MATH 4107: Abstract Algebra I

Frank Qiang
Instructor: Austin Christian

Georgia Institute of Technology
Fall 2023

Contents

Lecture 1

Aug. 21 — Binary Operations

Definition 2.15. A **binary operation** $\circ$ on a set A is a function $\circ : A \times A \to A$, i.e. for every element $(a, b) \in A \times A$, $a \circ b$ is an element of A.

Here are some examples:

1. $+$ is a binary operation on $\mathbb{R}$, i.e.

$$\begin{aligned} + : \mathbb{R} \times \mathbb{R} &\to \mathbb{R} \\ (a, b) &\mapsto a + b. \end{aligned}$$

   Similarly, $\times$ and $-$ are also binary operations on $\mathbb{R}$. However, $\div$ is not (but is on $\mathbb{R} \setminus \{0\}$).

2. $+$ and $\times$ are binary operations on $\mathbb{N}$, but $-$ and $\div$ are not! For example, we have

$$\begin{aligned} - : \mathbb{N} \times \mathbb{N} &\to \mathbb{Z} \\ (2, 4) &\mapsto -2 \notin \mathbb{N}. \end{aligned}$$

   This shows that $\mathbb{N}$ is not *closed* under $-$.

   However, in some sense, these are the "wrong" examples of binary operations. Here's the "right" example:

3. If X is any set, let

$$A = \{f \mid f : X \to X \text{ is a function}\}.$$

   Then function composition is a binary operation on A:

$$\begin{aligned} \circ : A \times A &\to A \\ (f, g) &\mapsto f \circ g. \end{aligned}$$

Note that functions are applied right-to-left,

$$X \xrightarrow{g} X \xrightarrow{f} X \qquad (f \circ g : X \to X)$$

i.e. $f \circ g$ means that g is applied first, then f.

Problem 2.17. Let $M(\mathbb{R})$ be the set of matrices (of any size) with real number entries. Is matrix addition a binary operation on $M(\mathbb{R})$? How about matrix multiplication? What if you restrict to square matrices of a fixed size $n \times n$?

Solution. Matrix addition is not a binary operation on $M(\mathbb{R})$ because the sum of two matrices of different sizes is not defined. A similar argument causes matrix multiplication to fail as well. However, if we restrict to $n \times n$ matrices, then both addition and matrix multiplication are well-defined and output another $n \times n$ matrix, so they are binary operations on $M_{n\times n}(\mathbb{R})$. □

Problem 2.18. Let A be a set. Determine whether $\cup$ (union) and $\cap$ (intersection) are binary operations on $\mathcal{P}(A)$ (i.e., the power set of A).

Solution. The union of two sets is a binary operation on $\mathcal{P}(A)$. To see this, take any $X, Y \in \mathcal{P}(A)$. Then for any $a \in X \cup Y$, $a \in X$ or $a \in Y$, so $a \in A$. So $X \cup Y \subseteq A$, and thus $X \cup Y \in \mathcal{P}(A)$.

Similarly, for intersections, take any $x \in X \cap Y$. Then $x \in X$ and $x \in Y$, so $x \in A$. Thus $X \cap Y \subseteq A$, and $X \cap Y \in \mathcal{P}(A)$. Note that $X \cup Y = \varnothing$ or $X \cap Y = \varnothing$ is fine, as $\varnothing \in \mathcal{P}(A)$. □

Lecture 2

Aug. 23 — Symmetries, Groups

Problem 2.20. Consider a square puzzle piece that fits perfectly into a square hole. Let R_4 be the set of net actions consisting of the rotations of the square by an appropriate amount so that it fits back into the hole. Assume we can tell the corners of the square apart from each other so that if the square has been rotated and put back into the hole we can notice the difference. Each net action is called a *symmetry* of the square.

(a) Describe all of the distinct symmetries in R_4. How many distinct symmetries are in R_4?

(b) Is composition of symmetries a binary operation on R_4?

Solution. (a) The distinct symmetries are the 0°, 90°, 180°, and 270° rotations, so there are 4 distinct symmetries in R_4. We can be sure that this includes every symmetry since a 360° rotation is the same as no rotation at all.

(b) The composition of symmetries is a binary operation on R_4. To see this, we can momentarily ignore the fact that we can tell each corner apart. Then a symmetry is exactly an action that takes the square back to itself. Thus, applying two symmetries in succession will still take the square back to itself, so their composition is also a symmetry on R_4. □

Problem 2.21. Consider a puzzle piece like the one in the previous problem, except this time, let's assume that the piece and the hole are an equilateral triangle. Let D_3 be the full set of symmetries that allow the triangle to fit back into the hole. In addition to rotations, we will also allow the triangle to be flipped over—called a reflection.

(a) Describe all of the distinct symmetries in D_3. How many distinct symmetries are in D_3?

(b) Is composition of symmetries a binary operation on D_3?

Solution. (a) The distinct symmetries are the 0°, 120°, and 240° rotations, each with or without a reflection. Thus there are 6 distinct symmetries in D_3.

(b) The composition of symmetries is a binary operation on D_3. We can label each vertex of the triangle with numbers and identify each state of the triangle with a permutation of the numbers. If we call the set of such states A, then we can realize symmetries as functions $f : A \to A$. From here, we know that the composition of symmetries is a binary operation since the composition of functions is a binary operation. □

Problem 2.23. Consider the set S_3 consisting of the net actions that permute the positions of three coins (without flipping them over) that are sitting side by side in a line. Assume that you can tell the coins apart.

(a) Write down all distinct net actions in S_3 using verbal descriptions. Some of these will be tricky to describe. How many distinct net actions are in S_3?

(b) Is composition of net actions a binary operation on S_3?

Solution. (a) The distinct net actions are:

1. Do nothing.
2. Swap the first and second elements.
3. Swap the second and third elements.
4. Swap the first and third elements.
5. Shift all elements to the right by one, with wraparound.
6. Shift all elements to the left by one, with wraparound.

So there are 6 total distinct net actions in S_3.

(b) We can similarly number each position with a number from 1 to 3, and define A to be the set of all permutations of the set $\{1,2,3\}$. Then we can realize net actions in S_3 as functions $f : A \to A$. Since function composition is a binary operation, the composition of actions in S_3 is a binary operation as well. □

Definition 2.25. Let A be a nonempty set and let $*$ be a binary operation on A.

(a) We say that $*$ is **associative** if $(a * b) * c = a * (b * c)$ for all $a, b, c \in A$.

(b) We say that $*$ is **commutative** if $a * b = b * a$ for all $a, b \in A$.

Problem 2.26. Provide an example of each of the following.

(a) A binary operation on a set that is commutative.

(b) A binary operation on a set that is not commutative.

Solution. (a) The usual multiplication on $\mathbb{R}$ is commutative.

(b) Matrix multiplication on $M_{n\times n}(\mathbb{R})$ is in general not commutative. For example,

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix},$$

but

$$\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 23 & 34 \\ 31 & 46 \end{pmatrix},$$

so these two matrices do not commute. □

Theorem 2.29. *If A is a nonempty set and F is the set of functions from A to A, then function composition is an associative binary operation on F.*

Proof. If $f, g : A \to A$, then we also have $f \circ g : A \to A$, so function composition is indeed a binary operation on F. Now we show that $\circ$ is associative. For this, first recall that

$$(f \circ g)(x) = f(g(x))$$

by definition. Then for any $f, g, h : A \to A$ and a point $x \in A$, we have

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x),.$$

Since $(f \circ g) \circ h$ and $f \circ (g \circ h)$ agree at every point, they must be equal. Hence $\circ$ is associative. □

Lecture 3

Aug. 28 — Groups

Definition 2.33. A **group** $(G, *)$ is a set G with a binary operation $* : G \times G \to G$ such that

0. G is closed under $*$,
1. the operation $*$ is associative,
2. *(existence of an identity)* there exists $e \in G$ such that for all $g \in G$, $e * g = g = g * e$.
3. *(existence of inverses)* for all $g \in G$, there exists $g' \in G$ such that $g' * g = e = g * g'$.

The *order* of a group G, denoted $|G|$, is the cardinality of the set G. We say that a group G is *abelian* if its binary operation $*$ is commutative.

Problem 2.34. Explain why Axiom 0 is unnecessary.

Solution. This is because we already specified that $*$ is a binary operation on G, so G must already be closed under $*$ by the definition of a binary operation. □

Problem 2.35. Verify that each of the following is a group under composition of actions and determine the order. Which of the groups are abelian?

(b) R_4 (see Problem 2.20)

Solution. (b) Let r_θ denote the rotation by θ degrees and $\circ$ be the binary operation on R_4, i.e.

$$r_\phi \circ r_\theta = r_{\phi+\theta}.$$

For associativity, define A to be the states that the square can be in, and then we can realize the actions in R_4 as functions $f : A \to A$. Then $\circ$ must be associative since function composition is associative. The identity element is r_0, since

$$r_0 \circ r_\theta = r_{0+\theta} = r_\theta = r_{\theta+0} = r_\theta \circ r_0$$

for any θ. For inverses, we propose that $r_\theta^{-1} = r_{360-\theta}$, since

$$r_{360-\theta} \circ r_\theta = r_{360-\theta+\theta} = r_0 = r_{\theta+360-\theta} = r_\theta \circ r_{360-\theta}$$

for any θ. Also note that $r_{360-\theta} \in R_4$, since we know θ is a multiple of 90 and thus $360 - \theta$ is also a multiple of 90. Thus, R_4 is indeed a group.

Since $r_{360} = r_0$, we can enumerate the elements of R_4 as

$$R_4 = \{r_0, r_{90}, r_{180}, r_{270}\},$$

so $|R_4| = 4$. We can also verify that R_4 is abelian by observing that

$$r_\phi \circ r_\theta = r_{\phi+\theta} = r_{\theta+\phi} = r_\theta \circ r_\phi$$

for any ϕ and θ, where we have appealed to the fact that addition on $\mathbb{R}$ is commutative. □

Remark. The moral here is that associativity is annoying to check. A shortcut, when possible, is to realize your group as a set of functions $f : X \to X$ for some set X, and then appeal to function composition to show that $*$ is associative.

Problem 2.36. Determine whether each of the following is a group. If the pair is a group, determine the order, identify the identity, describe the inverses, and determine whether the group is abelian. If the pair is not a group, explain why.

(a) $(\mathbb{Z}, +)$

(c) $(\mathbb{Z}, \cdot)$

(d) $(\mathbb{Z}, \div)$

(j) $([0,1], *)$, where $a * b := \min\{a, b\}$

Solution. (a) This is a group of infinite order. Addition on $\mathbb{Z}$ is associative, the identity is 0, and the inverse of $n \in \mathbb{Z}$ is $-n$. Addition on $\mathbb{Z}$ is also commutative, so $(\mathbb{Z}, +)$ is abelian.

(b) This is not a group because there are no inverses. For example, $2 \in \mathbb{Z}$, but $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$.

(c) This is not a group because $\div$ is not even a binary operation on $\mathbb{Z}$. For example, $1, 2 \in \mathbb{Z}$, but their quotient $1 \div 2 = \frac{1}{2} \notin \mathbb{Z}$.

(j) This is not a group. If it were, then the identity element would have to be 1, since $\min\{1, a\} = a$ for any $a \in [0,1]$. But then note that

$$\min(0.5, a) \leq 0.5 \neq 1,$$

so there cannot possibly be an inverse for 0.5. □

Theorem 2.37. *If G is a group, then there is a unique identity element in G. That is, there is only one element $e \in G$ such that $ge = eg = g$ for all $g \in G$.*

Proof. Let e_1 and e_2 both be identity elements. Then

$$e_1 = e_1 e_2 = e_2$$

by applying the identity property on either side. □

Problem 2.38. Provide an example of a group of order 1. Can you find more than one such group?

Solution. One such group is $(\{0\},+)$. Technically, $(\{1\},\cdot)$ is also a group of order 1, but in some sense, these are the same, since the only binary operation we can have on a singleton set $\{a\}$ is $*:\{a\}\times\{a\}\to\{a\}$ defined by $(a,a)\mapsto a$. □

Remark. We'll later learn that we can answer this question by saying there is only one such group *up to isomorphism*.

Theorem 2.39 (Cancellation law)**.** *Let G be a group and let $g,x,y\in G$. Then $gx=gy$ if and only if $x=y$. Similarly, $xg=yg$ if and only if $x=y$.*

Proof. We show the first statement.

($\Rightarrow$) Suppose $gx=gy$. Then left multiplying by the inverse g^{-1} on both sides yields

$$x=g^{-1}gx=g^{-1}gy=y,$$

as desired.

($\Leftarrow$) Suppose $x=y$. Then left multiplying by g on both sides yields $gx=gy$.

The proof of the second statement is similar. □

Theorem 2.47. *If G is a group and $g\in G$, then for all $n,m\in\mathbb{Z}$, we have the following:*

(a) $g^ng^m=g^{n+m}$,

(b) $(g^n)^{-1}=g^{-n}$,

(c) $(g^n)^m=g^{nm}$.

Proof of (a). By the definition of exponents in groups and associativity, for $n,m\geq 0$, we have

$$g^ng^m=\underbrace{(gg\cdots g)}_{n\text{ times}}\underbrace{(gg\cdots g)}_{m\text{ times}}=\underbrace{gg\cdots ggg\cdots g}_{n+m\text{ times}}=g^{n+m}.$$

If $n,m<0$, then we can make a similar demonstration using g^{-1} to see that $g^ng^m=g^{n+m}$. Now if $n<0$ and $m\geq 0$ with $|n|\leq m$, then $|n|$ copies of g in g^m will be cancelled out by the $|n|$ copies of g^{-1}, so we will be left with $g^{m-|n|}=g^{m+n}$. In the case that $|n|>m$, then m copies of g^{-1} in $g^{-|n|}$ will be cancelled out by the m copies of g, so we are left with $g^{-(|n|-m)}=g^{-|n|+m}=g^{n+m}$. The remaining case where $n\geq 0$ and $m<0$ is similar. □

Lecture 4

Aug. 30 — Groups

Definition 2.50. Let G be a group and $S = \{a, b, c, \dots\} \subseteq G$. We call $a, b, c, \dots$ **letters** and elements of the form (products of $a, b, c, \dots$ and their inverses)

$$e, a, b, c, ab, ba, ac^{-1}, \dots$$

words in S. The set of all words in S is called the **group generated by** S and is denoted $\langle S \rangle$.

A *generating set* for G is a set S such that $G = \langle S \rangle$. A generating set S is called *minimal* if $S \setminus s$ is no longer a generating set for any $s \in S$. A group G is called *cyclic* if it is generated by a single element, i.e. there exists $g \in G$ such that $G = \langle g \rangle$.

Remark. Suppose that $\{a, b, c\}$ is a minimal generating set for some group G. This does *not* mean that we cannot find $\{d, f\}$ which is also a minimal generating set for G (but it does mean that $\{d, f\} \not\subseteq \{a, b, c\}$). For example, note that $(\mathbb{Z}, +) = \langle 1 \rangle = \langle 2, 3 \rangle$, and both generating sets are minimal.

Theorem 2.52. *If G is a group under $*$ and S is a subset of G, then $\langle S \rangle$ is also a group under $*$.*

Proof. Associativity is automatically satisfied in $\langle S \rangle$ since $*$ is inherited from G. The identity element e is also inherited from G and is in $\langle S \rangle$ by convention. To see that $\langle S \rangle$ is closed under $*$, let $x, y \in \langle S \rangle$ with

$$x = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n}, \quad y = s_{n+1}^{\epsilon_{n+1}} s_{n+2}^{\epsilon_{n+2}} \cdots s_m^{\epsilon_m}.$$

Then $xy \in \langle S \rangle$ since

$$xy = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n} s_{n+1}^{\epsilon_{n+1}} s_{n+2}^{\epsilon_{n+2}} \cdots s_m^{\epsilon_m}$$

is also a word in S. For inverses, let x be defined as above. Then we have

$$x^{-1} = s_n^{-\epsilon_n} \cdots s_2^{-\epsilon_2} s_1^{-\epsilon_1},$$

which is also a word in S since $-\epsilon_i \in \{-1, 1\}$ if $\epsilon_i \in \{-1, 1\}$. We can verify that this works as

$$xx^{-1} = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots \underbrace{s_n^{\epsilon_n} s_n^{-\epsilon_n}}_{=e} \cdots s_2^{-\epsilon_2} s_1^{-\epsilon_1} = e,$$

where the inner terms all cancel to become e. The same works for $x^{-1}x$, so $x^{-1} \in \langle S \rangle$. Thus, $\langle S \rangle$ indeed forms a group under $*$. □

Problem 2.55. Consider the rotation group R_4 that we introduced in Problem 2.20. Let r be the element of R_4 that rotates the square by 90° clockwise.

