk$, and similarly $a^{mk} = b^{-mk} = e$ and $n|mk$. We have $m|nk$ and $n|mk$ if and only if $\frac{m}{\gcd(m,n)} | \frac{n}{\gcd(m,n)} k$, which implies that $\frac{m}{\gcd(m,n)} | k$. Similarly $\frac{n}{\gcd(m,n)} | k$. Since $\gcd(\frac{m}{\gcd(m,n)}, \frac{n}{\gcd(m,n)}) = 1$, we have

$$\frac{mn}{\gcd(m,n)^2} | k \implies \frac{\operatorname{lcm}(m,n)}{\gcd(m,n)} | k.$$

If we assume $\gcd(m,n) = 1$, then $\operatorname{lcm}(m,n) = mn$ divides k.

In summary, we have shown if $\gcd(m,n)=1$ and $(ab)^k=e$, then $mn|k$. Notice that $(ab)^{mn}=e$. So $mn|o(ab)$ and $o(ab)|mn$ implies $mn=o(ab)$. ■

I was wondering why $\gcd(a,b)=1 \implies \operatorname{lcm}(a,b)=ab$, but here is a more general statement that answers my question:

Proposition:

We have
$$\gcd(a,b)\operatorname{lcm}(a,b)=ab.$$

Proof. Later.

Lecture 11/5/2019 (Week 6 Tuesday):

Recall: Suppose G is a group and $g \in G$ is of finite order. Then

$$|\langle g \rangle| = o(g)$$

and

$$\langle g \rangle = \{1, g, ..., g^{n-1}\}$$

where $n = o(g)$.

Recall: Also remember that $G \cong \mathbb{Z}_n$ if G is a cyclic group of order n. In particular, $[a]_n \to g_0^a$ is a well defined group isomorphism, if g_0 is the generating element of G.

Recall: If $g \in G$ has finite order, then

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

Recall: $g^n = g^m$ iff $n \equiv m \pmod{o(g)}$. In particular, $g^n = 1$ if and only if $o(g)|n$.

Lemma:

Let G be a group, and $a, b \in G$ with $ab = ba$. Let $o(a) = n$, $o(b) = m$. Then

$$o(ab)|\text{lcm}(m, n)$$

$$\frac{\text{lcm}(m, n)}{\text{gcd}(m, n)}\Big|o(ab).$$

In particular if $\gcd(m, n) = 1$, then $o(ab) = mn$.

Proof. Let

$$l = \text{lcm}(m, n)$$

$$r = gcd(m, n).$$

Then write $m = rm'$ and $n = rn'$. This means that $l = rm'n'$. Now observe that

$$(ab)^l = a^l b^l \text{ since } ab = ba.$$

$$o(a)|l \implies a^l = 1$$

$$o(b)|l \implies b^l = 1.$$

The three observations above imply that $(ab)^l = 1$, and hence $o(ab)|l$. This proves the first part of the lemma. Suppose that $o(ab) = k$. Then

$$(ab)^k = 1 \implies a^k b^k = 1$$
$$\implies a^k = b^{-k} \ (\star)$$
$$(\star)^n \implies a^{kn} = b^{-kn}$$
$$\text{Also } o(a)|kn \implies a^{kn} = 1.$$

Hence $b^{-kn} = 1$, so $m|kn$. Now

$$(\star)^m \implies a^{km} = b^{-km}$$

$$o(b)| - km \implies b^{-km} = 1 \implies a^{km} = 1.$$

We conclude that $n|km$. Now

$$n|km \implies rn'|krm'$$
$$\implies n'|km'.$$

Now observe that $\gcd(m,n) = r \implies \gcd(m/r, n/r) = 1 \implies \gcd(m', n') = 1$. By Euclid's lemma,

$$n'|k.$$

Now observing that $m|kn \implies rm'|krn'$

$$\implies m'|kn'.$$

Since we also have $\gcd(m', n') = 1$ we have $m'|k$. Now using the fact that $\gcd(m', n') = 1$, we conclude that $m'n'|k \implies (l/r)|k$. ■

Proposition:

Let $\sigma \in S_n$ and $\sigma = \tau_1\tau_2 \cdots \tau_m$ where τ_i's are disjoint cycles, where the length of τ_i is l_i. Then

$$o(\sigma) = \text{lcm}(l_1, ..., l_m).$$

Proof. Let $k = o(\sigma)$ and $s = \text{lcm}(l_1, ..., l_m)$. We first want to show $k|s \implies k \leq s$. To show $k|s$, it suffices to show that the identity permutation equals the below.

$$\sigma^s = (\tau_1 \cdots \tau_m)^s$$
$$= \tau_1^s \cdots \tau_m^s.$$

For each τ_i we clearly have $o(\tau_i) = l_i$. So this implies that $\tau_i^s = \text{id}$. Hence in the above calculation we have $\sigma^s = \text{id} \implies o(\sigma)|s$.

Now notice that $M_{\tau_i^r} \subset M_{\tau_i}$, and so $\tau_1^r, ..., \tau_m^r$ (they are not necessarily cycles!) are disjoint. Notice that

$$\text{id} = \sigma^k = \tau_1^k \tau_2^k \cdots \tau_m^k.$$

Since τ_i^k are disjoint, we have

$$M_{\tau_1^k \cdots \tau_m^k} = \cup_{i=1}^m M_{\tau_i^k} = \emptyset$$

where the last equality follows from the fact that $\text{id} = \sigma^k = \tau_1^k \tau_2^k \cdots \tau_m^k$. Then

$$\implies \forall i, M_{\tau_i^k} = \emptyset \implies \tau_i^k = \text{id}$$

$$\implies o(\tau_i)|k \implies l_i|k \implies s|k.$$

Combining observations $k = o(\sigma)|s$ and $s|k$, we conclude that $k = s$. ■

Remark: (Note to myself) I was wondering about why $l_i|k \implies s|k$. A rigorous proof might be cumbersome, but let me record my thought process here. So if you think the implication isn't true, then you probably were thinking that it is possible for the lcm of the l_i's to be something greater than k, but this doesn't happen. For example, say

$$l_1 = 5|k, l_2 = 5|k, l_3 = 6|k.$$

Then $\text{lcm}(5, 5, 6) = \text{lcm}(5, 6) = 30$. The key idea here is that the lcm only depends on the l_i's that are distinct, so if we know that $l_i|k \implies l_i \leq k$, then it cannot be the case that the lcm ends up to be something greater than k, because the l_i that are distinct are necessary a subset of the prime factors (counting multiplicities) of k.

Theorem:

Suppose that $G = \langle g \rangle$ is a cyclic group of order n. Then for any $d|n$, G has a *unique* subgroup of order d. Furthermore, any subgroup of G is one of those.

Theorem (reworded):

Suppose that $G = \langle g \rangle$ is a cyclic group of order n. Then if H is a subgroup of G, then $H = \langle g^d \rangle$ for some $d|n$. Conversely, if $d|n$, G has a unique subgroup of order d, namely $\langle g^{n/k} \rangle$.

Proof. (Existence) Suppose that $d|n$. Then

$$o(g_0^m) = \frac{o(g_0)}{\gcd(o(g_0), m)} = \frac{|\langle g_0 \rangle|}{\gcd(|\langle g_0 \rangle|, m)} = \frac{n}{\gcd(n, m)}.$$

So,

$$\implies o(g_0^{n/d}) = \frac{n}{\gcd(n, n/d)} = \frac{n}{n/d} = d$$

$$\implies |\langle g_0^{n/d} \rangle| = o(g_0^{n/d}) = d.$$

So $< g_0^{n/d} >$ is a subgroup of order d. Now we show that any subgroup of G is cyclic. To prove this, recall that $f : \mathbb{Z} \to \langle g_0 \rangle$ given by $f(n) = g_0^n$ is a group homomorphism. Let H be a subgroup of $\langle g_0 \rangle$. We claim that $f^{-1}(H)$ is a subgroup of $\mathbb{Z}$.

Why is this the case? First, $0 \in f^{-1}(H)$ because $f(0) = 1 \in H$. Now if $m \in f^{-1}(H)$ then

$$f(m) \in H \implies f(m)^{-1} \in H \implies f(-m) \in H$$

$$-m \in f^{-1}(H).$$

Finally if $m, k \in f^{-1}(H)$, then $f(m), f(k) \in H \implies f(m) \cdot f(k) \in H$

$$\implies f(m+k) \in H \implies m + k \in f^{-1}(H).$$

We know that every subgroup of $\mathbb{Z}$ is of the form $m\mathbb{Z}$. Hence $f^{-1}(H) = m\mathbb{Z}$. Applying f to both sides, we get, since f is surjective, $H = f(f^{-1}(H)) = f(m\mathbb{Z}) \implies \{g_0^{mk} | k \in \mathbb{Z}\} =< g_0^m >$.