(a) Describe the action of r^{-1} on the square and express r^{-1} as a word using r only.

(b) Prove that $R_4 = \langle r \rangle$ by writing every element of R_4 as a word using r only.

(c) Is $\{r\}$ a minimal generating set for R_4?

(d) Is R_4 a cyclic group?

Solution. (a) The action of r^{-1} is a rotation of the square by 90° counterclockwise, which is the same as a rotation by 270° clockwise. Thus we have $r^{-1} = rrr$.

(b) The elements of R_4 are $r_0, r_{90}, r_{180}, r_{270}$, so we can write these as words in r by

$$r_0 = e, \quad r_{90} = r, \quad r_{180} = rr, \quad r_{270} = rrr.$$

So $R_4 = \langle r \rangle$.

(c) Yes, $\{r\}$ is a minimal generating set for R_4. Removing r from the generating set results in

$$\langle \{r\} \setminus r \rangle = \langle \varnothing \rangle = \{e\} \neq R_4,$$

so $\{r\}$ is minimal.

(d) By definition, R_4 is cyclic since it is generated by a single element, namely r. □

Problem 2.56. Consider the dihedral group D_3 introduced in Problem 2.21. To give us a common starting point, let's assume the triangle and hole are positioned so that one of the tips of the triangle is pointed up. Let r be the rotation by 120° in the clockwise direction and let s be the reflection in D_3 that fixes the top of the triangle.

(a) Describe the action of r^{-1} on the triangle and express r^{-1} as a word using r only.

(b) Describe the action of s^{-1} on the triangle and express s^{-1} as a word using s only.

(c) Prove that $D = \langle r, s \rangle$ by writing every element of D_3 as a word in r or s.

(d) Is $\{r, s\}$ a minimal generating set for D_3?

(e) Explain why there is no single generating set for D_3 consisting of a single element. This proves that D_3 is not cyclic.

Solution. (a) The action of r^{-1} is the rotation by 120° counterclockwise, which is the same as a rotation by 240° clockwise. Thus $r^{-1} = rr$.

(b) The action of s^{-1} is exactly the same as that of s, also a reflection that fixes the top of the triangle. So we have $s^{-1} = s$.

(c) We can write the elements of D_3 as

$$D_3 = \langle r, s \rangle = \{e, r, rr, s, sr, srr\}.$$

Thus $\{r, s\}$ generates D_3.

(d) Yes, $\{r, s\}$ is a minimal generating set. To see this, note that removing r yields

$$\langle s \rangle = \{e, s\} \neq D_3$$

since $s^{-1} = s$ and removing s yields

$$\langle r \rangle = \{e, r, r^2\} \neq D_3$$

since $r^{-1} = r^2$. Thus, $\{r, s\}$ is minimal.

(e) Suppose otherwise that D_3 is cyclic, i.e. there is $x \in D_3$ such that $D_3 = \langle x \rangle$. Then D_3 would be abelian, since each $g \in D_3$ can be written as x^n, and x clearly commutes with itself and each of its powers. But we we know that D_3 is not abelian since $rs \neq sr$, so there cannot exist a generating set for D_3 with only a single element. □

Remark. For general finite groups, a good way to verify that a group is not cyclic is by checking that no element has order equal to the order of the group, where the order of an element x is the lowest n such that $x^n = e$.

Problem 2.60. Find a minimal generating set for $(\mathbb{Z}, +)$. Is $\mathbb{Z}$ a cyclic group under addition?

Solution. Yes, we have $(\mathbb{Z}, +) = \langle 1 \rangle$ since every $n \in \mathbb{Z}$ can be written as $n(1)$, so $\mathbb{Z}$ is cyclic. □

Remark. This is a good example of a cyclic group where $G = \langle g \rangle$ but there is no n such that $g^n = e$.

Lecture 5

Sept. 6 — Cayley Diagrams

Problem 2.71. Let R_6 denote the group of rotational symmetries of a regular hexagon and let r be the rotation by 60° clockwise. It's not two hard to see that $R_6 = \langle r \rangle$ and $|R_6| = 6$. The Cayley diagram for R_6 with generating set $\{r\}$ is given in Figure 2.4.

(a) Is R_6 cyclic?

(b) Is R_6 abelian?

(c) Write r^{-1} as a word in r.

(d) Can you find a shorter word to describe r^8?

(e) Does r^2 generate the group?

(f) Does r^5 generate the group?

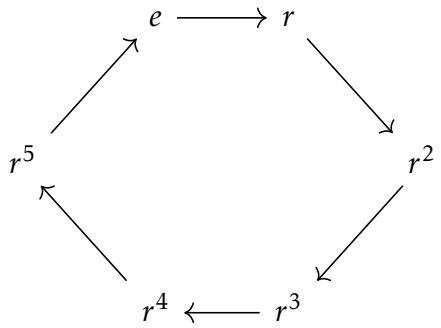


Figure 2.4: Cayley diagram for R_6 with generating set $\{r\}$.

Solution. (a) Yes, R_6 is cyclic since $R_6 = \langle r \rangle$ as mentioned in the problem statement.

(b) Yes, R_6 is abelian since all cyclic groups are abelian. This is because any $g \in R_6$ can be written as g^i. So for any $g^i, g^j \in R_6$, we have

$$g^i g^j = g^{i+j} = g^{j+i} = g^j g^i,$$

where we have appealed to the commutativity of addition on the real numbers.

(c) The action of r^{-1} is the rotation by 60° counterclockwise, which is the same as a rotation by 300° clockwise. Thus $r^{-1} = rrrrr$.

(d) Since $r^6 = e$, we can write $r^8 = r^6 r^2$ as r^2 instead.

(e) No, r^2 does not generate the group. We can compute the subgroup generated by r^2

$$\langle r^2 \rangle = \{e, r^2, r^4\} \neq R_6,$$

where we have noted that $r^6 = e$.

(f) Yes, r^5 generates the group. We can compute that

$$\langle r^5 \rangle = \{e, r^5, r^4, r^3, r^2, r\} = R_6,$$

which is the entire group. □

Problem 2.73. Consider the group $(\mathbb{Z}, +)$.

(a) Construct a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{1\}$.

(b) Construct a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{-1\}$. How does the diagram compare to the one in Part (a)?

(c) It turns out that $\mathbb{Z} = \langle 2, 3 \rangle$. Construct a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{2, 3\}$.

Solution. (a) The following

$$\cdots \longrightarrow -2 \longrightarrow -1 \longrightarrow 0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow \cdots$$

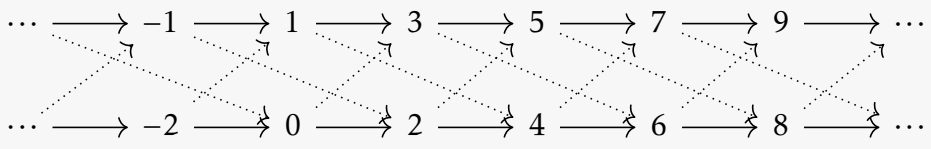
is a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{1\}$.

(b) The following

$$\cdots \longleftarrow -2 \longleftarrow -1 \longleftarrow 0 \longleftarrow 1 \longleftarrow 2 \longleftarrow 3 \longleftarrow \cdots$$

is a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{-1\}$. This is the same as Part (a) but with all arrows reversed.

(a) The following



is a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{2, 3\}$. □

Problem 2.76. Consider the diagrams given in Figures 2.5 and 2.6. Explain why neither of these diagrams could possibly be the Cayley diagram for a group.

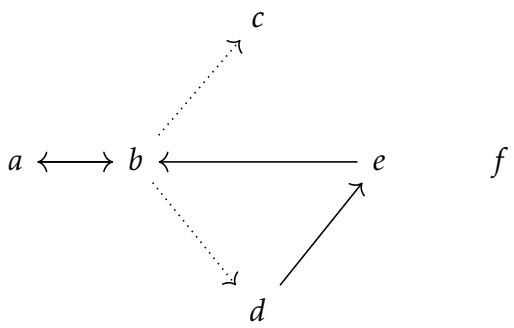


Figure 2.5

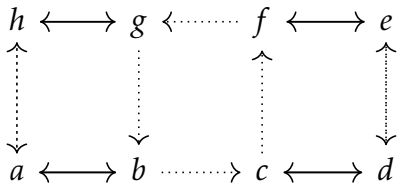


Figure 2.6

Solution. In both figures, there are arrows that are sometimes bidirectional and sometimes not (the solid arrows in Figure 2.5 and the dotted arrows in Figure 2.6). This means that an element is sometimes its own inverse and sometimes not, which cannot happen. □

Remark. A Cayley diagram should look the same from the perspective of any vertex.

Problem 3.1. Recall the definition of "subset." What do you think "subgroup" means? Try to come up with a potential definition. Try not to read any further before doing this.

Solution. A subgroup of a group $(G,*)$ should be a subset $H \subseteq G$ that is also a group in its own right under the same binary operation $*$. □

Lecture 6

Sept. 11 — Subgroups

Problem 3.2. Examine your Cayley diagrams for D_4 (with generating set $\{r, s\}$) and R_4 (with generating set $\{r\}$) and make some observations. How are they similar and how are they different? Can you reconcile the similarities and differences by thinking about the actions of each group.

Solution. Look at Figures 6.1 and 6.2. The Cayley diagram for R_4 seems like it appears on the inside and outside of the Cayley diagram for D_4, but D_4 is bigger overall. This is because the actions of R_4 are each also actions of D_4, but D_4 has another action that is not in R_4. □

Problem 3.3. If you ignore the labels on the vertices and just pay attention to the configuration of arrows, it appears that there are two copies of the Cayley diagram for R_4 in the Cayley diagram for D_4. Isolate these two copies by ignoring the edges that correspond to the generator s. Now, paying close attention to the words that label the vertices from the original Cayley diagram for D_4, are either of these groups in their own right?

Solution. The inner copy is indeed a group, but the outer copy technically is not since it does not contain the identity element. □

Remark. We'll see later that a clone is a *right coset* of a group.

Definition 3.4. Let G be a group and H a nonempty subset of G. Then H is a **subgroup** of G, written $H \leq G$, if H is a group in its own right under the binary operation inherited from G.

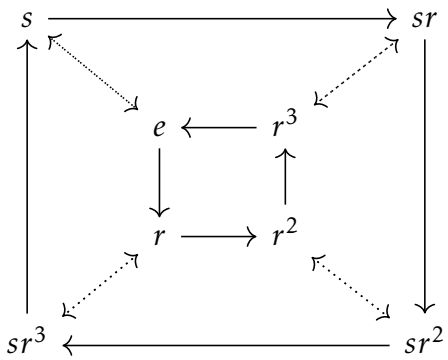


Figure 6.1: Cayley diagram for D_4 with generating set $\{r, s\}$.

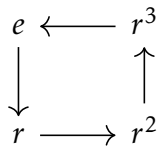


Figure 6.2: Cayley diagram for R_4 with generating set $\{r\}$.

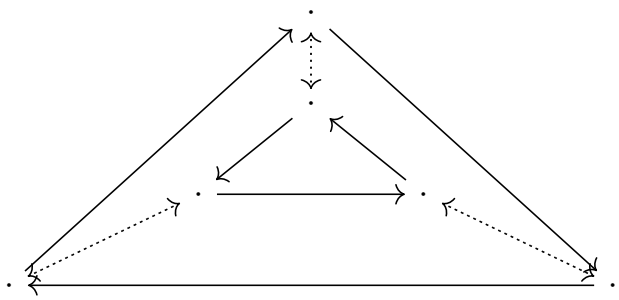


Figure 6.3: Cayley diagram for D_3 with generating set $\{r, s\}$.

Theorem 3.6 (Two step subgroup test)**.** *Suppose G is a group and H is a nonempty subset of G. Then $H \leq G$ if and only if (i) for all $h \in H$, $h^{-1} \in H$ as well, and (ii) H is closed under the binary operation of G.*

Proof. ($\Rightarrow$) This direction is trivial: (i) and (ii) are just axioms 3 and 0 of a group.

($\Leftarrow$) Suppose H is a nonempty subset that satisfies (i) and (ii). Note that axioms 0 and 3 are exactly properties (i) and (ii), and axiom 1 (associativity) is also satisfied since the binary operation is inherited from G. All that remains is to check that the identity e is in G. But this follows from (i) and (ii), since $h, h^{-1} \in H$ implies that $hh^{-1} = e \in H$ as well. Thus $H \leq G$. □

Problem 3.13. We currently have two different Cayley diagrams for D_3 (see Problems 2.21 and 2.57).

(a) Can you find the Cayley diagram for the trivial subgroup $\langle e \rangle$ is either Cayley diagram for D_3? Identity all of the clones of $\langle e \rangle$ in both Cayley diagrams for D_3.

(b) Can you find the Cayley diagram for the subgroup $\langle r \rangle = R_3$ in either Cayley diagram for D_3? If possible, identify all of the clones of R_3 in the Cayley diagrams for D_3.

(c) Can you find the Cayley diagrams for $\langle s \rangle$ and $\langle s' \rangle$ in either Cayley diagram for D_3? If possible, identify all of the clones of $\langle s \rangle$ and $\langle s' \rangle$ in the Cayley diagrams for D_3.

Solution. (a) The Cayley diagram for $\langle e \rangle$ is simply the vertex e in each of Figures 6.3 and 6.4. The clones of $\langle e \rangle$ are each of the vertices in either figure.

(b) The Cayley diagram for R_3 is the inner triangle in Figure 6.3 (if we assume the identity element is on the inside). The clones are the inside and outside triangles in Figure 6.3. There are no clones of R_3 in Figure 6.4.

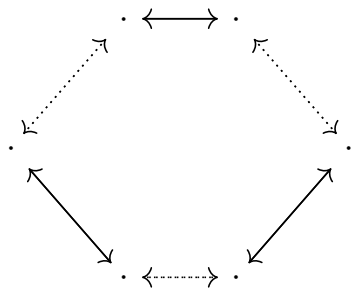


Figure 6.4: Cayley diagram for D_3 with generating set $\{s, s'\}$.

(c) In Figure 6.3, the Cayley diagram for $\langle s \rangle$ is the dotted arrow that is connected to the identity, and the clones are the other dotted arrows. There are no copies of $\langle s' \rangle$ in Figure 6.3. In Figure 6.4, the Cayley diagrams for $\langle s \rangle$ and $\langle s' \rangle$ are the solid and dotted arrows that are connected to the identity, respectively, and the clones are the other solid and dotted arrows. □

Problem 3.17. Consider the group $(\mathbb{Z}, +)$ (under ordinary addition).

(a) Show that the even integers, written $2\mathbb{Z} := \{2k \mid k \in \mathbb{Z}\}$, form a subgroup of $\mathbb{Z}$.

(b) Show that the odd integers are not a subgroup of $\mathbb{Z}$.

(c) Show that all subsets of the form $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ for $n \in \mathbb{Z}$ are subgroups of $\mathbb{Z}$.

(d) Are there any other subgroups besides the ones listed in Part (c)? Explain your answer.

(e) For $n \in \mathbb{Z}$, write the subgroup $n\mathbb{Z}$ in the "generated by" notation. That is, find a set S such that $\langle S \rangle = n\mathbb{Z}$. Can you find more than one way to do it?

Solution. (a) We apply the general case of Part (c) for $n = 2$.

(b) The odd integers cannot form a subgroup, since the identity element 0 is not odd.

(c) We apply the two step subgroup test. The set $n\mathbb{Z}$ is clearly nonempty since $0 \in n\mathbb{Z}$. The set $n\mathbb{Z}$ is closed under inverses, since for any $nk \in n\mathbb{Z}$ with $k \in \mathbb{Z}$, we also have $-nk \in n\mathbb{Z}$ since $-k \in \mathbb{Z}$ (the integers are closed under taking additive inverses). Finally, $n\mathbb{Z}$ is closed under the group operation, since for any $nk, nl \in n\mathbb{Z}$, we also have $nk + nl = n(k + l) \in n\mathbb{Z}$ since $k + l \in \mathbb{Z}$.

(d) No, there are not any other subgroups. To see this, let H be a subgroup of $\mathbb{Z}$. If we take

$$m = \min\{n \mid n \in H, n \geq 0\},$$

which exists by the well-ordering principle, then $H = m\mathbb{Z}$ by applying Bezout's lemma.

(e) We can write $n\mathbb{Z}$ as $\langle n \rangle$. We can also write $n\mathbb{Z} = \langle -n \rangle = \langle n, 2n \rangle = \langle 3n, 2n \rangle$, etc. □

Lecture 7

Sept. 13 — Isomorphisms

If G is a group, the *center* of G is

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

For any G, $Z(G)$ is an abelian subgroup of G. In particular, if G is abelian, then $Z(G) = G$.

Problem 3.24. Find the center of each of the following groups.

(a) S_2

(b) V_4

(e) D_4

(f) R_4.

Solution. (a) Note that S_2 is abelian, so $Z(S_2) = S_2$.

(b) Recall that $V_4 = \langle v, h \rangle$ and $vh = hv$, so V_4 is abelian and $Z(V_4) = V_4$.

(c) First note that

$$rs \neq sr, \quad sr(r^3) \neq r^3(sr), \quad (sr^3)(sr^2) \neq (sr^2)(sr^3),$$

so none of these elements can be in $Z(D_4)$. Now, note that $r^2 r = rr^2$ and $r^2 s = sr^2$, so $r^2 \in Z(D_4)$ (since $\{r, s\}$ generates D_4). Thus $Z(D_4) = \{e, r^2\}$.

(d) Note that R_4 is also abelian, so $Z(R_4) = R_4$. □

Remark. To check if g is in center of G, we only need to check commutativity with the generators.

Problem 3.27. Provide an example of a group G with subgroups H and K such that $H \cup K$ is not a subgroup of G.

Solution. Let $G = (\mathbb{R} \setminus \{0\}, \cdot)$, $H = \langle 2 \rangle$, and $K = \langle 3 \rangle$. Then

$$H \cup K = \{2^n \mid n \in \mathbb{Z}\} \cup \{3^n \mid n \in \mathbb{Z}\},$$

but $2(3) = 6 \notin H \cup K$, so $H \cup K$ is not a subgroup. □

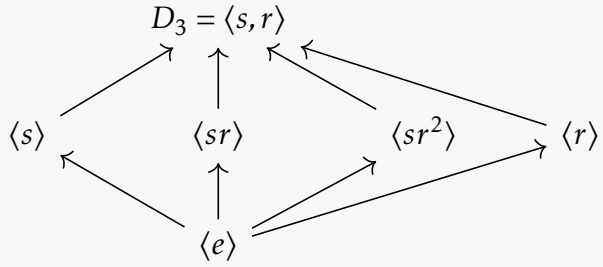
Remark. The is analogous to the case of vector spaces, where the union of two subspaces is typically no longer a subspace.

Problem 3.31. Find all the subgroups of $D_3 = \{e, r, r^2, s, sr, sr^2\}$ (where r and s are the usual symmetries of an equilateral triangle) and then draw the subgroup lattice for D_3.

Solution. The subgroups of D_3 are

$$\langle e \rangle, \quad \langle r \rangle, \quad \langle s \rangle, \quad \langle sr \rangle, \quad \langle sr^2 \rangle, \quad \langle s, r \rangle.$$

One can check that any other choice of generators will coincide with one of these existing subgroups. The following



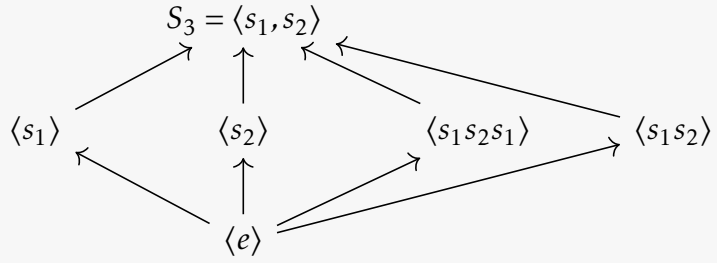
is a subgroup lattice for D_3. □

Problem 3.32. Find all the subgroups of $S_3 = \langle s_1, s_2 \rangle$ (where s_1 is the action that swaps the positions of the first and second coins and s_2 is the action that swaps the second and third coins; see Problem 2.59) and then draw the subgroup lattice for S_3. How does your lattice compare to the one in Problem 3.31? You should look back at parts (e) and (f) of Problem 2.72 and ponder what just happened.

Solution. The subgroups of D_3 are

$$\langle e \rangle, \quad \langle s_1 \rangle, \quad \langle s_2 \rangle, \quad \langle s_1 s_2 \rangle, \quad \langle s_1 s_2 s_1 \rangle, \quad \langle s_1, s_2 \rangle.$$

One can check that any other choice of generators will coincide with one of these existing subgroups. The following



is a subgroup lattice for S_3. Note that this looks identical to the one for D_3, since D_3 and S_3 are isomorphic, which we can also see in the Cayley diagrams from Problem 2.72. □

Problem 3.35. We have seen two different Cayley diagrams for D_3, one with generating set $\{s, r\}$ and one with generating set $\{s, s'\}$. As Figure 3.5 illustrates, there is a matching between D_3 and S_3 that relies on the generating sets $\{s, s'\}$ and $\{s_1, s_2\}$, respectively. Find a different matching between D_3 and S_3 that utilizes the generating set $\{r, s\}$ for D_3.

Solution. The key idea is that we need an element of order 3 from S_3 in order to match with D_3 (since r is of order 3). So if we use the generating set $\{s_2 s_1, s_2\}$ (note that $|s_2 s_1| = 3$), then the matching $r \mapsto s_2 s_1$ and $s \mapsto s_2$ works. □

Lecture 8

Sept. 18 — More Isomorphisms

Definition 3.48. Let $(G_1, *)$ and $(G_2, \odot)$ be groups. We say that G_1 is **isomorphic** to G_2 if there exists a bijection $\phi : G_1 \to G_2$ satisfying the *homomorphic property*

$$\phi(x * y) = \phi(x) \odot \phi(y) \tag{$\star$}$$

for all $x, y \in G_1$. We call such a bijection an **isomorphism**.

We call $(\star)$ the *homomorphic property*. In the case that $(G_1, *) = (G_2, \odot)$, we call ϕ an *automorphism*.

Problem 3.50. Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$, where $\mathbb{R}^+$ is the set of positive real numbers. It turns out that these two groups are isomorphic, but this would be difficult to discover using our previous techniques because the groups are infinite. Define $\phi : \mathbb{R} \to \mathbb{R}^+$ via $\phi(r) = e^r$ (where e is the natural base, not the identity). Prove that ϕ is an isomorphism.

Solution. We can see that ϕ is a bijection by appealing to its inverse, the logarithm. Note that

$$\ln(e^r) = e^{\ln(r)} = r,$$

so ϕ is bijective. Next we check the homomorphism property:

$$\phi(x)\phi(y) = e^x e^y = e^{x+y} = \phi(x + y).$$

Thus ϕ is an isomorphism. □

Problem 3.51. For each of the following pairs of groups, determine whether the given function is an isomorphism from the first group to the second group.

(a) $(\mathbb{Z}, +)$ and $(\mathbb{Z}, +)$, $\phi(n) = n + 1$.

(b) $(\mathbb{Z}, +)$ and $(\mathbb{Z}, +)$, $\phi(n) = -n$.

(c) $(\mathbb{Q}, +)$ and $(\mathbb{Q}, +)$, $\phi(x) = x/2$.

Solution. (a) This is *not* an isomorphism since

$$\phi(x) + \phi(y) = (x + 1) + (y + 1) = x + y + 2 \neq x + y + 1 = \phi(x + y),$$

so ϕ does not satisfy the homomorphic property.

(b) We show that ϕ is an isomorphism. First, ϕ is clearly a bijection since $-x = -y$ if and only if $x = y$. Next, it also satisfies the homomorphic property since

$$\phi(x) + \phi(y) = (-x) + (-y) = -x + -y = -(x + y) = \phi(x + y).$$

Thus ϕ is indeed an isomorphism.

(c) We show that ϕ is an isomorphism. We can see that ϕ is clearly a bijection since $\frac{x}{2} = \frac{y}{2}$ if and only if $x = y$. Next it also satisfies the homomorphism property since

$$\phi(x) + \phi(y) = \frac{x}{2} + \frac{y}{2} = \frac{x + y}{2} = \phi(x + y).$$

Thus ϕ is indeed an isomorphism. □

Theorem 3.54. *If $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$, then $\phi(g^{-1}) = [\phi(g)]^{-1}$.*

Proof. Using the fact that $\phi(e_1) = e_2$, where e_1 and e_2 are the identity elements of G_1 and G_2,

$$\begin{aligned} e_2 = \phi(e_1) = \phi(g * g^{-1}) &= \phi(g) \odot \phi(g^{-1}) \\ &= \phi(g^{-1} * g) = \phi(g^{-1}) \odot \phi(g). \end{aligned}$$

So $\phi(g^{-1}) = [\phi(g)]^{-1}$. □

Theorem 3.55. *If $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$, then the function $\phi^{-1} : G_2 \to G_1$ is an isomorphism.*

Proof. First we show that ϕ^{-1} is also a bijection. For surjectivity, note that for any $g \in G_2$, we have $\phi^{-1}(\phi(g)) = g$, so $\phi(g)$ is a preimage of g under ϕ^{-1}. For injectivity, suppose $\phi^{-1}(g) = \phi^{-1}(h)$ for some $g, h \in G_2$. Then we can apply ϕ to both sides to get that

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

So ϕ is both injective and surjective, and therefore bijective.

Now we show that ϕ satisfies the homomorphic property. Let $g, h \in G_2$. Since ϕ is a bijection, we can find $g', h' \in G_1$ such that $g = \phi(g')$ and $h = \phi(h')$. Then by the homomorphic property of ϕ,

$$\phi^{-1}(g'h') = \phi^{-1}(\phi(g)\phi(h)) = \phi^{-1}(\phi(gh)) = gh = \phi^{-1}(\phi(g))\phi^{-1}(\phi(h)) = \phi^{-1}(g')\phi^{-1}(h'),$$

as desired. Thus ϕ^{-1} is an isomorphism. □

Lecture 9

Sept. 20 — Cyclic Groups

Theorem 3.62. *Suppose $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$. If G_1 is cyclic, then G_2 is cyclic.*

Proof. Let $g \in G_1$ be an element that generates G_1. Then we propose that $\phi(g)$ generates G_2. Let $h \in G_2$ be an arbitrary element. Since ϕ is a bijection, there exists $g' \in G_1$ such that $\phi(g') = h$. But g generates G_1, so $g' = g^n$ for some $n \in \mathbb{Z}$. Then we have $\phi(g^n) = h$, so

$$h = \phi(g^n) = \phi(g)^n$$

as ϕ respects the group structure. Thus we have $G_2 = \langle \phi(g) \rangle$. □

Theorem 3.65. *If $\phi : G_1 \to G_2$ is an isomorphism and $H \leq G_1$, then $\phi(H) \leq G_2$.*

Proof. We proceed by the two step subgroup test. First, $\phi(H)$ is nonempty since $e_1 \in H$ and thus $\phi(e_1) \in \phi(H)$. Now let $h \in \phi(H)$. Since ϕ is a bijection, there exists $h' \in H$ such that $\phi(h') = h$. Then by Theorem 3.54 we have

$$h^{-1} = \phi(h')^{-1} = \phi(h^{-1}) \in \phi(H),$$

where $h^{-1} \in H$ since H is a subgroup. For closure under the binary operation, let $g \in \phi(H)$ be another arbitrary element with $g' \in H$ such that $\phi(g') = g$. Then we have

$$gh = \phi(g')\phi(h') = \phi(g'h') \in \phi(H),$$

where $g'h' \in H$ since H is a subgroup. Thus $\phi(H) \leq G_2$. □

Problem 4.14. Find the order of each of the following matrices in $\mathrm{GL}_2(\mathbb{R})$.

$$\text{(a)} \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \quad \text{(b)} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{(c)} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$$

Solution. (a) Let M be the matrix in question. We can square M to see that

$$M^2 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I,$$

so the order of M is 2.

(b) Once again let M be the matrix, and we can compute that

$$M^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I,$$

so $M^4 = I$. Thus the order of M is 4.

(c) Let M be the matrix. Note that if two matrices are equal, then their determinants are equal as well. But $\det M = 2$, so $\det M^n = 2^n$. Then $\det M^j = \det M^k$ if and only if $j = k$, which means that all the M^k are distinct. Thus M must be of infinite order. □

Theorem 4.16 (Division algorithm)**.** *Given any $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, there exist $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $m = nq + r$.*

Remark. The above theorem is a result from number theory that we will use without proof.

Theorem 4.17. *Suppose G is a group and let $g \in G$. The subgroup $\langle g \rangle$ is finite if and only if there exists $n \in \mathbb{N}$ such that $g^n = e$.*

Proof. ($\Rightarrow$) Suppose $\langle g \rangle$ is finite. Since $\mathbb{N}$ is infinite and there are only finitely many choice for g^n to be, by the pigeonhole principle there exist $m, k \in \mathbb{N}$ with $m < k$ such that $g^m = g^k$. Then $g^{k-m} = e$, and $k - m \in \mathbb{N}$ since $m < k$.

($\Leftarrow$) Suppose we have $n \in \mathbb{N}$ such that $g^n = e$. By the division algorithm, we can write any $k \in \mathbb{Z}$ as $k = qn + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then

$$g^k = g^{qn+r} = g^{qn}g^r = e^q g^r = g^r.$$

So any g^k can be written as g^r for $0 \leq r < n$. Since there are only finitely many choices for r, we have $|\langle g \rangle| < \infty$. □

Lecture 10

Sept. 25 — Cyclic and Symmetric Groups

Theorem 4.24. *Suppose G is a group and let $g \in G$ such that $|g| = n$. Then $g^i = g^j$ if and only if n divides $i - j$.*

Proof. ($\Rightarrow$) Let $g^i = g^j$. Multiply by g^{-j} on both sides to get $g^{i-j} = e$. Now use the division algorithm to write $i - j = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then

$$e = g^{nq+r} = g^{nq}g^r = e^q g^r = g^r,$$

where we used Corollary 4.20 to get $g^n = e$. So $g^r = e$ and we must have $r = 0$ since $0 \leq r < n$ and n is minimal. Thus $i - j = nq$, so $n|i - j$.

($\Leftarrow$) Let i and j be such that $n|i - j$. Then $i - j = nk$ for some $k \in \mathbb{Z}$, so

$$g^{i-j} = g^{nk} = e^k = e$$

by Corollary 4.20. Multiplying by g^j from here yields $g^i = g^j$. □

Problem 4.37. Consider $U_{10} = \{1, 3, 7, 9\}$.

(a) Find the group table for U_{10}.

(b) Is U_{10} cyclic? If so, list elements of U_{10} that individually generate U_{10}. If U_{10} is not cyclic, explain why.

(c) Is U_{10} isomorphic to either of R_4 or V_4? Justify your answer.

(d) Is U_{10} isomorphic to $\mathbb{Z}_4$? Justify your answer.

(e) Draw the subgroup lattice for U_{10}.

Solution. (a) The following

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

is a group table for U_{10}.

(b) Yes, U_{10} is cyclic. Note that

$$1 \overset{\times 3}{\longmapsto} 3 \overset{\times 3}{\longmapsto} 9 \overset{\times 3}{\longmapsto} 7, \quad 1 \overset{\times 7}{\longmapsto} 7 \overset{\times 7}{\longmapsto} 9 \overset{\times 7}{\longmapsto} 3,$$

so 3 and 7 both individually generate U_{10}.

(c) Yes, U_{10} is isomorphic to R_4. We can define an isomorphism $\phi : U_{10} \to R_4$ by $3 \mapsto r$ and then extending ϕ by the homomorphic property. However, U_{10} is *not* isomoprhic to V_4 since R_4 is not isomorphic to V_4 and isomorphisms form an equivalence relation (and are thus transitive).