The second-to-last step is showing that if H is a subgroup of G, then $|H| \Big| n$. We prove this as follows. From the previous step, we know that

$$H =< g_0^m >$$

for some m. Then

$$|H| = | < g_0^m > |$$
$$= \frac{n}{\gcd(n, m)} | n.$$

The final step is to show uniqueness: suppose H is a subgroup of order d, we have to show that

$$H =< g^{n/d} > .$$

We have already proved that $H =< g_0^m >$ for some m. So

$$|H| = d \implies d = \frac{n}{\gcd(n, m)} \implies \frac{n}{d} = \gcd(n, m)$$

$$\exists r, s \in \mathbb{Z}, \ \ rn + sm = \frac{n}{d}$$

$$\implies g_0^{n/d} = g_0^{rn+sm} = g_0^{rn} g_0^{sm} = g_0^{sm}$$

as $o(g_0) = n$. Then

$$\implies g_0^{n/d} = (g_0^m)^s \in < g_0^m >= H.$$

So $< g_0^{n/d} > \subset H$. Since $| < g_0^{n/d} > | = |H| = d$ and $< g_0^{n/d} > \subset H$, we deduce that $H =< g_0^{n/d} >$. ■

Remark: The flowchart in this proof goes like this. First assume that $G = \langle g_0 \rangle$ is a cyclic group of order n. Then:
(1) Prove that $d|n \implies$ there exists a subgroup of G of order d, namely $< g_0^{n/d} >$. Indeed,

$$o(g_0^{n/d}) = \frac{o(g_0)}{\gcd(o(g_0), n/d)} = \frac{n}{\gcd(n, n/d)} = d.$$

(2) (*Only* an intermediate step) Next, show that any subgroup $H \leq G$ is cyclic. Indeed, $H = f(m\mathbb{Z})$, so H is a cyclic group.
(3) Then show that $H \leq G \implies |H|$ divides n. From the previous intermediate step, we know that $H =< g_0^m >$ for some m, which implies that $|H| = \frac{n}{\gcd(n,m)}|n$.
(4) Lastly show that any subgroup $H \leq G$ of order d must be $< g_0^{n/d} >$. Write $H =< g_0^m >$ for some m, and obtain

$$\frac{n}{d} = \gcd(n, m).$$

Argue that $g_0^{n/d} \in H$, and thus $< g_0^{n/d} > \subset H$, but $| < g_0^{n/d} > |$ and H both have order d, so they are the same set.

Example:

We have $(\mathbb{R}^+, \cdot) \cong (\mathbb{R}, +)$. Indeed, taking $\ln : \mathbb{R}^+ \to \mathbb{R}$, we have

$$\ln(xy) = \ln(x) + \ln(y).$$

Natural log is a bijection because $\exp : \mathbb{R} \to \mathbb{R}^+$ is the inverse function of ln.

Example:

Is $(\mathbb{R}\backslash\{0\}, \cdot)$ isomorphic to $(\mathbb{R}, +)$? If $f : \mathbb{R}\backslash\{0\} \to \mathbb{R}$ is a group isomorphism, then

$$f(-1)f(-1) = f((-1)^2) = 0.$$

Contradiction since $f(-1) = 0 = f(1)$.

Lecture 11/7/2019 (Week 6 Thursday):

Theorem (Cayley):

If G is group, then G can be realized as a subgroup of a symmetric group. That is, there is an injective group homomorphism $G \to S_X$ (for some set X). In fact we show that there is an injective group homomorphism $f : G \to S_G$.

Proof. We want to define $f : G \to S_G$ such that $\forall g \in G$, $f(g)$ is a bijection.

$$f(g) : G \to G.$$

For $g' \in G$, we define

$$f(g)(g') = gg'.$$

We claim that $f(g)$ is a bijection. We claim that $f(g^{-1})$ is the inverse of $f(g)$. Indeed,

$$(f(g) \circ f(g^{-1}))(g') = g(g^{-1}g') = g'$$
$$(f(g^{-1}) \circ f(g))(g') = g^{-1}(gg') = g'.$$

Hence $f(g)$ is indeed invertible, so it is a bijection. Now we check that $f(g)$ is a group homomorphism. We have for any $g' \in G$

$$f(g_1g_2)(g') = (g_1g_2)(g')$$

$$(f(g_1) \circ f(g_2))(g') = g_1(g_2g').$$

Hence we conclude that the two *functions* $f(g_1g_2)$ and $f(g_1) \circ f(g_2)$ are equal to each other.

The last thing we need to show is that f is injective. Suppose that $f(g_1) = f(g_2)$. This means that $\forall g' \in G$ we have

$$f(g_1)(g') = f(g_2)(g') \iff g_1g' = g_2g' \implies g_1 = g_2.$$

This is exactly what we wanted to show. ■

Remark: So each g gives a permutation $f(g)$ through f. So f is a function from G to another set of functions.

Corollary:

(Added by Brian) For any group G,

$$\{f : G \to G | \exists g \text{ s.t. } \forall g' \in G, \;\; f(g') = gg'\} \leq S_G$$

Example:

Let $G = \{1, a, a^2\}$ (assume that $a^3 = 1$). For the multiplication table we have

$$\begin{pmatrix} \cdot & 1 & a & a^2 \\ 1 & 1 & a & a^2 \\ a & a & a^2 & 1 \\ a^2 & a^2 & 1 & a \end{pmatrix}.$$

So with the notation above, $f(1)(1) = 1$, $f(1)(a) = a$, and $f(1)(a^2) = a^2$.

Example:

Let $G = \{1, \zeta, \zeta^2\} \subset \mathbb{C}$, the three roots of unity. Then we have

$$f(\zeta)(1) = \zeta$$

$$f(\zeta)(\zeta) = \zeta^2$$

$$f(\zeta)(\zeta^2) = 1.$$

This is really nice because it gives us the second row in the following permutation table:

$$\begin{pmatrix} \cdot & 1 & \zeta & \zeta^2 \\ 1 & 1 & \zeta & \zeta^2 \\ \zeta & \zeta & \zeta^2 & 1 \\ \zeta^2 & \zeta^2 & 1 & \zeta \end{pmatrix}.$$

We see that f is an injection. We see that each of the functions $f(1), f(\zeta), f(\zeta^2)$ are bijections $G \to G$. It also isn't too hard to verify that f is a group homomorphism.

Definition:

Let $(G, \cdot)$ be a group. We define

$$\mathrm{Aut}(G) = \{\theta : G \to G | \theta \text{ is an automorphism}\}.$$

That is θ is a isomorphism from a group to itself.

Lemma:

$\theta : G \to H$ is an isomorphism $\implies$ $\theta^{-1} : H \to G$ is an isomorphism.

Proof. θ^{-1} is invertible, so it is a bijection. We want to show

$$\theta^{-1}(h_1 h_2) = \theta^{-1}(h_1)\theta^{-1}(h_2)$$

$$\iff h_1 h_2 = \theta(\theta^{-1}(h_1)\theta^{-1}(h_2))$$

$$= \theta(\theta^{-1}(h_1))\theta(\theta^{-1}(h_2)) = h_1 h_2.$$

This proves that θ^{-1} is also a homomorphism. We conclude that θ^{-1} is an isomorphism. ■

Lemma:

Suppose that

$$G \xrightarrow{\theta} H \xrightarrow{\psi} L$$

where θ and ψ are group homomorphisms. Then

$$\psi \circ \theta : G \to L$$

is also a group homomorphism.

Proof. We have

$$(\psi \circ \theta)(g_1 g_2) = \psi(\theta(g_1))\psi(\theta(g_2))$$

$$= (\psi \circ \theta)(g_1 g_2) = (\psi \circ \theta)(g_1)(\psi \circ \theta)(g_2).$$

This completes the proof. ■

Proposition:

$(\mathrm{Aut}(G), \circ)$ is a group.

Proof. Let $\theta, \psi \in \mathrm{Aut}(G)$. Then by the previous results, we know that $\psi \circ \theta$ and $\theta \circ \psi$ are both bijective and group homomorphisms. Hence $\psi \circ \theta, \theta \circ \psi \in \mathrm{Aut}(G)$.

Also function composition is associative, the identity function is in $\mathrm{Aut}(G)$, and the inverse of an automorphism is also an automorphism. ■

Recall: $c : G \to \mathrm{Aut}(G)$, $c(g) = c_g$, where $c_g : G \to G$, $c_g(g') = gg'g^{-1}$. We have proved that $c_g \in \mathrm{Aut}(G)$. We have also seen that

$$c_{g_1} \circ c_{g_2} = c_{g_1 g_2}. \star$$

This means that $c(g_1) \circ c(g_2) = c(g_1 g_2)$. Therefore c is a group homomorphism.