(d) Yes, U_{10} is isomorphic to $\mathbb{Z}_4$ since R_4 is isomorphic to $\mathbb{Z}_4$ and isomorphisms are transitive.

(e) The following

$$\begin{array}{c} U_{10} = \langle 3 \rangle \\ \uparrow \\ \langle 9 \rangle \\ \uparrow \\ \langle 1 \rangle \end{array}$$

is a subgroup lattice for U_{10}. Note that it has the same structure as the one for R_4. □

Theorem 4.44. *If G is a finite cyclic group with generator g such that $|G| = n$, then for all $m \in \mathbb{Z}$,*

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

Proof. Note that $\gcd(m, n)\operatorname{lcm}(m, n) = mn$. So

$$m\frac{n}{\gcd(m, n)} = \operatorname{lcm}(m, n) = qn$$

for some $q \in \mathbb{Z}$. Then we have

$$(g^m)^{\frac{n}{\gcd(m,n)}} = g^{qn} = e^q = e.$$

Now we want to show that this is minimal. Suppose $g^{mk} = e$. We know that $m|mk$ (trivially) and $n|mk$ by Theorem 4.24 (really Corollary 4.25). This means that $mk \geq \operatorname{lcm}(m, n)$, or

$$k \geq \frac{\operatorname{lcm}(m, n)}{m} = \frac{n}{\gcd(m, n)}.$$

Finally apply Corollary 4.20 to conclude that this is indeed the order of g^m. □

Remark. We can now compute the order of *any* element in a finite group.

Theorem 4.54. *Suppose G is a finite abelian group and let $x, y \in G$ such that $|x| = m$ and $|y| = n$. If $\gcd(m, n) = 1$, then $|xy| = mn$.*

Proof. Since G is abelian, we have $xy = yx$ and thus

$$(xy)^{mn} = x^{mn}y^{mn} = e^n e^m = e.$$

Now we just need to show that mn is the minimal such exponent. Suppose $(xy)^k = e$ for some $k > 0$. Since $(xy)^k = e$, we have $(xy)^{mk} = e$, which means that $x^{mk}y^{mk} = e$ since G is abelian. The order of x is m, so we have $x^{mk} = e$ and thus actually $y^{mk} = e$. We can similarly argue by symmetry that $x^{nk} = e$ as well. By Corollary 4.25, we can conclude from this that $n|mk$ and $m|nk$. Now since $\gcd(m, n) = 1$, this can only happen if $n|k$ and $m|k$. Thus $k \geq mn$ and we're done. □

Lecture 11

Sept. 27 — Symmetric Groups

Theorem 4.55. *Suppose G is a finite abelian group. If n is the maximal order among all elements in G, then the order of every element in G divides n.*

Proof. Pick $g \in G$ such that $|g| = n$ and consider $\langle g \rangle$. Let $h \in G$ be an arbitrary element. If $h \in \langle g \rangle$, then $h = g^m$ for some m. So by Theorem 4.44 we have

$$|h| = \frac{n}{\gcd(m,n)},$$

or $|h|\gcd(m,n) = n$, so $|h|$ divides n. Now assume $h \notin \langle g \rangle$, and let $|h| = m$. Suppose for contradiction that m does not divide n. Then we can consider $d = \gcd(m,n)$. By Theorem 4.44,

$$|h^d| = \frac{m}{\gcd(m,d)} = \frac{m}{d}.$$

Note that since we have divided out $\gcd(m,n)$ from m, we must now have $\gcd(\frac{m}{d}, n) = 1$. Then $|h^d| = \frac{m}{d}$ and $|g| = n$, so by Theorem 4.54 we have

$$|h^d g| = \frac{mn}{d} > n.$$

(Here note that $\frac{m}{d} \neq 1$ since otherwise we would have $\gcd(m,n) = m$ and thus $m|n$, which we assumed was not the case.) So we have found an element $h^d g$ with order greater than n, which contradicts the maximality of n. Thus m must divide n. □

Definition 4.67. A **permutation** of a set A is a bijection $\sigma : A \to A$.

The *symmetric group* on n elements, S_n, is the set of all permutations of $\{1, 2, \ldots, n\}$.

Theorem 4.76. *The set of permutations on n objects forms a group under the operation of composition. That is, $(S_n, \circ)$ is a group. Morever, $|S_n| = n!$.*

Proof. A permutation is by definition a bijection, so the composition of permutations must still be a permutation since the composition of bijections is a bijection. Furthermore, permutations are functions, so $\circ$ is associative as function composition is associative. The identity permutation

is simply the permutation σ defined by $\sigma(a) = a$ for any a. Finally, the inverse of a permutation exists since permutations are bijections.

To see that $|S_n| = n!$, we can note that the effect of a permutation σ on a fixed state A completely determines the permutation. There are $n!$ states that σ can map A to, so $|S_n| = n!$. □

Lecture 12

Oct. 4 — More Symmetric Groups

Recall that a permutation of a set A is a bijection

$$\sigma : A \to A.$$

The collection S_n of permutations of $A = \{1, 2, 3, \ldots, n\}$ forms a group under composition, called the symmetric group. A *cycle* is a permutation σ of the form $(a_1 a_2 \ldots a_n)$, i.e.

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \quad \ldots, \quad \sigma(a_n) = a_1, \quad \sigma(a_n),$$

and $\sigma(b) = b$ for all other $b \in A$.

Theorem 4.85. *Suppose α and β are two disjoint cycles. Then $\alpha\beta = \beta\alpha$. That is, products of disjoint cycles commute.*

Proof. Let $\alpha, \beta : A \to A$ and let

$$\alpha = (a_1 a_2 \ldots a_n) \quad \text{and} \quad \beta = (b_1 b_2 \ldots b_m).$$

Since α and β are disjoint, β fixes any $a \in \alpha$ and α fixes any $b \in \beta$. So fix some $x \in A$ and we consider three cases. First if $x \in \alpha$, then

$$\alpha(\beta(x)) = \alpha(x) = \beta(\alpha(x)),$$

since $\alpha(x) \in \alpha$ as well so β will fix $\alpha(x)$. Apply a similar argument in the case of $x \in \beta$. Finally, if $x \notin \alpha$ and $x \notin \beta$, then $\alpha(\beta(x)) = \beta(\alpha(x)) = x$. The two agree in all cases, so we have $\alpha\beta = \beta\alpha$. □

Theorem 4.89. *Suppose $\alpha \in S_n$ such that α consists of m disjoint cycles of lengths $k_1, \ldots k_m$. Then $|\alpha| = \operatorname{lcm}(k_1, \ldots, k_m)$.*

Proof. Let $\alpha = \sigma_1 \sigma_2 \ldots \sigma_m$ where σ_i is a cycle of length k_i and let $|\alpha| = r$. By Theorem 4.88, we have $|\sigma_i| = k_i$. In particular, $\sigma_i^{k_i} = e$. Now observe that

$$e = \alpha^r = (\sigma_1 \sigma_2 \ldots \sigma_m)^r = \sigma_1^r \sigma_2^r \ldots \sigma_m^r$$

since disjoint cycles commute by Theorem 4.85. So pick an arbitrary $i \in \{1, \ldots, n\}$, and

$$i = e(i) = (\sigma_1^r \sigma_2^r \ldots \sigma_m^r)(i) = \sigma_j^r(i)$$

for some j by disjointness. Then $\sigma_j^r = e$, and we must have $k_j | r$ for all j. So we now conclude $r \geq \operatorname{lcm}(k_1, \ldots, k_m)$. But we also have

$$\alpha^{\operatorname{lcm}(k_1,\ldots,k_m)} = \sigma_1^{\operatorname{lcm}(k_1,\ldots,k_m)} \sigma_2^{\operatorname{lcm}(k_1,\ldots,k_m)} \ldots \sigma_m^{\operatorname{lcm}(k_1,\ldots,k_m)} = ee\ldots e = e$$

since each k_i is a factor of $\operatorname{lcm}(k_1, \ldots, k_m)$. So in fact $r = \operatorname{lcm}(k_1, \ldots, k_m)$ by Theorem 4.20. □

A cycle of length 2 is called a *transposition*. A transposition of the form $(i, i+1)$ is called an *adjacent transposition*.

Problem 4.97. Consider the arbitrary k-cycle $(a_1, a_2, \ldots, a_k)$ from S_n (with $k \leq n$). Find a way to write this permutation as a product of 2-cycles.

Solution. We can write the cycle as

$$(a_1 a_2 \ldots a_k) = (a_1 a_2)(a_2 a_3)\ldots(a_{k-1} a_k).$$

For any $1 \leq i < k$, notice that $(a_i a_{i+1})$ maps $a_i \mapsto a_{i+1}$ and it is completely fixed otherwise. In the case of $i = k$, we have

$$a_k \mapsto a_{k-1} \mapsto a_{k-2} \mapsto \cdots \mapsto a_1,$$

which also works as desired. □

Remark. We could have also written $(a_1 a_2 \ldots a_k) = (a_1 a_k)(a_1 a_{k-1})\ldots(a_1 a_2)$.

Corollary. *Problem 4.97 implies the following:*

1. *Transpositions generate S_n.*
2. *Transposition decompositions are not unique.*

Remark. The size of the decompositions are not unique either: $\sigma = \sigma e = \sigma(12)(12)$. Less trivial counterexamples also exist.

Remark. Note that $(12)(23) \neq (23)(12)$. Theorem 4.85 does not apply since the cycles are not disjoint.

Exercise. Find a subgroup of S_6 isomorphic to D_3.

Solution. We have $D_3 \cong S_3 \cong \langle (12)(23), (12) \leq S_6$. A possible isomorphism $\phi : S_6 \to D_3$ we can use is given by $(12)(23) \mapsto r$ and $(12) \mapsto s$. □

Remark. A perhaps easier and more informative way of constructing such a ϕ is to look at a Cayley diagram (Figure 12.1) with the vertices labeled by numbers. Then we can simply follow the generators to get the following isomorphism:

$$e \mapsto e, \quad r \mapsto (123)(456), \quad r^2 \mapsto (132)(465)$$
$$s \mapsto (16)(34)(25), \quad rs \mapsto \cdots, \quad r^2 s \mapsto \cdots.$$

This procedure also motivates the idea behind the proof of Cayley's theorem.

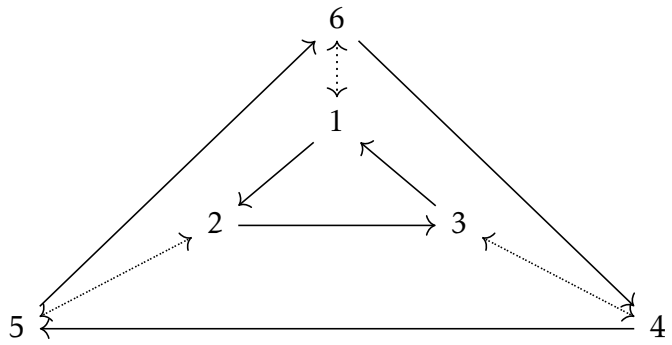


Figure 12.1: Cayley diagram for D_3 with generating set $\{r, s\}$, relabeled by $\{1, \ldots, 6\}$.

Theorem 4.105 (Cayley's theorem)**.** *Any group G of order n is isomorphic to some subgroup of S_n.*

Proof. We will construct an injective map $\varphi : G \to S_n$. First define $\mu_g : G \to G$ by $\mu_g(h) = gh$. Then define the map $\varphi : G \to S_n$ by

$$g \mapsto \underbrace{(h \mapsto gh)}_{\mu_g}.$$

Now we show that φ satisfies the homomorphic property. Take $g_1, g_2 \in G$. Then for any $h \in G$,

$$\varphi(g_1 g_2)(h) = g_1 g_2 h = g_1(g_2 h) = \varphi(g_1)(\varphi(g_2)(h)) = (\varphi(g_1) \circ \varphi(g_2))(h).$$

So $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ since they agree at all point. Now for injectivity, let $g_1, g_2 \in G$ such that $\varphi(g_1) = \varphi(g_2)$. Then pick some arbitrary point $h \in G$ and

$$g_1 h = \varphi(g_1)(h) = \varphi(g_2)(h) = g_2 h,$$

so by right-cancellation we have $g_1 = g_2$. Thus φ is injective. Finally φ is always surjective onto its image $\varphi(G)$, so φ is an isomorphism from G to $\varphi(G)$. Then $G \cong \varphi(G) \leq S_n$. □

Remark. The μ_g defined above is called the *left-regular representation* of G.

Lecture 13

Oct. 11 — Cosets, Lagrange's Theorem

Definition 5.1. Given a subgroup $H \leq G$ and $a \in G$, the **left coset** of H containing a is

$$aH := \{ah \mid h \in H\}$$

and the **right coset** containing a is

$$Ha := \{ha \mid h \in H\}.$$

Definition 5.9. Given a subgroup $H \leq G$ define

$$a \sim_L b \text{ if } a^{-1}b \in H \quad \text{and} \quad a \sim_R b \text{ if } ab^{-1} \in H$$

for all $a, b \in G$.

Remark. In fact $\sim_L$ and $\sim_R$ are equivalence relations (proof in homework), so we write $[a]_{\sim L}$ and $[a]_{\sim R}$ to denote the left and right equivalence classes of a.

Theorem 5.10. *If G is a group and $H \leq G$, then $[a]_{\sim L} = aH$ and $[a]_{\sim R} = Ha$ for all $a \in G$.*

Proof. Take any $b \in aH$. Then $b = ah$ for some $h \in H$, and multiplying by a^{-1} on the left yields $a^{-1}b = h \in H$. So $a \sim_L b$ and $b \in [a]_{\sim L}$, which implies $aH \subseteq [a]_{\sim L}$. Now take any $b \in [a]_{\sim L}$, which satisfies $a \sim_L b$, i.e. $a^{-1}b \in H$. Then $a^{-1}b = h$ for some $h \in H$, and multiplying by a gives $b = ah \in aH$. So $[a]_{\sim L} \subseteq aH$ and thus $[a]_{\sim L} = aH$. The proof for $[a]_{\sim R} = Ha$ is similar. □

Remark. The coset aH is a subgroup if and only if $a \in H$, in which case $aH = H$. For $a \notin H$, aH is not a subgroup since $a^{-1} \notin H$, which means that $e = aa^{-1} \notin aH$.

Theorem 5.12. *Let G be a group, $H \leq G$, and $a \in G$. Define $\phi : H \to aH$ via $\phi(h) = ah$. Then ϕ is a bijection.*

Proof. For surjectivity let $g \in aH$. By the definition of aH, there is some $h \in H$ such that $ah = g$. So $\phi(h) = ah = g$ and ϕ is surjective. For injectivity, suppose $\phi(g) = \phi(h)$. This means that $ag = ah$, which implies $g = h$ by cancellation. So ϕ is also injective and thus it is a bijection. □

Remark. Note that ϕ does not satisfy the homomorphic property unless $a = e$ (since $\phi(e) = a$). So ϕ is not an isomorphism in general, which makes sense since aH is not in general a group.

Theorem 5.16 (Lagrange's theorem)**.** *Let G be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.*

Proof. Consider the set of left cosets of H and call it F, i.e.

$$F = \{aH : a \in G\}.$$

First we show three facts:

1. $G \subseteq \bigcup_{f \in F} f$.

   Proof of (1). For any $g \in G$, we have $g \in gH \in F$. □

2. $\bigcup_{f \in F} f \subseteq G$.

   Proof of (2). Let $g \in g_1 H \in F$ for some $g_1 \in G$. Then $g = g_1 h \in G$ for some $h \in H$. □

3. For any $aH, bH \in F$, if $aH \neq bH$, then $aH \cap bH = \varnothing$.

   Proof of (3). We show the contrapositive. Suppose $aH \cap bH \neq \varnothing$, and we show that $aH = bH$. Since $aH \cap bH \neq \varnothing$, there is some g such that

   $$g = ah_1 = bh_2.$$

   Multiplying by h^{-1} gives $a = bh_2 h_1^{-1}$. Now for any $ah \in aH$, we have

   $$ah = bh_2 h_1^{-1} h \in bH$$

   since $h_2 h_1^{-1} h \in H$. Then $aH \subseteq bH$ and by symmetry $bH \subseteq aH$. So $aH = bH$. □

Noting that (1) and (2) imply $G = \bigcup_{f \in F} f$, we have

$$|G| = \left| \bigcup_{f \in F} f \right| = \sum_{f \in F} |f| = |F||H|,$$

where the last inequality comes from the fact that $\phi : H \to aH$ is bijective, so that $|H| = |aH|$ for any a. Then since $|F| \in \mathbb{Z}$, we conclude that $|H|$ divides $|G|$. □

Remark. The key idea of the proof of Lagrange's theorem is that the cosets of H partition G.