Recall: $\ker(c) = \{g \in G | c(g) = \mathrm{id}\}$. We have

$$\begin{aligned} c_g = \mathrm{id} &\iff c_g(g') = g' \;\; \forall g' \in G \\ &\iff gg'g^{-1} = g' \\ &\iff gg' = g'g. \end{aligned}$$

Hence $\ker(c) = Z(G)$.

Definition:

$\mathrm{Im}(c)$ is called the set of inner automorphisms; it is denoted by $\mathrm{Inn}(G)$.

$$\mathrm{Inn}(G) = \{c_g : G \to G | c_g(g') = gg'g^{-1} \forall g' \in G\}$$

Definition:

Let $(G, \cdot)$ be a group and $H \leq G$ a subgroup of G. For all $g \in G$, let

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

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

These are the *right and left cosets*, respectively.

Example:

Let $G = \mathbb{R}^2$. Let $H = \{(x, x) | x \in \mathbb{R}\}$. Consider the coset $H + (1, 0)$. Then this gives the line $y = x$ shifted one unit to the right. These kinds of cosets partition the plane into parallel lines. Also notice that

$$H + (1, 1) = H.$$

Example:

If $G = \mathbb{Z}$, and $H = n\mathbb{Z}$, then the cosets of H are

$$\{n\mathbb{Z}, 1 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z}\}.$$

Theorem:

$$\{Hg | g \in G\}$$

is a partition of G. (The left coset is also a partition of G).

Lemma:

$g_1 \in Hg_2 \iff Hg_1 = Hg_2$.

Proof. ($\Longleftarrow$) If $Hg_1 = Hg_2$, then since $g_1 = 1 \cdot g_1 \in Hg_1$, we know $g_1 \in Hg_2$.

($\Longrightarrow$) If $g_1 \in Hg_2$, then $g_1 = h_0 g_2$ for some $h_0 \in H$. Hence $g_1 g_2^{-1} = h_0 \in H$. We show both inclusions in $Hg_1 = Hg_2$.

($\subset$) $\forall h \in H$, $hg_1 = h(h_0 g_2) = \underbrace{(hh_0)}_{\in H} g_2 \in Hg_2$. We conclude that $Hg_1 \subset Hg_2$.

($\supset$) $\forall h \in H$, $hg_2 = h(h_0^{-1} g_1) = \underbrace{(hh_0^{-1})}_{\in H} g_1 \in Hg_1$. This is what we wanted to prove. ■

Lemma:

$Hg_1 = Hg_2$ if and only if $g_1 g_2^{-1} \in H$. (Intuition: multiply both sides by g_2^{-1}.

Proof. ($\Longrightarrow$) $Hg_1 = Hg_2 \implies g_1 \in Hg_2$

$$\implies \exists h_0 \in H, g_1 = h_0 g_2 \implies g_1 g_2^{-1} = h_0 \in H.$$

($\Longleftarrow$) $g_1 g_2^{-1} = h_0 \in H$

$$\implies g_1 = h_0 g_2 \in Hg_2 \implies Hg_1 = Hg_2.$$

Lemma:

$Hg_1 \cap Hg_2 \neq \emptyset \iff Hg_1 = Hg_2$.

Proof. Reverse direction is left as exercise (but it is trivial). For the forward direction, if $Hg_1 \cap Hg_2 \neq \emptyset$.

$$\implies \exists g \in Hg_1 \cap Hg_2$$

$$\implies g \in Hg_1 \implies Hg = Hg_1 \text{ (first lemma)}$$

$$g \in Hg_2 \implies Hg = Hg_2 \implies Hg = Hg_2.$$

Hence $Hg_1 = Hg_2$. ■

Lecture 11/12/2019 (Week 7 Tuesday):

Recall: Let G be a group with $H \leq G$. A left coset of H is $gH = \{gh | h \in H\}$, and a right coset of H is $Hg = \{hg | h \in H\}$.

Recall: We have proved last lecture that $g_1 H = g_2 H$ if and only if $g_1 \in g_2 H$ if and only if $g_2^{-1} g_1 \in H$.

Proposition:

$\{gH | g \in G\}$ is a partition of G (so are the collection of right cosets).

Proof. (Disjointness) Suppose that $g_1 H \cap g_2 H \neq \emptyset$. We must show that $g_1 H = g_2 H$. To start, suppose that $g \in g_1 H \cap g_2 H$. Then $g \in g_1 H \implies gH = g_1 H$. Similarly, since $g \in g_2 H \implies gH = g_2 H$. Hence $g_1 H = g_2 H$. We conclude that if two left cosets intersect, then they are the same set.

(Union of all the cosets is G) We need to show that

$$\bigcup_{g \in G} gH = G.$$

Now $\forall g \in G$, notice that $g = g \cdot e \in gH \subset \bigcup_{g' \in G} g'H$. Hence $G = \bigcup_{g' \in G} g'H$ as we needed to show. ■

Alternatively, define a equivalence relation by $g_1 \sim g_2$ if $g_2^{-1} g_1 \in H$. The only interesting to show is that this is transitive. Well, if $g_2^{-1} g_1 \in H$ and $g_3^{-1} g_2 \in H$, then multiplying, we obtain $g_3^{-1} g_1 \in H$. Then this equivalence relation will partition G the desired way.

Definition:

A subgroup N is called a *normal subgroup* if for every $g \in G$, we have

$$gN = Ng.$$

Remark: If G is Abelian, then every subgroup of G is normal.

Notation:

The set of left cosets is denoted by G/H, and the set of right cosets is denoted by $H\backslash G$. $\star$

The reason for the notation is because, taking the left cosets G/H for example, you are looking at elements of the form gh.

Definition:

The *index* of H in G is $|G/H|$; this number is denoted by $[G : H]$.

Example:

We have:

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z}\} = \mathbb{Z}_n.$$

Proposition:

(a) $|H| = |gH| = |Hg|$; there are bijections between these sets.
(b) There exists a bijection $G/H \to H\backslash G$.
In particular $|G/H| = |H\backslash G|$.

Proof. (a) A bijection $H \to gH$ is given by $h \mapsto gh$. Similarly, $H \to Hg$ given by $h \mapsto hg$ is a bijection. Indeed, if $f : H \to gH$ is given by $f(h) = gh$, then $f^{-1} : gH \to H$ given by $f^{-1}(h') = g^{-1}h'$ is its inverse function. Notice that $h' \in gH$ implies that $h' = gh$ for some $h \in H$. And so $g^{-1}h' = h \in H$, and f^{-1} is thus well-defined. It is straightforward to verify that $f \circ f^{-1} = \mathrm{id}$ and that $f^{-1} \circ f = \mathrm{id}$. The other remaining case is handled similarly.

(b) A bijection is given by $i : G/H \to H\backslash G$, $i(gH) = Hg^{-1}$. We need to show that this is well-defined. That means we have to show that if $g_1H = g_2H$, then $Hg_1^{-1} = Hg_2^{-1}$.

Recall: $g_1H = g_2H$ if and only if $g_1^{-1}g_2 \in H$. Similarly $Hg_1' = Hg_2'$ if and only if $g_1'g_2'^{-1} \in H$.

Hence if $g_1H = g_2H$, then $g_1^{-1}g_2 \in H$. This happens iff

$$g_1^{-1}(g_2^{-1})^{-1} \in H \iff Hg_1^{-1} = Hg_2^{-1}.$$

Reading the implication in the forward direction, we have shown that i is well-defined. Reading the implication in the backwards direction, we have shown that i is injection.

It remains to show that i is surjective. An element of $H\backslash G$ is of the form Hg for some $g \in G$, but we have $i(g^{-1}H) = Hg$. ■

The intuition for coming up with this function is the realization that

$$\{gh | h \in H\} \xrightarrow{-1} \{h^{-1}g^{-1} | h \in H\} = Hg^{-1}.$$

Theorem: (Lagrange)

Suppose G is a finite group, and $H \leq G$. Then:

$$|G| = [G : H]|H|.$$

That is,

$$|G/H| = |G|/|H|.$$

Most importantly, the order of every subgroup of G divides the order of G.

Proof. Suppose that $[G : H] = m$, and $G/H = \{g_1H, ..., g_mH\}$. So

$$G = \bigsqcup_{i=1}^{m} g_iH$$

$$\implies |G| = \sum_{i=1}^{m} |g_iH| = \sum_{i=1}^{m} |H| = m|H|.$$

This proves the theorem. ■

Corollary:

If G is a finite group, then for every $g \in G$, $g^{|G|} = 1$. Equivalently, $o(g)||G|$.

Proof. $|\langle g\rangle| = o(g)$. By Lagrange's theorem, $|\langle g\rangle|||G|$. Hence $o(g)||G|$. ■

Euler's Theorem:

$\gcd(a, n) = 1 \implies a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n) = |\{k \in [1, ..., n] | \gcd(k, n) = 1\}|$

Proof. Let $G = \mathbb{Z}_n^\times$. Recall that

$$\mathbb{Z}_n^\times = \{[r]_n | 1 \leq r \leq n, \gcd(r, n) = 1\}.$$

Then $|G| = \phi(n)$. Now

$$\gcd(a, n) = 1 \implies [a]_n \in G \implies [a]_n^{|G|} = [1]_n.$$

But we then also have

$$[a^{\phi(n)}]_n = [a]_n^{|G|} = [1]_n$$

since $|G| = \phi(n)$. We conclude that $a^{\phi(n)} \equiv 1 \pmod{n}$. ■

Corollary:

(Fermat's little theorem) If p is a prime, then

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

Proof. Nothing to prove if $a \equiv 0 \pmod{p}$. If $a \not\equiv 0 \pmod{p}$, then $\gcd(a, p) = 1$. By Euler's theorem,

$$a^{\phi(p)} \equiv 1 \pmod{p} \implies a^{p-1} \equiv 1 \pmod{p} \implies a^p \equiv a \pmod{p}.$$

This proves the corollary. ■

Proposition:

Suppose G is a group, and $K \leq H \leq G$ are subgroups. Then $[G : K] = [G : H][H : K]$ if both sides are finite.

Remark: If $|G| < \infty$, then $[G : K] = |G|/|K|$ and $[G : H] = |G|/|H|$ and $[H : K] = |H|/|K|$, and the equality is clear.

Proof. Suppose that

$$G/H = \{g_i H | i \in I\}$$

$$H/K = \{h_j K | j \in J\}$$

and $g_i H \neq g_{i'} H$ if $i \neq i'$ and $h_j K \neq h_{j'} K$ if $j \neq j'$. We claim that

$$f : G/H \times H/K \to G/K, \;\; f(g_i H, h_j K) = g_i h_j K$$

is a bijection. If this were true, then one side of the equality is finite if and only if the other side is finite. Of course if this claim is true we are done. We want to show that f is injective. Well we want to show that $f(g_i H, h_j K) = f(g_{i'} H, h_{j'} K)$ implies $(g_i H, h_j K) = (g_{i'} H, h_{j'} K)$. The proof will be done next time.

(Added by Brian) Now it's 6:51 pm in 64 degrees and I can't wait until next time to see the proof. So let me try to prove it. We have

$$f(g_i H, h_j K) = f(g_{i'} H, h_{j'} K) \iff g_i h_j K = g_{i'} h_{j'} K$$

$$\iff (g_{i'} h_{j'})^{-1} g_i h_j \in K \iff h_{j'}^{-1} g_{i'}^{-1} g_i h_j \in K \subset H$$

$$\iff g_{i'}^{-1} g_i \in H \iff g_i H = g_{i'} H.$$

Also by the above we have

$$h_{j'}^{-1} h_j \in K \implies h_j K = h_{j'} K.$$

Hence, f is an injection. To show that f is a surjection, simply observe that if $g \in G$ is given, then

$$f(gH, eK) = (ge)K = gK.$$

Hence $[G : K] = [G : H][H : K]$. ■

Lecture 11/14/2019 (Week 7 Thursday):

Recall the following proposition:

Proposition:

Suppose G is a group, and $K \subset H \subset G$ are subgroups. Then

$$[G : K] = [G : H][H : K].$$

Proof. Let

$$G/H = \{g_i H | i \in I\}$$

$$H/K = \{h_j K | j \in J\}$$

with $g_i H \neq g_{i'} H$ if $i \neq i'$, and $h_j K \neq h_{j'} K$ if $j \neq j'$. We define

$$f : G/H \times H/K \to G/K$$

by $f(g_i H, h_j K) = g_i h_j K$. We claim that f is a bijection. First, we show that f is injective. Well,

$$g_i h_j K = g_{i'} h_{j'} K \implies (g_i h_j)^{-1}(g_{i'} h_{j'}) \in K$$

$$\implies h_j^{-1} g_i^{-1} g_{i'} h_{j'} \in K \ \ (\star)$$

$$\implies g_i^{-1} g_{i'} \in h_j H h_{j'}^{-1} = H.$$

Hence $g_i H = g_{i'} H \implies i = i'$ $(\star\star)$. By $(\star)$ and $(\star\star)$ we have $h_j^{-1} h_{j'} \in K \implies h_j K = h_{j'} K \implies j = j'$. Hence f is injective.

Next we show that f is surjective. For all $g \in G$, we want to find i and j such that $gK = g_i h_j K$. Since $gH \in G/H$, for some $i \in I$ we have $gH = g_i H$. Hence $g_i^{-1} g \in H$, and $(g_i^{-1} g)K \in H/K$. So for some $j \in J$ we have

$$g_i^{-1} g K = h_j K \implies gK = g_i h_j K$$

as desired. Hence f is a bijection, and the proposition follows. ■

Definition:

Suppose H is a subgroup of G. We say H is a normal subgroup if $\forall g \in G$,

$$gH = Hg.$$

Lemma:

Suppose that H is a subgroup of G. Then the following are equivalent:
(1) H is a normal subgroup
(2) $\forall g \in G, gHg^{-1} \subset H$
(3) $\forall g \in G, gHg^{-1} = H$.

Proof. (1) $\implies$ (2) and (3). If H is a normal subgroup, then $\forall g \in G$, $gH = Hg$, and thus

$$(gH)g^{-1} = (Hg)g^{-1} = H.$$

Now we show that (2) $\implies$ (3). $\forall g \in G$, $gHg^{-1} \subset H$ (Fact a). And so for g^{-1} we obtain

$$g^{-1}H(g^{-1})^{-1} \subset H \implies g^{-1}Hg \subset H.$$

From here, you get that $g(g^{-1}Hg)g^{-1} \subset gHg^{-1}$, and so $H \subset gHg^{-1}$ (Fact b). Facts a and b together imply that $\forall g \in G$, $gHg^{-1} = H$.

Now we show that (3) $\implies$ (1). $\forall g \in G$, $gHg^{-1} = H$

$$\implies (gHg^{-1})g = Hg$$

$$\implies gH = Hg$$

as desired. ■

Lemma:

Suppose that $\phi : G_1 \to G_2$ is a group homomorphism. Then $\ker(\phi)$ is a normal subgroup.

Proof. We need to show that $\forall g \in G$, we have

$$g \ker(\phi) g^{-1} \subset \ker(\phi).$$

That is, we have to show that $\forall g \in G$, $\forall x \in \ker(\phi)$, we have $gxg^{-1} \in \ker(\phi)$. Now

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1})$$
$$= \phi(g)1_{G_2}\phi(g)^{-1} = 1_{G_2}.$$

Hence $gxg^{-1} \in \ker(\phi)$. ■

Remark: $\text{Im}(\phi)$ is not necessarily a normal subgroup.

Example:

In S_3 consider $H = \{\mathrm{id}, (1\ \ 2)\} \leq S_3$. We claim that H is not a normal subgroup. Notice that

$$(2\ \ 3)(1\ \ 2)(2\ \ 3) = \ (1\ \ 3) \notin H.$$

This means that

$$(2\ \ 3)H(2\ \ 3)^{-1} \not\subset H.$$

Example:

(Added by Brian) Consider the group homomorphism $\phi : \mathbb{Z}/2\mathbb{Z} \to S_3$ given by $\phi(1) = (1\ \ 2)$ and $\phi(0) = \mathrm{id}$. Then since

$$(1\ \ 3)\underbrace{(1\ \ 2)}_{\in \mathrm{Im}(\phi)}(1\ \ 3) = (2\ \ 3) \notin \mathrm{Im}(\phi)$$

we conclude that $\mathrm{Im}(\phi)$ is not a normal subgroup.

Example:

$A_n \lhd S_n$. We prove this as follows. Define $\mathrm{sgn}(\sigma) = 1$ if σ is even, and -1 if σ is odd. Notice that $\mathrm{sgn}(\sigma) = (-1)^{n_\sigma}$, where σ can be written as a product of n_σ transpositions. Now $\forall \sigma_1, \sigma_2 \in S_n$, write

$$\sigma_1 = \tau_1 \cdots \tau_{n_{\sigma_1}}$$

$$\sigma_2 = \tau_1' \cdots \tau_{n_{\sigma_2}}'$$

where τ_i and τ_j' are transpositions. Then

$$\sigma_1\sigma_2$$

has $n_{\sigma_1} + n_{\sigma_2}$ transpositions. Hence

$$\mathrm{sgn}(\sigma_1)\mathrm{sgn}(\sigma_2) = (-1)^{n_{\sigma_1}}(-1)^{n_{\sigma_2}} = \mathrm{sgn}(\sigma_1\sigma_2).$$

Hence sgn is a group homomorphism, and $\ker(\mathrm{sgn}) = A_n$ is a normal subgroup of S_n. ■

Definition:

We say that G is a *simple* group if $G \neq \{1\}$ and $N \lhd G \implies N = \{1\}$, or $N = G$.