Remark. With this proof, we have actually shown something a little stronger:

If G is finite and $H \leq G$, then $|G| = k|H|$, where k is the number of left cosets of H in G.

We can also make the same argument about right cosets, so in fact #(left cosets) = #(right cosets).

Remark. We can also conclude via Lagrange's theorem that the number of clones (really right cosets) in a Cayley diagram is $|G|/|H|$.

Lecture 14

Oct. 16 – Normal Subgroups and Quotients

Definition 5.23. Let G be a group and let $H \leq G$. The **index** of H in G is the number of cosets (left or right) of H in G. Equivalently, if G is finite, then the index of H in G is equal to $|G|/|H|$. We denote the index via $[G : H]$.

Definition 5.26. Let G be a group and let $H \leq G$. If $aH = Ha$ for all $a \in G$, then we say that H is a **normal subgroup**. If H is a normal subgroup of G, then we write $H \trianglelefteq G$.

Theorem 5.33. *Suppose G is a group and let $H \leq G$ such that $[G : H] = 2$. Then $H \trianglelefteq G$.*

Proof. We need to show that $gH = Hg$ for all $g \in G$. If $g \in H$, then trivially we have $gH = H = Hg$. If $g \notin H$, then $gH \neq H$ and $H \neq Hg$. But $[G : H] = 2$ and cosets partition G, so in fact we have $gH = G \setminus H = Hg$. Thus we have $H \trianglelefteq G$ in either case. □

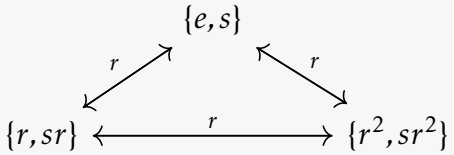
Theorem 5.36. *Suppose G is a group and let $H \leq G$. Then $H \trianglelefteq G$ if and only if $gHg^{-1} \subseteq H$ for all $g \in G$.*

Proof. ($\Rightarrow$) Since $H \trianglelefteq G$, we have $gH = Hg$ for all g. So for all $h \in H$, there is $h_1 \in H$ such that $gh = h_1 g$. So $ghg^{-1} = h_1 \in H$, which means $gHg^{-1} \subseteq H$.

($\Leftarrow$) Assume $gHg^{-1} \subseteq H$ for all g. Now fix an $h \in H$. Then for all $g \in G$, there is $h_1 \in H$ such that $gh_1g^{-1} = h$, or $gh_1 = hg$. So we have $gH \subseteq Hg$ and a similar argument by swapping g and g^{-1} gives $gH \subseteq Hg$. So $gH = Hg$ and $H \trianglelefteq G$. □

Problem 6.26. Let's see what happens if we attempt the quotient process for a subgroup that is not normal. Consider $H = \langle s \rangle \leq D_3$. In Problem 5.2, we discovered that the left cosets of H are not the same as the right cosets of H. This implies that H is not normal in D_3. Consider the standard Cayley diagram for D_3 that uses the generators r and s. Draw the diagram that results from attempting the quotient process on D_3 using the subgroup H. Explain why this diagram cannot be the diagram for a group.

Solution. Here we end up with the following diagram:



This cannot be the diagram for a group since there are two r arrows coming out of each coset. □

Problem 6.27. In Problem 5.3, we learned that the subgroup $K = \langle r \rangle$ is normal in D_3 since the left cosets are equal to the right cosets. Note that this follows immediately from Theorem 5.33 since $[D_3 : K] = 2$. Draw the diagram that results from performing the quotient process to D_3 using the subgroup K. Does the resulting diagram represent a group? If so, what group is it isomorphic to?

Solution. Taking the quotient by K instead gives the diagram:

$$\{e, r, r^2\} \overset{s}{\longleftrightarrow} \{s, sr, sr^2\}$$

This diagram makes sense and indeed represents a group isomorphic to $\langle s \rangle = \{e, s\}$. □

Theorem 6.31. *Let G be a group and let $H \leq G$. Then left coset multiplication (as defined above) is well defined if and only if $H \trianglelefteq G$.*

Proof. ($\Leftarrow$) Let $H \trianglelefteq G$, and we need to show that $(aH)(bH) = (ab)H$ for any choice of representatives from aH and bH. So let $a_1 \in aH$ and $b_1 \in bH$. Here it suffices to show that $a_1 b_1 \in (ab)H$. Since $a_1 \in aH$ and $b_1 \in bH$, we have $a_1 = ah_1$ and $b_1 = bh_2$ for some $h_1, h_2 \in H$. Then

$$a_1 b_1 \in (ab)H \iff (ah_1)(bh_2) = (ab)H \iff (ah_1)(bh_2) = abh_3$$

for some $h_3 \in H$. Multiplying by a^{-1} on both sides gives $h_1 bh_2 = bh_3$, and multiplying h_2^{-1} on both sides gives $h_1 b = bh_3 h_2^{-1}$. Since h_3 was arbitrarily chosen and $h_3, h_2^{-1} \in H$, we can really just set $h = h_3 h_2^{-1}$ as some arbitrary element from H. Then it remains to show that $h_1 b = bh$ for some $h \in H$. But $H \trianglelefteq G$, and in particular $Hb \subseteq bH$. So $h_1 b \in Hb \subseteq bH$, i.e. $h_1 b = bh$ for some $h \in H$. So left coset multiplication is is indeed well defined.

($\Rightarrow$) Assume left coset multiplication is well defined. By the previous argument, this is equivalent to being able to find $h \in H$ that satisfies $h_1 b = bh$ for all $h_1 \in H$. This is precisely the condition that $Hb \subseteq bH$. Furthermore, since $h_1 b = bh$ holds for any $h_1, h \in H$, we can look at

$$h_1^{-1} b = bh^{-1} \iff bh = h_1 b$$

after multiplying by h_1 and h on the left and right, respectively. This condition now precisely corresponds to $bH \subseteq Hb$. Then $bH = Hb$ and $H \trianglelefteq G$. □

Lecture 15

Oct. 18 — Product Groups

The intuition behind normal subgroups is that they are precisely *"the subgroups by which we can divide,"* where dividing by a subgroup means to *treat elements of the subgroup as identity elements.*

Why do we want this? Suppose $G = \mathbb{R}$ with addition as the group operation. Then G *"acts on"* $\mathbb{R}^2$: Given $\theta \in G$, rotate $\mathbb{R}^2$ counterclockwise by θ radians. Here, note that $H = 2\pi\mathbb{Z} \leq G$ does not do anything to $\mathbb{R}^2$! So we want to *"crush out"* H since it acts trivially.

What does this have to do with cosets?

- Fact: Clones of H in the Cayley diagram are precisely the right cosets of H.
- Observation: Given an arrow $\xrightarrow{a}$ not in H, the crushed diagram should have an arrow $H \xrightarrow{a} aH$.

This is because arrows in Cayley diagrams act on the left. The arrow $H \xrightarrow{a} aH$ becomes problematic if $aH \neq Ha$, since otherwise aH is no longer a right coset and composing the operation makes no sense. This is why we need our subgroups to be normal in order to divide.

Remark. The intuition behind why clones are right cosets is that right cosets (clones) do not affect left multiplication (arrows).

Theorem 6.32. *Let G be a group and let $H \trianglelefteq G$. Then the set of left cosets of H in G form a group under left coset multiplication.*

Proof. Note that we have already shown that left coset multiplication is well-defined in Theorem 6.31. In particular, the multiplication is automatically closed since $(aH)(bH) = (ab)H$ for any $a, b \in G$. Now, for associativity, let $a, b, c \in G$. Then

$$(aH \cdot bH)cH = (ab)H \cdot cH = (abc)H = aH \cdot (bc)H = aH \cdot (bH \cdot cH),$$

since the group operation on G is associative. For the identity element, note that

$$aH \cdot eH = (ae)H = aH,$$

so $eH = H$ is an identity. For inverses, note that

$$aH \cdot a^{-1}H = (aa^{-1})H = eH,$$

so $(aH)^{-1} = a^{-1}H$. Note that the proof of the other side for the identity and inverses are similar. Thus the left cosets of H in G indeed form a group under left coset multiplication. □

Remark. The identity element of this group of cosets is H, which is exactly what we wanted!

Theorem 6.1. *Suppose $(G,*)$ and $(H,\odot)$ are two groups, where e and e' are the identity elements of G and H, respectively. Then $(G\times H,\star)$ is a group, where $\star$ is defined as above. Morever, (e,e') is the identity of $G\times H$ and the inverse of $(g,h)\in G\times H$ is given by $(g,h)^{-1}=(g^{-1},h^{-1})$.*

Proof. Since each component of $G\times H$ is already a group, we can simply check

$$\begin{aligned}(a,b)\star((c,d)\star(e,f)) &= (a,b)\star(c*e,d\odot f) = (a*(c*e),b\odot(d\odot f))\\ &= ((a*c)*e,(b\odot d)\odot f) = (a*c,b\odot d)\star(e,f) = ((a,b)\star(c,d))\star(e,f)\end{aligned}$$

since $*$ and $\odot$ are associative. Then

$$(a,b)\star(e,e') = (a*e,b\odot e') = (a,b) = (e*a,e'\odot b) = (e,e')\star(a,b),$$

since e and e' are the identities for each slot. Similarly, we have

$$(g,h)\star(g^{-1},h^{-1}) = (g*g^{-1},h\odot h^{-1}) = (e,e') = (g^{-1}*g,h^{-1}\odot h) = (g^{-1},h^{-1})\star(g,h),$$

since g^{-1} and h^{-1} are the inverses for each slot. Thus $G\times H$ is indeed a group. □

Theorem 6.12. *Suppose $G_1,G_2,\dots,G_n$ are groups and let $(g_1,g_2,\dots,g_n)\in\prod_{i=1}^n G_i$. If $|g_i|=r_i<\infty$, then $|(g_1,g_2,\dots,g_n)|=\operatorname{lcm}(r_1,r_2,\dots,r_n)$.*

Proof. We need to find the smallest $k\in\mathbb{N}$ such that

$$(g_1,g_2,\dots,g_n)^k = (g_1^k,g_2^k,\dots,g_n^k) = (e_1,e_2,\dots,e_n).$$

Observe that $g^k=e_i$ for each i, so we have $r_i|k$ for every i. So $k\geq\operatorname{lcm}(r_1,r_2,\dots,r_n)$. But also

$$(g_1,g_2,\dots,g_n)^{\operatorname{lcm}(r_1,r_2,\dots,r_n)} = (g_1^{\operatorname{lcm}(r_1,r_2,\dots,r_n)},g_2^{\operatorname{lcm}(r_1,r_2,\dots,r_n)},\dots,g_n^{\operatorname{lcm}(r_1,r_2,\dots,r_n)}) = (e_1,e_2,\dots,e_n),$$

since $\operatorname{lcm}(r_1,r_2,\dots,r_n)$ is a multiple of r_i for every i. Thus $k=\operatorname{lcm}(r_1,r_2,\dots,r_n)$. □

Remark. Consider a bike lock with 4 dials. Suppose that we rotate each dial by n_i rotations each time, and we want to find how many times we need to rotate in order to return to the original position. We can write the symmetry group of this lock as

$$\mathbb{Z}_{10}\times\mathbb{Z}_{10}\times\mathbb{Z}_{10}\times\mathbb{Z}_{10}.$$

Then we can simply find the order of the each element and apply the above theorem.

Theorem 6.15. *The group $\mathbb{Z}_m\times\mathbb{Z}_n$ is cyclic if and only if m and n are relatively prime.*

Proof. ($\Leftarrow$) If $\gcd(m,n)=1$, then $\operatorname{lcm}(m,n)=mn$. Then look at $g=(1,1)$. The order of $1\in\mathbb{Z}_m$ is m and the order of $1\in\mathbb{Z}_n$ is n. So $|(1,1)|=mn=|\mathbb{Z}_m\times\mathbb{Z}_n|$ and thus $\mathbb{Z}_m\times\mathbb{Z}_n=\langle(1,1)\rangle$.

($\Rightarrow$) Suppose $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic. Then $nm = |\mathbb{Z}_m \times \mathbb{Z}_n| = |(x, y)|$ for some generator $(x, y) \in \mathbb{Z} \times \mathbb{Z}_n$. Then observe that x and y must individually generate $\mathbb{Z}_m$ and $\mathbb{Z}_n$, respectively, so $m = |x|$ and $n = |y|$. Then $nm = \text{lcm}(n, m)$, so $\gcd(m, n) = 1$ as desired. □

Lecture 16

Oct. 23 — Quotient Groups

Theorem 6.23 (Fundamental theorem of finitely-generated abelian groups)**.** *Let G be a finitely-generated abelian group.*[a] *Then*

$$G \cong \mathbb{Z}_{p_1^{n_2}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_m^{n_m}} \times \mathbb{Z}^k,$$

where $p_1, \dots, p_m$ are prime and are allowed to repeat.

[a] i.e. there exist $g_1, \dots, g_n \in G$ such that $\langle g_1, \dots, g_n \rangle = G$.

The idea behind the theorem is the following:

- Direct products allow us to build new, "bigger" groups.
- Given a *normal* subgroup $H \trianglelefteq G$, we can take the quotient to get a "smaller" group G/H.
- Every group contains cyclic subgroups.
- We expect the "building blocks" to be cyclic groups.

  However, note that this cannot possibly work for a general group since combining cyclic groups can only result in an abelian group.

For example, all abelian groups of order 24 (up to isomorphism) are

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4, \quad \mathbb{Z}_8 \times \mathbb{Z}_3 \, (\cong \mathbb{Z}_{24}),$$

since $24 = 2^3 \times 3$.

Remark. A group that has no nontrivial subgroups is called a *simple* group.

Recall that G/H treats H as the identity. Another way to write the familiar group D_4 is

$$D_n = \langle r, s \mid r^n = s^2 = e, \underbrace{rs = sr^{n-1}}_{rsrs=e} \rangle.$$

This is called the *generator-relation presentation* of D_n. Really, we are working with the *free group*

$$F = \langle r, s \rangle = \{\text{words in the letters } r,\, s,\, r^{-1},\, s^{-1}\}$$

with the normal subgroup $H = \langle r^n, s^2, rsrs \rangle \trianglelefteq F$. Then $D_n = F/H$.

Theorem 6.39. *We have the following.*

(a) For $n \geq 2$, $S_n/A_n \cong \mathbb{Z}_2$.

(b) For all $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

(c) For all $n \in \mathbb{N}$, $\mathbb{R}/n\mathbb{R} = \{e\}$.

Proof. (a) Notice that

$$|S_n/A_n| = |S_n|/|A_n| = 2,$$

so it must be isomorphic to $\mathbb{Z}_2$ since that is the only group of order 2 up to isomorphism.