Example:

$[S_n : A_n] =?$ Well, observe that $S_n = A_n \cup (1\ 2)A_n$. Why is this true? Because if $\sigma \in S_n$ is odd, then $(1\ 2)\sigma$ is even, so $(1\ 2)\sigma \in A_n$, and finally $\sigma \in (1\ 2)A_n$. If $\sigma \in S_n$ is even, then $\sigma \in A_n$. Hence, we have $[S_n : A_n] = 2$.

Example:

If $H \leq G$ and $[G : H] = 2$, then $H \lhd G$. Indeed,

$$[G : H] = 2 \implies \exists g_0 \in G$$

such that

$$G = H \bigsqcup g_0 H.$$

So $\forall g \in G$, $gH = H$ or $gH = g_0 H$. So $\forall g \in G \backslash H$, $gH = g_0 H$. So $G \backslash H = g_0 H = gH$ if $g \in G \backslash H$.

Also, there exists $g_1 \in G$ such that $G = H \bigsqcup H g_1$. By a similar argument we have $G \backslash H = H g_1 = Hg$, for all $g \in G \backslash H$. Hence

$$\forall g \in G \backslash H, gH = G \backslash H = Hg$$

$$\forall g \in H, gH = H = Hg.$$

This completes the argument.

Example:

The center of G, $Z(G) \lhd G$. We have to show that $\forall g \in G$, $\forall x \in Z(G)$, we have

$$gxg^{-1} \in Z(G).$$

But for all $x \in Z(G)$, we have $gxg^{-1} = gg^{-1}x = x \in Z(G)$.

Definition:

Suppose that $H, K \leq G$. Let

$$HK = \{hk | h \in H, k \in K\}.$$

This is called the *product set* of H, K. HK is not necessarily a subgroup.

Lemma:

Suppose that $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.

This is the midterm cutoff.

Lecture 11/19/2019 (Week 8 Tuesday):

Recall: Suppose H and K are two subgroups of G. Define $HK = \{hk | h \in H, k \in K\}$.

Theorem:

HK is a subgroup if and only if $HK = KH$.

Proof. ($\implies$) Assume that HK is a subgroup. We show that $HK \subset KH$ and $KH \subset HK$. Now for all $h \in H$, $k \in K$, we have $hk \in HK$.

$$\implies (hk)^{-1} \in HK \implies k^{-1}h^{-1} \in HK$$

$$\text{Let } k^{-1}h^{-1} = h'k' \text{ for some } h' \in H, k' \in K$$

$$\implies hk = (h'k')^{-1} = (k')^{-1}(h')^{-1} \in KH.$$

Hence $HK \subset KH$. Now for all $k \in K$ and $h \in H$, our goal is to show that $kh \in HK$. It suffices to show that $(kh)^{-1} = h^{-1}k^{-1} \in HK$

$$\impliedby k^{-1} \in K, h^{-1} \in H.$$

Hence $KH \subset HK$.

($\impliedby$) We know $1 \in H \cap K$, hence $1 \cdot 1 = 1 \in HK$. Now for all $h \in H$ and $k \in K$, we have $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$, so HK is closed under taking inverses. Finally, let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$(h_1k_1)(h_2k_2) = h_1 \underbrace{(k_1h_2)}_{\in KH = HK} k_2.$$

Writing $k_1h_2 = h'k'$ for some $h' \in H$ and $k' \in K$, we have

$$h_1(h'k')k_2 = \underbrace{(h_1h')}_{\in H}\underbrace{(k'k_2)}_{\in K}.$$

This completes the proof. ■

Corollary:

Suppose $H \lhd G$ and $K \leq G$. Then $HK = KH \leq G$.

Proof. We have $HK = \{hk | h \in H, k \in K\} =$

$$\bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH.$$

Hence HK is a subgroup. Alternative proof: Notice that

$$hk = k(k^{-1}hk) \in KH$$

as H is closed under conjugation. Similarly,

$$kh = (khk^{-1})k \in HK.$$

Corollary:

If $H, K \lhd G$, then $HK \lhd G$.

Proof. We have already proved that $HK \leq G$. So it is enough to show that $\forall g \in G$,

$$g(HK)g^{-1} \subset HK.$$

For every $h \in H$ and $k \in K$, we have

$$g(hk)g^{-1} = \underbrace{(ghg^{-1})}_{\in H}\underbrace{(gkg^{-1})}_{\in K} \in HK$$

because $H, K \lhd G$. Hence HK is a normal subgroup. ■

Example:

(Quick example to foster understanding of cartesian product of groups) Find the order of $(1, 2) \in \mathbb{Z}_3 \times \mathbb{Z}_5^*$. Well, the neutral element is $(0, 1)$, and that $(1, 2)^n = (n, 2^n)$. Set

$$(n, 2^n) = (0, 1).$$

Notice that $[n]_3 = [0]_3 \implies 3|n$. Also we need $2^n \equiv 1 \pmod 5$. Hence $2^n \equiv 1 \pmod 5 \iff 4|n$. We conclude that $n = 12$. Since this group has order 12, this group is cyclic, and thus isomorphic to $\mathbb{Z}_{12}$.

Proposition:

(1) Suppose that $H, K \lhd G$. Then $H \cap K \lhd G$.
(2) Suppose that $H, K \lhd G$ with $H \cap K = \{1\}$. Then $HK \cong H \times K$.

Proof. (1) We have already proved that the intersection of two subgroups is a subgroup. So it is enough to show that $\forall g \in G$, we have

$$g(H \cap K)g^{-1} \subset H \cap K.$$

Now if $x \in H \cap K$, then we know

$$x \in H \implies \forall g \in G, gxg^{-1} \in H$$

$$x \in K \implies \forall g \in G, gxg^{-1} \in K$$

since H, K are normal. Hence $gxg^{-1} \in H \cap K$ and we conclude $g(H \cap K)g^{-1} \subset H \cap K$.

(2) Let $[h, k] = hkh^{-1}k^{-1}$ be the *commutator* of h and k. Notice that $[h, k] = 1 \iff hk = kh$. Now we have

$$[h, k] = \underbrace{(hkh^{-1})}_{\in K; K \lhd G} k^{-1} \in K \text{ as } K \leq G$$

$$h \underbrace{(kh^{-1}k^{-1})}_{\in H; H \lhd G} \in H \text{ as } H \leq G.$$

We conclude that $[h, k] \in H \cap K = \{1\}$. Hence $\forall h \in H, k \in K$, we have $[h, k] = 1 \iff hk = kh$.

Now define $f : H \times K \to HK$, $f(h, k) := hk$. We claim that this gives an isomorphism.

(f is a homomorphism) $f((h_1, k_1)(h_2, k_2)) \stackrel{?}{=} f(h_1, k_1)f(h_2, k_2)$. The LHS equals

$$f(h_1h_2, k_1k_2) = (h_1h_2)(k_1k_2).$$

The RHS equals

$$(h_1k_1)(h_2k_2) = \underbrace{h_1(k_1h_2)k_2 = h_1h_2k_1k_2}_{\text{because } [h_2,k_1]=1}.$$

(f is injective) Assume that $f(h, k) = f(h', k')$. Then

$$\implies hk = h'k' \implies \underbrace{(h')^{-1}h}_{\in H} = \underbrace{k'k^{-1}}_{\in K}.$$

Hence $(h')^{-1}h = e = k'k^{-1}$, and we conclude that $h' = h$ and $k' = k$, and finally $(h, k) = (h', k')$.

(f is surjective) By definition of HK we have that

$$HK = \{hk | h \in H, k \in K\} = \operatorname{Im}(f).$$

Hence f is an isomorphism. ■

Corollary:

If $H, K \lhd G$ and that $\gcd(|H|, |K|) = 1$, then $HK \cong H \times K$.

Proof. It is enough to show that $H \cap K = \{1\}$. By Lagrange's theorem,

$$|H \cap K| \Big| |H|$$

$$|H \cap K| \Big| |K|.$$

From the above and the fact that $\gcd(|H|, |K|) = 1$, we have $|H \cap K| = 1$. ■

Chinese Remainder Theorem:

Suppose that $\gcd(n, m) = 1$. Then

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}.$$

Proof. $\mathbb{Z}_{mn}$ has a subgroup H of order m. $\mathbb{Z}_{mn}$ also has a subgroup K of order n. Since $\mathbb{Z}_{mn}$ is abelian, $H, K \lhd \mathbb{Z}_{mn}$. Also $\gcd(|H|, |K|) = \gcd(m, n) = 1$. Hence $H \times K \cong H + K$. Any subgroup of a cyclic group is cyclic. So H and K are cyclic. Now $H \cong \mathbb{Z}_m$ and $K \cong \mathbb{Z}_n$. So

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong H + K \leq \mathbb{Z}_{mn}.$$

In particular $|H+K| = mn$, so $H+K = \mathbb{Z}_{mn}$. We conclude that $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. ■

Remark: Compare this with the Chinese remainder theorem from earlier in class. Explicitly, an isomorphism is given by $f : \mathbb{Z}_{mn} \to \mathbb{Z}_n \times \mathbb{Z}_m$, $f([k]_{mn}) = ([k]_m, [k]_n)$.

Example:

Let $n = 2$ and $m = 3$. We want to find a $x \in \mathbb{Z}_{2\times 3} = \mathbb{Z}_6$ such that $x \equiv 0 \pmod 2$ and $x \equiv 2 \pmod 3$. Setting f as in the above remark, we see that if $x = [2]_6$, then $f([2]_6) = ([0]_2, [2]_3)$ will work.

Lecture 11/21/2019 (Week 8 Thursday):

> **Proposition:**
>
> Let $H \leq G$. Define an operation on the left cosets of H as $g_1H \cdot g_2H = g_1g_2H$. Then this operation is well-defined if and only if H is a normal subgroup.

Proof. ($\Longrightarrow$) If the operation is well-defined, then

$$H \cdot gH = gH.$$

Since $hH = H$ and $gH = gH$, we also have

$$hH \cdot gH = (hg)H.$$

Hence $gH = (hg)H$ for every $h \in H$. Which means that for all $h \in H$, we have $g^{-1}hg \in H$. Hence $\forall g \in G$, $g^{-1}Hg \subset H$, so $H \lhd G$.

($\Longleftarrow$) Suppose that $g_1H = g_1'H$ and $g_2H = g_2'H$. We want to show that $(g_1g_2)H = (g_1'g_2')H$. Now

$$g_1H = g_1'H \implies g_1^{-1}g_1' \in H$$

$$g_2H = g_2'H \implies g_2^{-1}g_2' \in H.$$

Our goal is to show that $(g_1g_2)^{-1}(g_1'g_2') \in H \iff g_2^{-1}g_1^{-1}g_1'g_2' \in H$. Now

$$g_2^{-1}g_1^{-1}g_1'g_2' = \underbrace{g_2^{-1}g_2'}_{\in H}\underbrace{g_2'^{-1}g_1^{-1}g_1'g_2'}_{\in H; H \lhd G} \in H$$

as H is a subgroup. ■

> **Theorem:**
>
> Suppose $N \lhd G$. Then
> (1) $(G/N, \cdot)$ is a group
> (2) $\pi : G \to G/N$, $\pi(g) = gN$ is a surjective group homomorphism and we have $\ker(\pi) = N$.

π is called the natural projection map from G to the factor group G/N.

Proof. (1) (Associativity) We have $(g_1N \cdot g_2N) \cdot g_3N$

$$= (g_1g_2)g_3N$$

$$= g_1(g_2g_3)N$$

$$= g_1N \cdot (g_2N \cdot g_3N).$$

(2) (Neutral element) $(gN) \cdot N = N \cdot gN = gN$.

(3) (Inverse element) $(gN)(g^{-1}N) = (gg^{-1})N = N = (g^{-1}N)(gN)$.

Lecture 11/26/2019 (Week 9 Tuesday):

Remark: There were 9 students who got ≥ 40, 6 students who got $[36, 40)$. These are the A range scores. Now, $[26, 36)$ is B range. Any score lower than 16 is alarming. The first quartile is 38. The median is 30. The third quartile is 19.

Definition:

Let $H \leq G$. Define an operation on the left cosets of H as $(g_1H)(g_2H) := g_1g_2H$. This operation is well-defined iff $H \lhd G$.

Proposition:

Suppose $N \lhd G$. Then
(a) $(G/N, \cdot)$ is a group.
(b) $\pi : G \to G/N$ given by $\pi(g) = gN$ is a group homomorphism.
(c) π is surjective, and $\ker(\pi) = N$.

Proof. (b) We have

$$\begin{aligned}\pi(g_1g_2) &= (g_1g_2)N \\ &= (g_1N)(g_2N) = \pi(g_1)\pi(g_2).\end{aligned}$$

Hence π is a group homomorphism.

(c) We have $\mathrm{Im}(\pi) = \{\pi(g) | g \in G\}$

$$= \{gN | g \in G\} = G/N.$$

Hence π is surjective. Now $g \in \ker(\pi)$ iff $\pi(g) = N$ iff $gN = N$ iff $g \in N$. Hence $\ker(\pi) = N$. ■

Corollary:

In particular, $N \lhd G$ if and only if there is a group homomorphism $\theta : G \to H$ such that $N = \ker(\theta)$.

Theorem (1st Isomorphism Theorem):

Suppose $\theta : G \to H$ is a group homomorphism. Then $\overline{\theta} : G/\ker(\theta) \to \mathrm{Im}(\theta)$ given by $\overline{\theta}(g\ker(\theta)) = \theta(g)$ is an isomorphism. Hence $G/\ker(\theta) \cong \mathrm{Im}(\theta)$.

Proof. ($\overline{\theta}$ is well-defined) Suppose that $g_1\ker(\theta) = g_2\ker(\theta)$. Then $g_1^{-1}g_2 \in \ker(\theta)$. Hence

$$\theta(g_1^{-1}g_2) = e \implies \theta(g_1)^{-1}\theta(g_2) = e.$$

From this we deduce that $\theta(g_1) = \theta(g_2)$.

($\overline{\theta}$ is a group homomorphism) we have

$$\overline{\theta}((g_1\ker\theta)(g_2\ker\theta))) = \overline{\theta}(g_1g_2\ker(\theta)) = \theta(g_1g_2).$$

While,

$$\overline{\theta}(g_1\ker\theta)\overline{\theta}(g_2\ker\theta) = \theta(g_1)\theta(g_2).$$

Hence $\overline{\theta}$ is a group homomorphism because θ is a group homomorphism.

($\overline{\theta}$ is surjective) $\forall h \in \mathrm{Im}(\theta)$, there exists $g \in G$ such that $h = \theta(g)$. Hence $h = \overline{\theta}(g\ker\theta)$, which implies $h \in \mathrm{Im}(\overline{\theta})$. So $\overline{\theta}$ is surjective.

($\overline{\theta}$ is injective) We have

$$\overline{\theta}(g_1\ker\theta) = \overline{\theta}(g_2\ker\theta) \implies \theta(g_1) = \theta(g_2) \implies \theta(g_1)^{-1}\theta(g_2) = 1 \implies \theta(g_1^{-1}g_2) = 1$$

$$\implies g_1^{-1}g_2 \in \ker\theta \implies g_1\ker\theta = g_2\ker\theta.$$

This completes the proof. ■

We can summarize this information in a commuting diagram:

$$\begin{tikzcd}
g \arrow[d, mapsto] & G \arrow[r, "\theta"] \arrow[d] \arrow[rr, bend left, "\theta"] & \mathrm{Im}\theta \arrow[r, hook] & H \\
g\ker\theta & G/\ker\theta \arrow[ur, "\overline{\theta}"', "\sim"] & &
\end{tikzcd}$$

Example:

$\mathrm{Inn}(G) \cong G/Z(G)$. To prove this, recall that

$$c : G \to \mathrm{Aut}(G)$$

$$c(g) = c_g$$

(where $c_g(g') = gg'g^{-1}$) is a group homomorphism. Also $\mathrm{Im}(c) = \mathrm{Inn}(G)$. And we have $\ker(c) = Z(G)$ because

$$g \in \ker(c) \iff c(g) = \mathrm{id}$$

$$\iff \forall g', c_g(g') = g'$$

$$\forall g' \in G, gg'g^{-1} = g'$$

$$\iff \forall g' \in G, gg' = g'g \iff g \in Z(G).$$

So by the 1st isomorphism theorem $G/\ker(c) \cong \mathrm{Im}(c)$. This implies that $G/Z(G) \cong \mathrm{Inn}(G)$ as desired.

Example:

If $Z(G) = \{1\}$, then $G \cong \mathrm{Inn}(G)$. Indeed by the previous example,

$$G/Z(G) \cong \mathrm{Inn}(G).$$

Hence

$$\mathrm{Inn}(G) \cong G/\{1\} \cong G.$$

The last isomorphic relation follows because $\pi : G \to G/\{1\}$ given by $\pi(g) = g\{1\}$ is an isomorphism.