(b) Take the isomorphism $\phi : \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ given by $r \mapsto r + n\mathbb{Z}$. For injectivity, let $r_1 \neq r_2$. Then

$$\phi(r_1) = r_1 + n\mathbb{Z} \neq r_2 + n\mathbb{Z} = \phi(r_2)$$

since we can consider $r_1, r_2 \in \mathbb{Z}$, after which the result follows from the fact that the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are disjoint. For surjectivity, notice that for any $r + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$, we can find some other representative $0 \leq r' < n$ such that $r + n\mathbb{Z} = r' + n\mathbb{Z}$. Then $\phi(r') = r + n\mathbb{Z}$ and ϕ is surjective. For the homomorphic property, observe that

$$\phi(r_1 + r_2) = (r_1 + r_2) + n\mathbb{Z} = (r_1 + n\mathbb{Z}) + (r_2 + n\mathbb{Z}) = \phi(r_1) + \phi(r_2)$$

by the rules of coset addition in $\mathbb{Z}/n\mathbb{Z}$. Thus ϕ is an isomorphism, and $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

(c) Observe that $n\mathbb{R} = \mathbb{R}$, so $\mathbb{R}/n\mathbb{R} = \mathbb{R}/\mathbb{R} = \{e\}$. □

Theorem 6.40. *Let G be a group and let $H \trianglelefteq G$. If G is abelian, then so is G/H.*

Proof. Take $aH, bH \in G/H$. Then

$$(aH)(bH) = (ab)H = (ba)H = (bH)(aH)$$

since G is abelian. □

Remark. The quotient G/H is not necessarily isomorphic to a subgroup of G. A counterexample is the quotient $\mathbb{Z}/n\mathbb{Z}$ for $\mathbb{Z}$. We have

$$|\mathbb{Z}/n\mathbb{Z}| = n < \infty,$$

but the only finite subgroup of $\mathbb{Z}$ is the trivial group.

Theorem 6.43. *Let G be a group and let $H \trianglelefteq G$. If G is cyclic, then so is G/H.*

Proof. Let $G = \langle g_0 \rangle$ for some $g_0 \in G$ since G is cyclic. Then $g = g_0^k$ for some k for any $g \in G$, so

$$gH = g_0^k H = (g_0 H)^k.$$

Namely, we have $G/H = \langle g_0 H \rangle$. □

Theorem 6.46. *Let G be a group. If $G/Z(G)$ is cyclic, then G is abelian.*

Proof. Recall that

$$Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}.$$

Now suppose that $G/Z(G) = \langle gZ(G)\rangle$ for some g. Then for any $a, b \in G$,

$$aZ(G) = (gZ(G))^{n_1} = g^{n_1}Z(G)$$
$$bZ(G) = (gZ(G))^{n_2} = g^{n_2}Z(G)$$

for some $n_1, n_2 \in \mathbb{Z}$. In particular, we have $a = g^{n_1}z_1$ and $b = g^{n_2}z_2$ for some $z_1, z_2 \in Z(G)$. Then

$$ab = g^{n_1}z_1g^{n_2}z_2 = z_1g^{n_1}g^{n_2}z_2 = z_1g^{n_2}g^{n_1}z_2 = g^{n_2}z_2g^{n_1}z_1 = ba$$

since z_1 and z_2 commute with everything and powers of g commute. Thus G is abelian. □

Lecture 17

Oct. 25 — Homomorphisms

Recall that we call groups *isomorphic* if they *"represent the same symmetries with different names."* An example is the map $D_3 \xrightarrow{\cong} S_3$ defined by

$$e \mapsto 1, \quad r \mapsto (123), \quad r^2 \mapsto (132),$$
$$s \mapsto (23), \quad rs \mapsto (12), \quad r^2 s \mapsto (13).$$

Other settings may not give exactly the same collection of symmetries, but we might still have some correspondence. For example, the map $D_4 \to S_4$ given by

$$r \mapsto (1234), \quad s \mapsto (12)$$

cannot be surjective. The map $\mathbb{Z} \to \mathbb{Z}_4$ given by

$$n \mapsto n \bmod 4$$

cannot be injective. The map $\mathbb{Z} \to D_4$ given by

$$n \mapsto r^n$$

is neither injective nor surjective. Yet they still all somehow *"respect composition."*

Definition 7.1. A **homomorphism** from $(G_1, *)$ to $(G_2, \odot)$ is a function $\phi : G_1 \to G_2$ such that

$$\phi(x * y) = \phi(x) \odot \phi(y)$$

for all $x, y \in G$.

Theorem 7.5. *Let $\phi : G_1 \to G_2$ be a homomorphism with $e_1 \in G_1, e_2 \in G_2$ as identity elements. Then*

(a) $\phi(e_1) = e_2$.

(b) For all $g \in G_1$, $[\phi(g)]^{-1} = \phi(g^{-1})$.

(c) For all $H \leq G_1$, $\phi(H) \leq G_2$.

Proof. (a) Pick $g \in G_1$. Then

$$\phi(g) = \phi(ge_1) = \phi(g)\phi(e_1).$$

Left-cancellation implies $e_2 = \phi(e_1)$.

(b) Observe that

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e_1) = e_2$$

and

$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_1) = e_2,$$

so indeed we have $[\phi(g)]^{-1} = \phi(g^{-1})$.

(c) We use the two-step subgroup test. First we have $e_2 = \phi(e_1) \in \phi(H)$, so $\phi(H)$ is nonempty. Now for inverses, observe that for any $g \in \phi(H)$, there exists $h \in H$ such that $\phi(h) = g$. Then $g^{-1} = \phi(h^{-1})$. Since $h^{-1} \in H$, we have $\phi(h^{-1}) \in \phi(H)$. For closure, take $g, g' \in \phi(H)$. There must exist $h, h' \in H$ such that $\phi(h) = g$ and $\phi(h') = g'$. Then

$$hh' \in H \implies \phi(hh^{-1}) \in \phi(H) \implies \phi(h)\phi(h') \in \phi(H) \implies gg' \in \phi(H).$$

So we have $\phi(H) \leq G_2$. □

Theorem 7.7. *Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. If $g \in G_1$ such that $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.*

Proof. Let $|g| = n < \infty$. Then $g^n = e_1$, which implies that

$$e_2 = \phi(e_1) = \phi(g^n) = [\phi(g)]^n.$$

So $|\phi(g)|$ divides n. □

Theorem 7.11. *Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Then* $\ker(\phi) \trianglelefteq G_1$.

Proof. We first show that $\ker(\phi) \leq G_1$ via the two-step subgroup test. First $\phi(e_1) = e_2$, so $e_1 \in \ker(\phi)$ and $\ker(\phi)$ is nonempty. Now for closure, let $g, h \in \ker(\phi)$. Then

$$\phi(gh) = \phi(g)\phi(h) = e_2 e_2 = e_2,$$

so $gh \in \ker(\phi)$ as well. For inverses, let $g \in \ker(\phi)$. Then

$$\phi(g^{-1}) = [\phi(g)]^{-1} = e_2^{-1} = e_2,$$

so $g^{-1} \in \ker(\phi)$. Now we show that $\ker(\phi) \trianglelefteq G_1$ by showing that $g\ker(\phi)g^{-1} \subseteq \ker(\phi)$ for any $g \in G_1$. To this end, take any $g \in G_1$ and $h \in \ker(\phi)$. Then

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_1) = e_2,$$

so $ghg^{-1} \in \ker(\phi)$. Thus $g\ker(\phi)g^{-1} \subseteq \ker(\phi)$ and $\ker(\phi) \trianglelefteq G_1$. □

Theorem 7.12. *Let G be a group and let $H \trianglelefteq G$. Then the map $\gamma : G \to G/H$ is a homomorphism with* $\ker(\gamma) = H$. *This map is called the* ***canonical projection map***.

Proof. First we show that γ is indeed a homomorphism. Let $g, h \in G$. Then

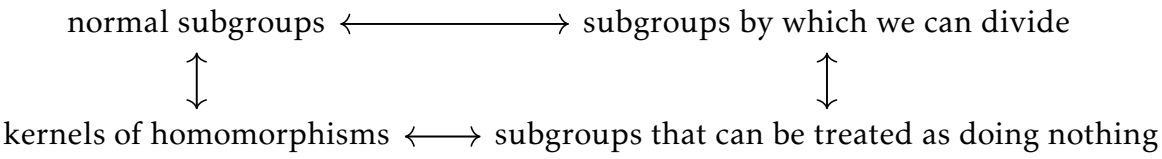
$$\gamma(gh) = (gh)H = (gH)(hH) = \gamma(g)\gamma(h)$$

by the rules of coset multiplication. Now we show that $\ker(\gamma) = H$. For this, note that

$$\gamma(g) = gH = H,$$

i.e. $g \in \ker(\gamma)$, if and only if $g \in H$. So $\ker(\gamma) = H$. □

Remark. This means that:



Problem 7.16. Suppose $\phi : Q_8 \to V_4$ is a group homomorphism satisfying $\phi(i) = h$ and $\phi(j) = v$.

(a) Find $\phi(1)$, $\phi(-1)$, $\phi(k)$, $\phi(-i)$, $\phi(-j)$, and $\phi(-k)$.

(b) Find $\ker(\phi)$.

(c) What well-known group is $Q_8/\ker(\phi)$ isomorphic to?

Solution. (a) First observe that

$$\phi(-1) = \phi(i^2) = \phi(i)\phi(i) = hh = e.$$

From this we have $\phi(1) = \phi(-1) = e$. Then we also have

$$\phi(-k) = \phi(k) = \phi(ij) = \phi(i)\phi(j) = hv$$

and $\phi(-i) = h$, $\phi(-j) = v$.

(b) From Part (a) we can see that $\ker(\phi) = \langle -1 \rangle = \{1, -1\}$.

(c) We have

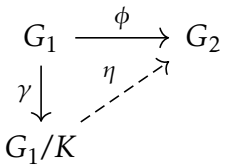
$$Q_8/\ker(\phi) = Q_8/\langle -1 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong V_4.$$

A possible isomorphism $\widetilde{\phi} : Q_8/\ker(\phi) \to V_4$ is given by $x\ker(\phi) \mapsto \phi(x)$. □

Lecture 18

Oct. 30 — The Isomorphism Theorems

Theorem 7.21 (First isomorphism theorem)**.** *Given a homomorphism of groups $\phi : G_1 \to G_2$ with $K = \ker \phi$, there exists a unique isomorphism $\eta : G_1/K \to \phi(G_1)$ such that this diagram commutes:*



i.e. $\phi = \eta \circ \gamma$, where $\gamma(g) = gK$ is the canonical projection.

Proof. We define $\eta : G_1/K \to \phi(G_1)$ in the obvious way by

$$\eta(gK) = \phi(g).$$

First we check that η is well-defined. Suppose that $g_1K = g_2K$ are two representatives of the same coset. We need to show that $\eta(g_1K) = \eta(g_2K)$. Note that

$$g_1K = g_2K \implies g^{-1}g_2 \in K,$$

so $\phi(g_1^{-1}g_2) = e_2 \in G_2$. Then

$$e_2 = \phi(g^{-1}g_2) = [\phi(g_1)]^{-1}\phi(g_2),$$

so $\phi(g_1) = \phi(g_2)$, which means that $\eta(g_1K) = \eta(g_2K)$ as desired. Now we show that η is injective. Suppose $\eta(g_1K) = \eta(g_2K)$, so that $\phi(g_1) = \phi(g_2)$. So

$$\phi(g_1^{-1}g_2) = [\phi(g_1)]^{-1}\phi(g)2 = e_2 \in G_2,$$

which means that $g^{-1}g_2 \in K$, or $g_1K = g_2K$. For surjectivity, note that for any $h \in \phi(G_1)$, there exists $g \in G_1$ such that $\phi(g) = h$. Then $\eta(gK) = \phi(g) = h$, so ϕ is surjective. For the homomorphic property, take any $gK, hK \in G_1/K$. Then we have

$$\eta(gK)\eta(hK) = \phi(g)\phi(h) = \phi(gh) = \eta(ghK) = \eta((gK)(hK)),$$

as required. So η is the desired isomorphism. □

Remark. The idea is: If $\phi(G_1)$ is hard to study, then look at $G_1/\ker(\phi)$ instead, or vice versa.

For example, define the map $\phi : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ by

$$t \mapsto \cos(2\pi t) + i \sin(2\pi t).$$

Here $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ is the punctured complex plane. The claim is that ϕ is a homomorphism with

$$\phi(\mathbb{R}) = S^1 = \text{unit circle in } \mathbb{C}$$

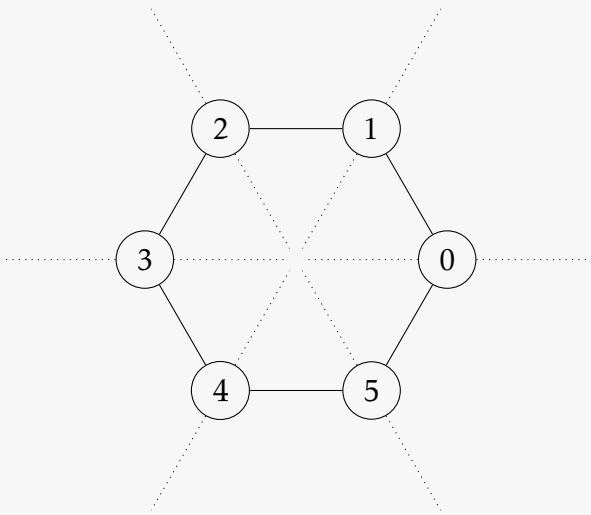
and $\ker \phi = \mathbb{Z}$. Then by the first isomorphism theorem, we have $\mathbb{R}/\mathbb{Z} \cong S^1$.

Problem 7.22. Let $\phi : Q_8 \to V_4$ be the homomorphism described in Problem 7.16. Use the First Isomorphism Theorem to prove that $\mathbb{Q}/\langle -1 \rangle \cong V_4$.

Solution. Recall that $\ker \phi = \langle -1 \rangle$ from Problem 7.16. We can also clearly see from our computations back then that $\phi(Q_8) = V_4$, so $\mathbb{Q}/\langle -1 \rangle \cong V_4$ by the first isomorphism theorem. □

Problem 7.24. Use the First Isomorphism Theorem to prove that $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$. Attempt to draw a picture of this using Cayley diagrams.

Solution. We can use the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_6$ given by $\phi(r) = r \bmod 6$. We can clearly see that $\phi(\mathbb{Z}) = \mathbb{Z}_6$ and $\ker \phi = 6\mathbb{Z}$, so $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$ by the first isomorphism theorem. Here



is an attempt at a Cayley diagram, where the lines indicate the missing parts of a coset of $\mathbb{Z}_6$. □

Lecture 19

Nov. 1 — Group Actions

The key question that the *second isomorphism theorem* addresses is:

> What happens to a subgroup $H \leq G$ when we crush out $N \trianglelefteq G$ to get G/N?

For example, let $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$ and $N = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \{0\}$. Then

$$G/N \cong \mathbb{Z}_4,$$

but what happens to $H = \{0\} \times \mathbb{Z}_3 \times \mathbb{Z}_4$?

The problem here is that in general we may have have $N \not\subseteq H$, so we cannot simply take H/N. Then some possible solutions are:

1. Grow N to get
$$HN = \{hn : h \in H, n \in N\},$$
the smallest group containing both H and N, then crush N.

   Result: HN/N. (In general $HN/N \ncong H$.)

2. Crush $H \cap N$ out of H.

   Result: $H/(H \cap N)$.

Theorem 7.29 (Second isomorphism theorem)**.** $HN/N \cong H/(H \cap N)$.

Proof. First observe that we can easily get $N \trianglelefteq HN$ from the fact that $N \trianglelefteq G$. Now we claim that $\phi : H \to HN/N$ given by

$$h \mapsto hN$$

is a surjective homomorphism with $\ker\phi = H \cap N$. Note that this simultaneously shows that $H \cap N = \ker\phi \trianglelefteq H$. For the homomorphic property, observe that

$$\phi(xy) = (xy)N = (xN)(yN) = \phi(x)\phi(y).$$

For surjectivity, let $x \in HN$. Then $x = hn$ for some $h \in H$ and $n \in N$. Then

$$NH/N \ni xN = (hn)N = hN$$

so $\phi(h) = hN = xN$. Now we check that $\ker\phi = H \cap N$. For this, let $h \in \ker\phi \subseteq H$. Then

$$\phi(h) = hN = N,$$

so $h \in N$. So $h \in H \cap N$ and thus $\ker\phi \subseteq H \cap N$. The reverse inclusion is identical, so $\ker\phi = H \cap N$. Finally we apply the first isomorphism theorem to conclude that $HN/N \cong H/(H \cap N)$. □

Definition. We say that a group G **acts on** a set X if we have a homomorphism $\phi : G \to S_X$, where S_X is the symmetry group of X. We call ϕ a **group action** and X a G-**set**.

For example, let $G = D_n$ and

$$X = \{\text{configurations of an } n\text{-gon}\}.$$

Then G acts on X in the natural way.