Example (continued):

As a result,

$$\mathrm{Inn}(S_n) \cong S_n \text{ if } n \geq 3.$$

Theorem (2nd Isomorphism Theorem):

Suppose G is a group and $N \lhd G$, $H \leq G$. Then

$$(HN)/N \cong H/(H \cap N).$$

Corollary:

$|HN| = |H||N|/|H \cap N|$.

Proof. By the 2nd IT we have

$$|(HN)/N| = |H/(H \cap N)|.$$

Now by Lagrange's theorem we have

$$|HN|/|N| = |H|/|H \cap N|.$$

Hence the result follows. ■

Remark: This equality holds even if N is not normal.

Proof of Theorem. Consider $f : H \to (HN)/N$ given by $f(h) = hN$. Since $h \in H \subset HN$, $hN \in (HN)/N$. Hence f is a well-defined function.

(f is a group homomorphism) We have

$$f(h_1 h_2) = h_1 h_2 N = (h_1 N)(h_2 N) = f(h_1) f(h_2).$$

(Finding kernel of f) Now, $h \in \ker(f) \iff f(h) = N \iff hN = N \iff h \in N$. Hence $h \in \ker(f) \iff h \in N \cap H$. So $\ker(f) = N \cap H$.

(Finding image of f) We have $\operatorname{Im}(f) = \{f(h) | h \in H\} = \{hN | h \in H\} \stackrel{?}{=} HN/N$. (Notice that $N \lhd G$ and $H \leq G$, so we get $HN \leq G$. Also $N \lhd HN$. So $(HN)/N$ makes sense and it is a group.)

(f is onto) An element of $(HN)/N$ is of the form $(hn)N$ for some $h \in H$ and $n \in N$. However, notice that $hnN = hN$ as $h^{-1}(hn) = n \in N$. This implies that $hnN = f(h)$, so f is onto.

(Applying 1st IT) By the 1st isomorphism theorem, we have

$$H/\ker(f) \cong \operatorname{Im}(f)$$

(with isomorphism given by $h(\ker f) \mapsto f(h)$. Hence using previous results,

$$H/(H \cap N) \cong (HN)/N.$$

The isomorphism is given by $h(H \cap N) \mapsto hN$. ■

Theorem (3rd Isomorphism Theorem):

Suppose $N \lhd G$, $H \lhd G$, $N \leq H$. Then

$$\frac{(G/N)}{(H/N)} \cong G/H.$$

Proof. Consider $f : G/N \to G/H$ given by $f(gN) = gH$.

(f is well defined) If $g_1N = g_2N$, then $g_1^{-1}g_2 \in N \subset H$, so $g_1^{-1}g_2 \in H$. This implies that $g_1H = g_2H$.

(f is a group homomorphism) We have

$$f((g_1N)(g_2N)) = f(g_1g_2N) = g_1g_2H$$

$$= (g_1H)(g_2H) = f(g_1N)f(g_2N).$$

(Finding $\mathrm{Im}(f)$, and showing f is onto) We have

$$\mathrm{Im}(f) = \{f(gN)|g \in G\} = \{gH|g \in G\} = G/H.$$

(Finding $\ker(f)$) We have $gN \in \ker(f)$

$$\iff f(gN) = H.$$

We will finish the proof next time.

Lecture 12/3/2019 (Week 10 Tuesday):

Recall the following theorem:

Third Isomorphism Theorem:

$H, K \lhd G$ and $K \leq H$ implies that

$$\frac{G/K}{H/K} \cong G/H.$$

Proof. Consider $f : G/K \to G/H$ given by $f(gK) = gH$. We have shown that f is a well-defined onto group homomorphism. By the 1st IT, we know that

$$\frac{G/K}{\ker(f)} \cong \mathrm{Im}(f).$$

Now $gK \in \ker(f) \iff f(gK) = H \iff gH = H \iff g \in H$. Hence $gK \in \ker(f) \iff gK \in H/K$. Hence $H/K = \ker(f)$. This proves the theorem. ∎

Corollary:

By the 1st isomorphism theorem,

$$\overline{f} : \frac{G/K}{H/K} \to G/H$$

$$\overline{f}((gK)H/K) = gH$$

is an isomorphism.

Recall: Consider subgroups of cyclic groups. Suppose C_n is a finite cyclic group of order n. Then

$$d|n \iff \exists! \text{ subgroup of order } d.$$

If $C_n = \langle g \rangle$, then the unique subgroup of order d is $\langle g^{n/d} \rangle$.

Theorem (Correspondence Theorem):

Suppose that $N \lhd G$. Then there is a bijection between the following sets:

$$\{\text{subgroups of } G/N\} \overset{\theta}{\leftarrow} \{H | H \leq G, N \subset H\}$$

given by $H/N \overset{\theta}{\leftarrow} H$. Moreover θ induces a bijection between

$$\{\text{normal subgroups of } G/N\} \leftarrow \{H | H \lhd G, N \subset H\}.$$

Remark: If H is a normal subgroup in G, then H/N is a normal subgroup in G/N, and vice versa.

Proof. Suppose $\overline{H}$ is a subgroup of G/N. Recall that $\pi : G \to G/N$, $\pi(g) = gN$ is an onto group homomorphism. Let $H := \pi^{-1}(\overline{H})$. (If $\overline{H} = H/N$, then $gN \in \overline{H} \iff g \in H$.)

We claim that $H \leq G$. We check the following.
(1) Since $\overline{H}$ is a subgroup, it contains the identity. And the preimage of the identity under a group homomorphism does contain the identity.
(2) If $h \in H$, then $\pi(h) \in \overline{H}$. Since $\overline{H}$ is a subgroup, $\pi(h)^{-1} \in \overline{H} \implies \pi(h^{-1}) \in \overline{H}$. Hence $h^{-1} \in \pi^{-1}(\overline{H})$.
(3) If $h_1, h_2 \in H$, then $\pi(h_1), \pi(h_2) \in \overline{H}$. Hence

$$\pi(h_1 h_2) = \pi(h_1)\pi(h_2) \in \overline{H}$$

as desired.

Since π is onto, we have $\overline{H} = \pi(\pi^{-1}(\overline{H})) = \pi(H) = \{hN | h \in H\} = H/N$.

Notice that $\pi^{-1}(1 \cdot N) = N$, so $1 \cdot N \in \overline{H}$. Hence $N \subset \pi^{-1}(\overline{H}) \implies N \subset H$. This implies that θ is onto.

Next, θ is an injection. We want to show that if $H_i \leq G$ and $N \subset H_i$, then $\theta(H_1) = \theta(H_2) \implies H_1 = H_2$. Now $\forall h_1 \in H_1$, (we know $H_1/N = H_2/N$) we have $h_1 N \in H_2/N$. This means that $\exists h_2 \in H_2$ such that $h_1 N = h_2 N$. Hence $h_2^{-1} h_1 \in N \subset H_2$. Hence $h_1 \in H_2$. So $H_1 \subset H_2$. By a similar argument, $H_2 \subset H_1$. Hence $H_1 = H_2$.

Quick remark: as part of the 3rd IT, if $H \lhd G$, then $\theta(H) \lhd G/N$.

So it remains to show that if $H/N \lhd G/N$ for some $N \subset H \leq G$, then $H \lhd G$. For al $g \in G$, we have to show that $gHg^{-1} \subset H$. Since $H/N \lhd G/N$, we have

$$(gN)(H/N)(gN)^{-1} = H/N \implies \pi(g)\pi(H)\pi(g)^{-1} = H/N \implies \pi(gHg^{-1}) = H/N.$$

Since $N \subset H$, we have $gNg^{-1} \subset gHg^{-1} \implies N \subset gHg^{-1}$ as $N \lhd G$. Now we have $N \subset H, gHg^{-1} \leq G$, and $\pi(H) = \pi(gHg^{-1})$. Hence by the first part $H = gHg^{-1}$.

Example:

We claim that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Indeed, $f : \mathbb{Z} \to \mathbb{Z}_n$ given by $f(a) = [a]_n$ is an onto group homomorphism with $\ker(f) = n\mathbb{Z}$. Then we are done by the first isomorphism theorem.

Example:

$\mathbb{R}/\mathbb{Z} \cong S^1 = \{z \in \mathbb{C} \big| |z| = 1\}$. Indeed, if $f : \mathbb{R} \to S^1$, $f(x) = e^{2\pi i x}$, then $\ker(f) = \mathbb{Z}$. Then we are done again by the first isomorphism theorem.

Example:

Let $a, b \in \mathbb{Z}$. Then $(\mathbb{Z} \times \mathbb{Z})/\langle (a,b) \rangle$ is cyclic iff $\gcd(a,b) = 1$.