Definition. Let X be a G-set. Call x_1 G-**equivalent** to x_2 if there exists $g \in G$ such that

$$g.x_1 = x_2.$$

Here $g.x_1$ means "g applied to x_1".

Remark. In fact G-equivalence is an equivalence relation.

Definition. Let X be a G-set. The G-equivalence class of $x \in X$ is called the **orbit** of x, written $\mathcal{O}_x \subseteq X$. The **stabilizer subgroup** of $x \in X$ is

$$G_x := \{g \in G \mid g.x = x\}.$$

The **fixed-point set** of $g \in G$ is

$$X_g := \{x \in X \mid g.x = x\}.$$

Remark. We have $x \in X_g$ if and only if $g \in G_x$.

For example, let

$$G = \mathrm{GL}_n(\mathbb{R}) = \{\text{invertible } n \times n \text{ matrices}\}$$

and $X = \mathbb{R}^n$. Pick $\vec{v} \in \mathbb{R}^n$, then

$$G_{\vec{v}} = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A\vec{v} = \vec{v}\}.$$

Lecture 20

Nov. 6 — More Group Actions

Remark. Stabilizer subgroups of two elements in the same orbit are not necessarily the same, but they are *conjugate* to each other.

Proposition 3. *Let X be a G-set, for some group G, and fix $x \in X$. Then G_x is a subgroup of G.*

Proof. We show this via the two-step subgroup test. First $e \in G_x$ since $e.x = x$, so G_x is nonempty. For inverses, let $g \in G_x$. Then

$$x = e.x = (g^{-1}g).x = g^{-1}.(g.x) = g^{-1}.x$$

since g fixes x. So $g^{-1} \in G_x$. For closure, let $g, h \in G_x$. Then

$$(gh).x = g.(h.x) = g.x = x$$

since g and h both individually fix x. So $gh \in G_x$, and thus G_x is a subgroup. □

Theorem 5 (Orbit-stabilizer theorem)**.** *Let X be a G-set. Then $|\mathcal{O}_x| = [G : G_x]$ for any $x \in X$.*

Proof. Define $\phi : \mathcal{O}_x \to \mathcal{L}_{G_x}$ by

$$y \mapsto gG_x,$$

where $y = g.x$. Note that g exists since $y \in \mathcal{O}_x$. Also here $\mathcal{L}_{G_x}$ is the set of left cosets of G_x in G.

First we show that ϕ is well-defined. Suppose

$$g_1.x = g_2.x = y.$$

Then we want to show that $g_1G_x = g_2G_x$. Observe that applying g_1^{-1} gives

$$x = e.x = (g_1^{-1}g_1).x = g_1^{-1}.(g_1.x) = g_1^{-1}.(g_2.x) = (g_1^{-1}g_2).x$$

since $g_1.x = g_2.x$. So we have $g^{-1}g_2 \in G_x$, which means that $g_1G_x = g_2G_x$, as desired.

For injectivity, suppose that $\phi(y_1) = \phi(y_2)$ for some $y_1, y_2 \in G_x$. Let $y_1 = g_1.x$ and $y_2 = y_2.x$. Then $g_1G_x = g_2G_x$ implies that $g_1 \in g_2G_x$, and thus $g_1 = g_2h$ for some $h \in G_x$. Then

$$g_1.x = (g_2h).x = g_2.x$$

since h fixes x, so $y_1 = y_2$.

For surjectivity, let $gG_x \in \mathcal{L}_{G_x}$. Observe that $y = g.x \in \mathcal{O}_x$ satisfies $\phi(y) = gG_x$, so ϕ is indeed surjective. Thus ϕ is a bijection from $\mathcal{O}_x$ to $\mathcal{L}_{G_x}$, and we conclude that $|\mathcal{O}_x| = |\mathcal{L}_{G_x}|$. □

Lecture 21

Nov. 8 — Even More Group Actions

Remark. The conjugacy class of $\sigma \in S_n$ is determined by its cycle structure. E.g. for D_4 we have

$$\mathcal{O}_{(12)} = \{(12),(13),(14),(23),(24),(34)\}, \quad \mathcal{O}_{(12)(34)} = \{(12)(34),(13)(24),(14)(23)\}.$$

For example, we have $(13) = (23)(12)(23)^{-1}$, $(14) = (24)(12)(24)^{-1}$, and $(34) = ((13)(24))(12)((13)(24))^{-1}$.

Remark. Group elements $g_1, g_2 \in G$ are conjugate if they *"do the same thing with different labels."* Here, think similar matrices. Recall linear algebra: $A \sim B$ if $A = SBS^{-1}$ for some invertible S. Then A and B represent the same linear transformation in different bases.

Theorem 6 (The class equation)**.** *Suppose G is a finite group with r distinct conjugacy classes represented by $g_1, g_2, \ldots, g_r$. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)].$$

Proof. Recall that any G-set is partitioned by its orbits. In the conjugacy action of G on itself, each element of $Z(G)$ is its own orbit:

$$h \in Z(G) \implies \mathcal{O}_h = \{g.h \mid g \in G\} = \{ghg^{-1} \mid g \in G\} = \{gg^{-1}h \mid g \in G\} = \{h\}.$$

So we have the following disjoint union for G:

$$G = Z(G) \sqcup \bigsqcup_{i=1}^{r} \mathcal{O}_{g_i}.$$

Therefore,

$$|G| = |Z(G)| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}| = |Z(G)| + \sum_{i=1}^{r} [G : G_{g_i}] = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]$$

by the orbit-stabilizer theorem and noting that

$$G_x = \{g \in G \mid g.x = x\} = \{g \in G \mid gxg^{-1} = x\} = C_G(x)$$

under the conjugacy action of G on itself. □

Theorem 7. *Any group of prime-power order has nontrivial center.*

Proof. By the class equation, we have

$$p^n = |G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)] = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(g_i)|} = |Z(G)| + \sum_{i=1}^{r} \frac{p^n}{|C_G(g_i)|}$$

since G is finite. Observe that we cannot have $|C_G(g_i)| = p^n$ since that would imply $C_G(g_i) = G$, which means that $g_i \in Z(G)$ (as we have discussed previously, any $g \in Z(G)$ is in its own orbit). Then everything else in the equation is divisible by p, so $|Z(G)|$ must be divisible by p as well. Then $|Z(G)| > 1$ and we conclude that $Z(G)$ is nontrivial. □

Lemma 9. *Let X be a G-set and suppose that $x \sim_G y$. Then G_x is isomorphic to G_y.*

Proof. First observe that since $x \sim_G y$, there must exist some $h \in G$ such that $h.x = y$. Then we can define $\phi : G_x \to G_y$ by

$$g \mapsto hgh^{-1},$$

which we will show is an isomorphism. First observe that ϕ satisfies the homomorphic property since we have previously show that the conjugation map is an isomorphism. It also follows from this that $\ker \phi = \{e\}$, so ϕ is injective. Then it just remains to show that $\phi(G_x) = G_y$. For this, observe that if $g \in G_x$, i.e. $g.x = x$, then

$$hgh^{-1}.y = hg.x = h.x = y$$

where we noted that $h^{-1}.y = x$. So $\phi(g) = hgh^{-1} \in G_y$ as desired. This means that $\phi(G_x) \subseteq G_y$. For the reverse inclusion, let $g' \in G_y$, i.e. $g'.y = y$. Then

$$h^{-1}g'h.x = h^{-1}g'.y = h^{-1}.y = h^{-1}.hx = x,$$

so $\phi^{-1}(g') = h^{-1}g'h \in G_x$. So $G_y \subseteq \phi(G_x)$ and $\phi(G_x) = G_y$, which means that ϕ is an isomorphism from G_x to G_y. Thus we conclude that $G_x \cong G_y$, as desired. □

Remark. For finite G, we can use the fact that $|G_x| = |G_y|$ for $y \in \mathcal{O}_x$ by the orbit-stabilizer theorem.

Lecture 22

Nov. 15 — Rings

Definition 8.1. A **ring** is a triple $(R, +, \cdot)$ such that

1. $(R, +)$ is an abelian group,
2. $\cdot$ is an associative binary operation,
3. and distributive laws hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Theorem 8.2. *If R is a ring, then for all $a, b \in \mathbb{R}$:*

(a) $0a = a0 = 0$

(b) $(-a)b = a(-b) = -(ab)$

(c) $(-a)(-b) = ab$

Proof. (a) Observe that $a0 = a(0 + 0) = a0 + a0$. Then adding the additive inverse of $a0$ to both sides yields

$$0 = a0 + (-a0) = a0 + a0 + (-a0) = a0.$$

So $0 = a0$ as desired, and a similar proof shows that $0a = 0$.

(b) Note that

$$ab = (-a)b = (a + (-a))b = 0b = 0,$$

so $-(ab) = (-a)b$. Once again, a similar proof shows $a(-b) = -(ab)$.

(c) Using Part (b), we have

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab.$$

Note that we used $-(-x) = x$, which is a fact about additive inverses that we already have. □

Remark. Part (a) of this theorem shows that 0 cannot have a multiplicative inverse.

Theorem 8.9. *If R is a ring with 1, then the multiplicative identity is unique and $-a = (-1)a$.*

Proof. For uniqueness, let e and f both be multiplicative identities. Then $e = ef = f$. For the latter part, simply note that $(-1)a = -(1a) = -a$. □

Here are some more definitions:

- A **commutative** ring is one where $\cdot$ is commutative.
- If $a, b \in R$ are nonzero elements such that $ab = 0$, then we call a and b **zero divisors**.
- If $b \in R$ satisfies $ab = ba = 1$, then we call b the **multiplicative inverse** of a, written a^{-1}.
- A **division ring** is a ring where every nonzero element has a multiplicative inverse.
- A **field** is a commutative division ring.
- An **integral domain** is a ring that has no zero divisors.

The following are some examples of rings:

- $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$: These are commutative division rings, a.k.a. fields.
- $M_{n\times n}(\mathbb{R})$, $M_{n\times n}(R)$: These are not commutative and have zero divisors.
- $\mathbb{Z}_n$: These are commutative and form a field precisely when n is prime.
- $\mathbb{Z}$: This is commutative, has no zero divisors, but most elements are not invertible. This is an example of an integral domain.
- $P[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{R}\}$, $\{p(x)/q(x) \mid p, q \in P[x], q \neq 0\}$: The former is the polynomial ring over $\mathbb{R}$ (which is an integral domain), and the latter is the field of rational functions over $\mathbb{R}$.

Theorem 8.20. *If $U(R) \neq \varnothing$, then $U(R)$ forms a group under multiplication.*

Proof. First note that the multiplication on $U(R)$ is clearly associative as it is inherited from R. To check closure, observe that for $a, b \in U(R)$, we have elements $a^{-1}, b^{-1} \in R$. Since R is a ring, we have $b^{-1}a^{-1} \in R$, which gives

$$(ab)(b^{-1}a^{-1}) = aa^{-1} = 1,$$

so we indeed have $ab \in U(R)$. For the identity element, we simply note that 1 is a unit, so $1 \in U(R)$. For inverses, observe that for any $a \in U(R)$, a^{-1} exists and $(a^{-1})^{-1} = a$, so $a^{-1} \in U(R)$. □

Lecture 23

Nov. 20 — Ring Homomorphisms

Definition 8.27. For a ring $(R, +, \cdot)$, we call $S \subseteq R$ a **subring** if $(S, +, \cdot)$ is also a ring.

Problem 8.31. Suppose R is a ring and let $a \in R$. Define $S = \{x \in R \mid ax = 0\}$. Prove that S is a subring of R.

Solution. We check that S is nonempty, S is closed under subtraction, and S is closed under multiplication. To see that $S \neq \varnothing$, obvserve that $a0 = 0$ for any $a \in R$, so $0 \in S$. For closure under subtraction, let $x, y \in S$. Then $ax = ay = 0$, so we have

$$a(x - y) = ax - ay = 0 - 0 = 0,$$

so $x - y \in S$. For closure under multiplication, note that

$$a(xy) = (ax)y = 0y = 0,$$

so $xy \in S$. Thus S is a subring of R. □

Definition 8.33. A **homomorphism of rings** is a map $\phi : R \to S$ such that for all $r_1, r_2 \in R$, we have

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \quad \text{and} \quad \phi(r_1 r_2) = \phi(r_1)\phi(r_2).$$

We also define the **kernel** of ϕ to be $\ker \phi = \{r \in R \mid \phi(r) = 0\}$.

For example, for

$$R = \mathbb{Z}[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{Z}\}$$

and $S = \mathbb{Z}$, we can define $\phi : R \to S$ by $p(x) \mapsto p(0)$. Then

$$\ker \phi = \{a_1 x + a_2 x^2 + \cdots + a_n x^n \mid a_i \in \mathbb{Z}\},$$

i.e. all the polynomials with constant term zero.

Theorem 8.36. *Let $\phi : R \to S$ be a ring homomorphism.*

(a) *$\phi(R)$ is a subring of S.*

(b) *$\ker(\phi)$ is a subring of R.*

Proof. (a) For closure under $-$ and $\cdot$, take $a, b \in \phi(R)$. Then we can find $x, y \in R$ such that $\phi(x) = a$ and $\phi(y) = b$. Then

$$a - b = \phi(x) - \phi(y) = \phi(x - y) \in \phi(R)$$

via the homomorphic property. Similarly

$$ab = \phi(x)\phi(y) = \phi(xy) = \phi(R).$$

Finally $\phi(R)$ is nonempty since R is nonempty, so $\phi(R)$ is indeed a subring of S.

(b) For closure under $-$ and $\cdot$, take $a, b \in \ker\phi$ and note that

$$\phi(a - b) = \phi(a) - \phi(b) = 0_S - 0_S = 0_S$$

and that

$$\phi(ab) = \phi(a)\phi(b) = 0_S 0_S = 0_S.$$

Finally $\ker\phi$ is nonempty since $\phi(0_R) = 0_S$, so that $0_R \in \ker\phi$. Thus $\ker\phi$ is a subring of R. □

Remark. Subrings of the form $\ker\phi$ are extra special, since we can divide by them. Note that this is different from a subring being normal now, since *all* additive subgroups are now normal due to the additive group of a ring being abelian.

Theorem 8.38. *Let $\phi : R \to S$ be a ring homomorphism. If $\alpha \in \ker(\phi)$ and $r \in R$, then $\alpha r, r\alpha \in \ker(\phi)$. That is, $\ker(\phi)$ is closed under multiplication by elements of R.*

Proof. Note that $\phi(\alpha) = 0$, so

$$\phi(r\alpha) = \phi(r)\phi(\alpha) = \phi(r)0 = 0 = 0\phi(r) = \phi(\alpha)\phi(r) = \phi(\alpha r).$$

Thus we have $\alpha r, r\alpha \in \ker\phi$. □

Problem 1. If $\phi : R \to S$ is a homomorphism of rings, describe a ring structure of $R/\ker\phi$. You need to:

(a) Describe the elements of the set $R/\ker\phi$.

(b) Define operations on the set.

(c) Prove that these operations satisfy the definition of a ring.

Solution. (a) Define the elements of $R/\ker\phi$ to be the additive cosets of $\ker\phi$ in R.

(b) For $a + \ker\phi, b + \ker\phi \in R/\ker\phi$, define addition to be

$$(a + \ker\phi) + (b + \ker\phi) = (a + b) + \ker\phi$$

We have already checked that this is well-defined when verifying that $R/\ker\phi$ is a valid quotient group. We can similarly define multiplication to be

$$(a + \ker\phi)(b + \ker\phi) = (ab) + \ker\phi.$$

This is well-defined since for $r, s \in \ker\phi$, we have

$$(a + r + \ker\phi)(b + s + \ker\phi) = (ab) + (as + br + rs) + \ker\phi = (ab) + \ker\phi,$$

where $as, br, rs \in \ker\phi$ by Theorem 8.38.

(c) We first note that the additive cosets are already known to form a quotient group, so we just need to verify that the multiplication is associative, closed, and distributes over addition. For associativity, note that for $a, b, c \in R$,

$$\begin{aligned}((a + \ker\phi)(b + \ker\phi))(c + \ker\phi) &= (ab + \ker\phi)(c + \ker\phi) = (abc) + \ker\phi \\ &= (a + \ker\phi)(bc + \ker\phi) = (a + \ker\phi)((b + \ker\phi)(c + \ker\phi)),\end{aligned}$$

where we used the fact that the multiplication in R is associative. For closure, note that

$$(a + \ker\phi)(b + \ker\phi) = (ab) + \ker\phi,$$

which is also an additive coset of $\ker\phi$ since $ab \in R$. Finally, for distributivity, note that

$$\begin{aligned}(a + \ker\phi)((b + \ker\phi) + (c + \ker\phi)) &= (a + \ker\phi)((b + c) + \ker\phi) \\ &= (a(b + c)) + \ker\phi \\ &= (ab + ac) + \ker\phi \\ &= (ab + \ker\phi) + (ac + \ker\phi) \\ &= (a + \ker\phi)(b + \ker\phi) + (a + \ker\phi)(c + \ker\phi)\end{aligned}$$

since the distributive laws hold in R. We can similarly show that distributivity works on the other side, so $R/\ker\phi$ is indeed a ring. □

Problem 2. Explain why the structure defined above does not work for $\mathbb{Q}/\mathbb{Z}$.

Solution. We can take $a = 1/2$ and $b = 1/3$. For the representative $z_0 = 0$, we have

$$(a + z_0)(b + z_0) = \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6} \in \frac{1}{6} + \mathbb{Z}.$$

However, for the representative z_1, we have

$$(a + z_1)(b + z_1) = \frac{3}{2} \cdot \frac{4}{3} = \frac{4}{2} = 2 \in \mathbb{Z}.$$

These are in different cosets, so this multiplication is not well-defined. □

Lecture 24

Nov. 27 — Ideals and Quotient Rings

The key idea here is: What kind of $I \subseteq R$ can we replace $\ker \phi$ by to make R/I a ring?

Definition 8.39. We call a subring $I \subseteq R$ an **ideal** if $rI \subseteq I$ and $Ir \subseteq I$ for all $r \in R$.

Theorem 8.40. *Let R be a ring and let I be an ideal of R. Then the additive quotient group R/I is a ring under the binary operations:*

$$(r+I)+(s+I) = (r+s)+I$$
$$(r+I)(s+I) = (rs)+I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well-defined, then I is an ideal of R.

Proof. ($\Rightarrow$) First we show that $(R/I, +)$ is an abelian group. Since I is an ideal, we observe that it is an additive subgroup of R. Also R is abelian as an additive group, so $I \trianglelefteq R$ and R/I is an abelian subgroup. This also includes the fact that $+$ is well-defined. For multiplication, take $a, b \in R$ and arbitrary representatives $r, s \in I$. Then

$$(a+r+I)(b+s+I) = (ab)+(as+br+rs)+I = (ab)+I$$

since $as, br, rs \in I$ by the definition of an ideal. So the multiplication is well-defined. For associativity, let $r, s, k \in R$. Then

$$((r+I)(s+I))(k+I) = (rs+I)(k+I) = (rsk)+I = (r+I)(sk+I) = (r+I)((s+I)(k+I))$$

since the multiplication in R is associative. For the distributive property, we have

$$\begin{aligned}(r+I)((s+I)+(k+I)) &= (r+I)(s+k+I) = (rs+rk)+I \\ &= (rs+I)+(rk+I) = (r+I)(s+I)+(r+I)(k+I)\end{aligned}$$

since the distributive property holds in R. Distributivity on the other side is similar, so the additive quotient group R/I indeed forms a ring.

($\Leftarrow$) Suppose that the above operations are well-defined. Then for any $a, b \in R$ and $r, s \in I$, we have

$$(a+r+I)(b+s+I) = (ab)+I$$

Since I is already a subgroup of R, all we need to show is that $br \in I$ and $rb \in I$ for any $b \in R$ and $r \in I$. To see this, simply take $a = s = 0$ in the above equations to get

$$(r + I)(b + I) = (rb) + I = I$$

since $a = 0$ implies $ab = 0$. But this means $rb \in I$. Taking $r = b = 0$ gives $br \in I$, so I is an ideal. □

Theorem 8.43 (First Isomorphism Theorem for Rings)**.** *If $\phi : R \to S$ is a ring homomorphism, then* $\ker(\phi)$ *is an ideal of R and $R/\ker(\phi) \cong \phi(R)$.*

Proof. Note that we have already previously shown that $\ker\phi$ is an ideal of R (Theorem 8.38). Now define $\psi : R/\ker\phi \to S$ by $r + \ker\phi \mapsto \phi(r)$. This is already a well-defined map since R and $\ker\phi$ are also additive groups, so we can appeal to the first isomorphism theorem for groups. This also shows injectivity and that ψ is a group homomorphism. So it only remains to show that ψ is a ring homomorphism, i.e. that

$$\psi(r + \ker\phi)\psi(s + \ker\phi) = \psi(rs + \ker\phi).$$

To see this, observe that

$$\psi(r + \ker\phi)\psi(s + \ker\phi) = \phi(r)\phi(s) = \phi(rs) = \psi(rs + \ker\phi)$$

since ϕ is a ring homomorphism. So $R/\ker\phi \cong \phi(R)$. □

Definition 8.45. Given a subset $A \subseteq R$, the **ideal generated by** A, denoted (A), is the smallest ideal of R containing A. We call an ideal $I \subseteq R$ **principal** if $I = (\{a\})$ for some $a \in R$.

Remark. Normal subgroups are to ideals as cyclic subgroups are to principal ideals.

Theorem 8.49. *Assume R is a commutative ring with $1 \neq 0$. Let I be an ideal of R. Then $I = R$ if and only if I contains a unit.*

Proof. ($\Rightarrow$) If $I = R$, then $1 \in R = I$ is a unit.

($\Leftarrow$) Let $x \in I$ be a unit, then $1 = xx^{-1} \in I$. So $R = (1) \subseteq I$ and $R = I$. □

Remark. We may not have needed the commutativity assumption in this theorem.

Theorem 8.50. *Assume R is a commutative ring with $1 \neq 0$. Then R is a field if and only if its only ideals are (0) and R.*

Proof. ($\Rightarrow$) Take any ideal $I \neq (0)$. Then there exists $a \in I$, $a \neq 0$. Since R is a field, a is a unit and thus $I = R$ by Theorem 8.49.

($\Leftarrow$) Take any $a \in R$, $a \neq 0$. Since (0) and R are the only ideals, we must have $(a) = R$, so there exists an $r \in R$ such that $ra = 1$. So a is a unit and thus R is a field. □

Lecture 25

Nov. 29 — Maximal and Prime Ideals

Remark. We have {fields} $\subsetneq$ {integral domains} $\subsetneq$ {commutative rings}.

Definition 8.52. An ideal $M \subseteq R$ is **maximal** if the only ideals of R containing M are M and R.

Theorem 8.55. *Assume R is a commutative ring with 1. Then M is a maximal ideal if and only if the quotient ring R/M is a field.*

Proof. ($\Rightarrow$) Define $\psi : R \to R/M$ by $r \mapsto r + M$, and pick an ideal $J \subseteq R/M$. Note that $\psi^{-1}(J) \subseteq R$ is an ideal and $M \subseteq \psi^{-1}(J)$. So either $\psi^{-1}(J) = M$ or $\psi^{-1}(J) = R$ since M is maximal, which implies either $J = (0)$ or $J = R$. Then R/M is a field by Theorem 8.50.

($\Leftarrow$) Suppose $M \subseteq M'$ for some ideal M'. Then $\psi(M')$ is an ideal, so either $\psi(M') = (0)$ or $\psi(M') = R/M$. Then either $M' = M$ or $M' = R$, so M is maximal. □

Remark. We have {maximal ideals} $\subsetneq$ {prime ideals} $\subsetneq$ {ideals}. In particular, taking a quotient by a maximal ideal yields a field, a quotient by a prime ideal yields an integral domain, and a quotient by an general ideal yields a commutative ring.

Theorem 8.60. *Assume R is a commutative ring with 1. Then P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.*

Proof. ($\Rightarrow$) Assume $P \subseteq R$ is a prime ideal and suppose that

$$(a + I)(b + I) = ab + I = 0 + I \in R/I.$$

Note that this means $ab \in I$. Then we want to show that either $a + I = I$ or $b + I = I$, i.e. that either $a \in I$ or $b \in I$. But I is prime, so $ab \in I$ implies either $a \in I$ or $b \in I$.

($\Leftarrow$) Assume R/P is an integral domain and suppose that $ab \in I$. Then we need to show that $a \in I$ or $b \in I$. Since $ab \in I$, we have

$$0 + I = ab + I = (a + I)(b + I).$$

Since R/I is an integral domain, either $a + I = I$ or $b + I = I$, so either $a \in I$ or $b \in I$. □

Corollary 8.61. *All maximal ideals are prime.*

Proof. All fields are integral domains. □

Lecture 26

Dec. 4 — Review

Problem 12. Let G be a group, and denote by $Z(G)$ the center of G. Prove that if $G/Z(G)$ is cyclic, then G is abelian.

Solution. Refer to the proof of Theorem 6.46. □

Problem 38. Let R be the ring of all continuous functions from the closed interval $[0,1]$ to $\mathbb{R}$ and for each $c \in [0,1]$ let $M_c = \{f \in R \mid f(c) = 0\}$.

(a) Prove that M_c is a maximal ideal of R.

Hint: Construct a surjective homomorphism $\phi : R \to \mathbb{R}$ whose kernel is M_c.

(b) Prove that if M is *any* maximal ideal of R, then there is a real number $c \in [0,1]$ such that $M = M_c$.

(c) Prove that if b and c are distinct points in $[0,1]$, then $M_b \neq M_c$.

(d) Prove that M_c is not equal to the principal ideal generated by $x - c$.

Solution. (a) Define the evaluation map $\phi_c : R \to \mathbb{R}$ by $f \mapsto f(c)$, where function addition and multiplication are defined pointwise, i.e.

$$(f+g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x).$$

Checking the homomorphic properties follows immediately from this:

$$\phi_c(f+g) = (f+g)(c) = f(c) + g(c) = \phi_c(f) + \phi_c(g)$$

and

$$\phi_c(fg) = (fg)(c) = f(c)g(c) = \phi_c(f)\phi_c(g).$$

For surjectivity, note that for any $a \in \mathbb{R}$, the constant function $f(x) = a$ satisfies $\phi(f) = f(c) = a$. So $\phi(R) = \mathbb{R}$. We also have $\ker \phi_c = M_c$, since $f(c) = 0$ precisely when $f \in M_c$. Then by the first isomorphism theorem we have $R/M_c \cong \mathbb{R}$. Since $\mathbb{R}$ is a field, M_c must be maximal.

(b) Suppose $M \subseteq R$ is some ideal which is not contained in any ideal of the form M_c. Then for each $c \in [0,1]$, there exists some $f_c \in M$ such that $f_c(c) \neq 0$. Since f_c is continuous, there in fact exists an open interval I_c containing c on which f_c is nonzero. Then the set $\{I_c \mid c \in [0,1]\}$

is an open cover of $[0,1]$. Since $[0,1]$ is compact, we can find a finite subcover $I_1,\dots,I_n$ with corresponding functions $f_1,\dots,f_n$. Then take the function

$$f = f_1^2 + \cdots + f_n^2,$$

which vanishes nowhere on $[0,1]$ since some f_j does not vanish at any given point and $f_i^2 \geq 0$ for all i. Furthermore $f \in M$ since M is an ideal and thus closed under addition and multiplication of its elements. Also f is continuous since it is a sum of products of continuous functions. Since f vanishes nowhere on $[0,1]$, the function $1/f$ is defined and also continuous, so $g = 1/f \in M$. But then we have $1 = gf \in gM$, which implies $1 \in M$ since M being an ideal means that $gM \subseteq M$. Then $R = (1) \subseteq M$, so $M = R$, which is a contradiction. Thus M must be contained in some M_c. Finally, if we take M to be maximal, we conclude that $M = M_c$ for some $c \in [0,1]$.

(c) Take the function $f(x) = x - b \in M_b$. But $f(c) = c - b \neq 0$ since $c \neq b$, so $f \notin M_c$.

(d) Suppose for contradiction that M_c is generated by $x - c$. Then we can write any $f \in M_c$ as $f = g(x-c)$ for some $g \in R$. Now fix the function $f(x) = |x-c| \in M_c$. This requires

$$g = \frac{f}{x-c} = \frac{|x-c|}{x-c},$$

which is clearly discontinuous at $x = c$, so we cannot have $g \in R$. Contradiction. □

Problem 1. Let g be an element of finite order n in G.

(a) Prove that the elements $1, g, g^2, \dots, g^{n-1}$ are all distinct. Deduce that $|g| \leq |G|$.

(b) Prove that if n is odd, then $g^i \neq g^{-i}$ for all $i = 1, 2, \dots, n-1$.

(c) Prove that if $n = 2k$ and $1 \leq i < n$, then $g^i = g^{-i}$ if and only if $i = k$.

Solution. (a) First recall that n is the smallest positive integer for which $g^n = 1$. Now suppose for contradiction that $g^i = g^j$ for some $i \neq j$ and $1 \leq i, j \leq n-1$. Assume without loss of generality that $i < j$. Then multiplying both sides by g^{-i} gives

$$g^i g^{-i} = g^j g^{-i} \implies 1 = g^{j-i}.$$

But this contradicts the minimality of n, since $1 \leq j - i \leq n-1$.

For the second part, suppose that $n > |G|$. Then the elements $1, g, g^2, \dots, g^{|G|}$ are all distinct by the first part. Then G contains $|G|+1$ distinct elements, which is a contradiction. Thus $n \leq |G|$.

(b) Suppose otherwise that $g^i = g^{-i}$ for some $1 \leq i \leq n-1$. Then g^i is its own inverse, so $g^{2i} = 1$. Then we must have $n | 2i$. But n is odd, so in fact $n | i$. This is a contradiction since $i < n$.

(c) Suppose that $g^i = g^{-i}$ for some $1 \leq i < n$. Then $g^{2i} = 1$, so $n | 2i$, which implies that $2i \geq n$. But $i < n$, so $2i < 2n$. Now $n | 2i$ and $n \leq 2i < 2n$, so we must have $2i = n = 2k$. This gives $i = k$. □

Problem 4. Find all cyclic subgroups of D_8. Find a proper subgroup of D_8 which is not cyclic.

Solution. Using a Cayley diagram we may see that

$$\langle r\rangle = \langle r^3\rangle = \langle r^5\rangle = \langle r^7\rangle = \{e, r, \dots, r^7\}.$$

Also we may find the cyclic subgroups

$$\langle r^2\rangle = \langle r^6\rangle = \{e, r^2, r^4, r^6\}$$

and $\langle r^4\rangle = \{e, r^4\}$. Finally, we can see that reflections (i.e. $\langle sr^i\rangle$ for $0 \leq i > 8$) each generated their own subgroup containing just the identity and themselves. Finally $\langle s, r^2\rangle \cong D_4$ is not cyclic. □

Problem 26. The *center* of a ring R is

$$Z(R) = \{z \in R \mid zr = rz \text{ for all } r \in R\}.$$

Prove that the center of a division ring is a field.

Solution. Recall that a commutative division ring is a field. Since $Z(R)$ is clearly commutative, it suffices to show that $Z(R)$ is a division ring. First we show that $Z(R)$ is indeed a ring. Note that $Z(R)$ is nonempty since 1 commutes with any $r \in R$, so $1 \in Z(R)$. For closure under subtraction, let $z_1, z_2 \in Z(R)$. Then for any $r \in R$, we have

$$(z_1 - z_2)r = z_1 r - z_2 r = rz_1 - rz_2 = r(z_1 - z_2),$$

so $z_1 - z_2 \in Z(R)$. For closure under multiplication, we have

$$(z_1 z_2)r = z_1(z_2 r) = z_1(rz_2) = (z_1 r)z_2 = (rz_1)z_2 = r(z_1 z_2),$$

so $z_1 z_2 \in Z(R)$. Finally, we show that each nonzero $z \in Z(R)$ has $z^{-1} \in Z(R)$ (the inverse z^{-1} exists since R is a division ring). For this, we can simply note that

$$z^{-1}r = z^{-1}(rz)z^{-1} = z^{-1}(zr)z^{-1} = rz^{-1},$$

so $z^{-1} \in Z(R)$ as desired. Therefore $Z(R)$ is a commutative division ring and thus a field. □