$(\impliedby)$ For some $r, s \in \mathbb{Z}$ we have $ar + bs = 1$. We want to show that $(\mathbb{Z} \times \mathbb{Z})/\langle (a,b) \rangle \cong \mathbb{Z}$. To this end, we want to find a map $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ that is onto, with $\ker(f) = \langle (a,b) \rangle$. Now, any group homomorphism $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is of the form $f(x,y) = cx + dy$ for some $c, d \in \mathbb{Z}$ (indeed $f(x,y) = f(x(1,0) + y(0,1)) = xf(1,0) + yf(0,1)$). Will continue next time.

Lecture 12/5/2019 (Week 10 Thursday):

Group Actions

Definition:

Suppose G is a group and X is a set. A function $m : G \times X \to X$ is called a group action (or we say G acts on X with m, $G \curvearrowright X$), if
(1) $\forall x \in X$, $m(1_G, x) = x$;
(2) $m(g_1, m(g_2, x)) = m(g_1 g_2, x)$.
We often write $g \cdot x$ instead.

Meta-example:

Let X be an object. Recall that $\mathrm{Symm}(X)$ is the set of a functions $X \to X$ that are bijections and preserves properties of X. We have also discussed that $(\mathrm{Symm}(X), \circ)$ is a group. We may define a group action $\mathrm{Symm}(X) \curvearrowright X$ by $f \cdot x := f(x)$.

Example:

Consider $S_n \curvearrowright \{1, 2, ..., n\}$ by $\sigma \cdot i = \sigma(i)$.

Example:

Consider $GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ by $g \cdot v := gv$.

Example:

Consider $SL_2(\mathbb{R}) \curvearrowright \mathcal{H}$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

(Where $\mathcal{H} = \{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$). Side remark: these matrices don't change the length of a curve.

Example:

Consider $G \curvearrowright G/H$ by left translations:

$$g \cdot (g'H) = gg'H.$$

This is indeed an action because $1_G \cdot (g'H) = g'H$, and that

$$\begin{aligned} g_1 \cdot (g_2 \cdot (g'H)) = g \cdot ((g_2 g')H) &= (g_1(g_2 g'))H \\ &= (g_1 g_2) g' H. \end{aligned}$$

Example:

Consider $G \curvearrowright G$ by left translations:

$$g \cdot g' := gg'.$$

Example:

Consider $G \curvearrowright G$ by conjugation:

$$g \cdot g' := gg'g^{-1}.$$

This is indeed an action because $1_G \cdot g' = 1_G g' 1_G^{-1} = g'$, and that $g_1 \cdot (g_2 \cdot g') = (g_1 g_2) g'$ (check).

Example:

Consider $G \curvearrowright X$. Let $V := \{f : X \to \mathbb{C} | f \text{ is a function}\}$. Then G acts on V by $g \cdot f : X \to \mathbb{C}$,

$$(g \cdot f)(x) := f(g^{-1}x).$$

This is a group action as

$$(1_G \cdot f)(x) = f(1_G^{-1}x) = f(x).$$

And that

$$(g_1 \cdot (g_2 \cdot f))(x) = (g_2 \cdot f)(g_1^{-1}x) = f(g_2^{-1}g_1^{-1}x)$$

$$= f((g_1g_2)^{-1}x) = ((g_1g_2) \cdot f)(x).$$

We remark that V is a vector space. Notice also that this a linear action, as

$$g \cdot (f_1 + f_2) = g \cdot f_1 + g \cdot f_2.$$

Definition:

Suppose $G \curvearrowright X$. The *orbit* of $x \in X$ is $G \cdot x := \{g \cdot x | g \in G\}$.

Example:

Suppose that $H \leq G$ and $H \curvearrowright G$ by left-translations: $h \cdot g = hg$. Then the orbit of g is Hg. We have seen that $\{Hg | g \in G\}$ is a partition of G, and we denoted this by $H \backslash G$.

Definition:

Let $G \curvearrowright X$. We let $G \backslash X = \{G \cdot x | x \in X\}$.

Theorem:

$G \backslash X$ is a partition of X.

Lemma:

TFAE:

(1) $G \cdot x = G \cdot y$
(2) $y \in G \cdot x$
(3) $G \cdot x \cap G \cdot y \neq \varnothing$.

Proof. (1) $\implies$ (2) since $y = 1_G \cdot y \in G \cdot y = G \cdot x$. Now (2) $\implies$ (1) because

$$y \in G \cdot x \implies y = g_0 \cdot x \text{ for some } g_0 \in G.$$

Now $G \cdot y \subset G \cdot x$ because $\forall g \in G$, $g \cdot y = g \cdot (g_0 \cdot x) = (gg_0) \cdot x \in G_x$. Also $g_0^{-1} \cdot y = g_0^{-1} \cdot (g_0 \cdot x) = (g_0^{-1} g_0) \cdot x = 1_G \cdot x = x$. So by a similarly argument $G \cdot x \subset G \cdot y$. Hence $G \cdot x = G \cdot y$.

(1) $\implies$ (3) because $x \in G \cdot x = G \cdot y$ implies that $x \in G_x \cap G_y$

(3) $\implies$ (1) because if $z \in G \cdot x \cap G \cdot y$, then since $z \in G \cdot x$, $G \cdot z = G \cdot x$. Similarly $G \cdot z = G \cdot y$. ■

Proof of Theorem. We have already proved that distinct orbits are disjoint. So it remains to show that

$$\bigcup_{x \in X} G \cdot x = X$$

but $\forall x \in X$, $x \in G \cdot x$. Hence $x \in \bigcup_{x' \in X} G \cdot x'$. ■

Definition:

Let $G \curvearrowright X$. For all $x \in X$, we define $G_x := \{g \in G | g \cdot x = x\}$. This is called the *stabilizer* of X.

Lemma:

Suppose that $G \curvearrowright X$. Then for all $p \in X$, G_p is a subgroup.

Proof. We have $1_G \cdot p = p \implies 1_G \in G_p$. Also if $g \in G_p$, then $g \cdot p = p \implies g^{-1} \cdot p = p$. Finally if $g_1, g_2 \in G_p$, then $g_1 \cdot (g_2 \cdot p) = g_1 \cdot p = p = (g_1 g_2)p$. Hence $g_1 g_2 \in G_p$. ■

The Orbit-Stabilizer Theorem:

Let $G \curvearrowright X$. Then $\theta : G/G_p \to G \cdot p$ given by $gG_p \mapsto g \cdot p$ is a bijection. In particular, $[G : G_p] = |G \cdot p|$.

Proof.

(θ is well-defined) $g_1G_p = g_2G_p$ implies that $g_2 = g_1g$ for some $g \in G_p$. So

$$g_2 \cdot p = (g_1g) \cdot p = g_1 \cdot (g \cdot p) = g_1 \cdot p.$$

(onto) We have $G \cdot p = \{g \cdot p | g \in G\} = \{\theta(gG_p) | g \in G\} = \mathrm{Im}(\theta)$.

(one-to-one) $\theta(g_1G_p) = \theta(g_2G_p) \implies g_1p = g_2p \implies p = g^{-1}g_2 \cdot p$. Hence $g^{-1}g_2 \in G_p$, which suffices to show that $g_1G_p = g_2G_p$. ■

Example:

Consider $G \curvearrowright G$ by conjugation. Then the orbit of g equals $\{g'gg'^{-1} | g' \in G\}$, which is called the conjugacy class of g. We denote this by $Cl(g)$. Now the stabilizer group of g is $\{g' \in G | g'gg'^{-1} = g\} = C_G(g)$. Hence by the Orbit-Stabilizer theorem,

$$\underbrace{|Cl(g)|}_{|G \cdot p|} = [G : C_G(g)]$$

Example:

We have $|Cl(g)| = 1 \iff C_G(g) = G \iff g \in Z(G)$. Suppose $\{g_1, ..., g_t\}$ are representatives from conjugacy classes that have at least 2 elements. Then

$$|G| = |Z(G)| + \sum_{i=1}^{t} |Cl(g_i)|$$

$$= |Z(G)| + \sum_{i=1}^{t} [G : C_G(g_i)].$$

This is the *class equation.*

Thereom:

If $|G| = p^n$, where p is a prime and G is a group, then $Z(G) \neq \{e\}$ and that $|Z(G)| \geq p$.

Proof. By the class equation,

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(g_i)]$$

and that the $[G : C_G(g_i)]$ is not one. Therefore by Lagrange's theorem, $[G : C_G(g_i)] = p^{n_i} \implies p|[G : C_G(g_i)]$. By the modding the class equation by p,

$$0 \equiv |Z(G)| \pmod{p}.$$

Hence $p||Z(G)|$, so $1 \leq |Z(G)|$, and moreover $|Z(G)| \geq p$. ■