MAT301 Groups and Symmetry

Winter 2017

Payman Eskandari

CONTENTS

1. Preliminaries

1.1. A little bit of notation. As usual, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ respectively denote the set of all integers, rational numbers, real numbers, and complex numbers. We denote the set of all positive integers $\{1, 2, \cdots\}$ by $\mathbb{N}$ or $\mathbb{Z}_{>0}$. We denote the set of all $m \times n$ matrices with entries in $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ respectively by $Mat_{m\times n}(\mathbb{Q})$, $Mat_{m\times n}(\mathbb{R})$, and $Mat_{m\times n}(\mathbb{C})$.

Given two sets X and Y, the notation $X - Y$ means $\{x \in X : x \notin Y\}$, i.e. the set of all elements of X that are not in Y. For instance, $\mathbb{Q} - \{0\}$ means the set of all nonzero rational numbers. An alternative notation for $X - Y$ is $X \setminus Y$.

1.2. Recollections from arithmetic: Divisibility and the Division Algorithm. Recall that we say an integer m divides an integer n, or that m is a divisor of n, and write $m \mid n$, if there is an integer k such that $n = mk$. It is clear if m is a divisor of a nonzero integer n, then $|m| \leq |n|$. It is easy to see that if $m \mid n_1$ and $m \mid n_2$, then $m \mid an_1 + bn_2$ for any $a, b \in \mathbb{Z}$. It is also easy to see that divisibility is transitive, that is to say: if $\ell \mid m$ and $m \mid n$, then $\ell \mid n$.

The next result is usually referred to as the *division algorithm*.

PROPOSITION 1 (Division algorithm). Let $a, n \in \mathbb{Z}$ and $n > 0$. Then there are unique integers q and r (called the quotient and remainder of a in division by n) such that

(i) $a = nq + r$, and

(ii) $0 \leq r < n$.

PROOF. First let us show that there exist $q,\ r$ satisfying the conditions (i) and (ii) above. Since $n > 0$, the sequence of multiples of n

$$\ldots, -2n, -n, 0, n, 2n, \ldots$$

is strictly increasing and goes to infinity on both ends. Thus there is $q \in \mathbb{Z}$ such that $qn \leq a < (q+1)n$. Set $r = a - qn$. Condition (i) is certainly satisfied by our choices of q and r. To see r is in the desired range (Condition (ii)), subtract qn from $qn \leq a < (q+1)n$.

Now we turn our attention to uniqueness. Suppose q, r and q', r' satisfy (i) and (ii). We have

$$nq + r = nq' + r',$$

which can be rewritten as

$$n(q - q') = r' - r.$$

Thus $n \mid r' - r$. In view of $0 \leq r, r' < n$, we have

$$-n < r' - r < n.$$

Putting this together with $n \mid r' - r$, we see that $r' - r = 0$, and hence $q - q' = 0$ as well. □

1.3. Congruence. Fix and integer n. We say an integer a is congruent to an integer b and write $a \equiv b \pmod{n}$ if $n \mid a - b$. For instance, $4 \equiv 7 \pmod{3}$. As another example, note that $a \equiv 0 \pmod{n}$ is equivalent to $n \mid a$. The following two exercises summarize some important properties of congruence.

Exercise 1. Show that

(i) $a \equiv a \pmod{n}$

(ii) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

(Property (i) is called reflexivity, (ii) is called symmetry, and (iii) is called transitivity.)

Exercise 2. Let $a \equiv b \pmod{n}$ and $a' \equiv b' \pmod{n}$. Show that we have:

(i) $ac \equiv bc \pmod{n}$ for all $c \in \mathbb{Z}$

(ii) $a + a' \equiv b + b' \pmod{n}$

(iii) $aa' \equiv bb' \pmod{n}$

2. Binary Operations

2.1. Cartesian product of sets. Given two sets X and Y, one defines a new set

$$X \times Y = \{(x, y) : x \in X,\ y \in Y\}.$$

This is called *the cartesian product of* X *and* Y. In other words, $X \times Y$ is the set of all ordered pairs of the form (x, y), where x is an element of X and y is an element of Y. For instance,

$$\{1, 2\} \times \{a, b\} = \{(1, a), (1, b), (2, a), (2, b)\}$$

and

$$\{a, b\} \times \{1, 2\} = \{(a, 1), (a, 2), (b, 1), (b, 2)\}.$$

As another example,

$$\mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}$$

is simply the $\mathbb{R}^2$ plane.

2.2. Binary operations: Definition and some examples. Let S be a set. A *binary operation on* S is a function $S \times S \to S$. For instance, addition

$$\mathbb{R} \times \mathbb{R} \to \mathbb{R} \quad (x, y) \mapsto x + y$$

is a binary operation on $\mathbb{R}$.[†] Multiplication

$$\mathbb{R} \times \mathbb{R} \to \mathbb{R} \quad (x, y) \mapsto xy$$

is another binary operation on $\mathbb{R}$.

A binary operation on S takes a pair of elements of S as its input, and gives us an element of S as the output. Usually a binary operation is denoted by a symbol like $\star$, $*$, $\circ$, $+$, $\cdot$, etc. If we are denoting our binary operation by $\star$, we write $x \star y$ for the image of the pair (x, y) under $\star$, i.e. the output of $\star$ if the input is the pair (x, y). Thus to define an explicit binary operation $\star$ on a set S, we need to specify $x \star y$ for all $x, y \in S$.

For example, the formula $x \star y = x + y + xy$ defines a binary operation on $\mathbb{Z}$. We have

$$1 \star 2 = 1 + 2 + 1 \cdot 2 = 5, \quad 2 \star 3 = 2 + 3 + 2 \cdot 3 = 11.$$

[†]The notation $(x, y) \mapsto x + y$ means that the pair (x, y) is getting mapped (or sent) to $x + y$ by this function.

Exercise 3. Let $\star$ on $\mathbb{Z}$ be as in the example just above.

(a) Show that $x \star y = y \star x$ for all $x, y \in \mathbb{Z}$.

(b) Show that $x \star 0 = x$ for all $x \in \mathbb{Z}$.

Examples: One can define a binary operation on $\mathbb{Z}$ by sending $(x, y) \mapsto x - y$. But note that the same *recipe*, i.e. trying to send a pair (x, y) to $x - y$, does not define a binary operation on $\mathbb{Z}_{>0}$. Indeed, a binary operation on $\mathbb{Z}_{>0}$ is by definition a function $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$, i.e. must send every pair of positive integers to a positive integer. Our recipe of $(x, y) \mapsto x - y$ fails to do so. (Where is $(1, 2)$ mapped to?)

In the chart below, we list several examples. In each example, a set S together with a *candidate* for (or an attempt for defining) a binary operation is given. The last column tells us whether our candidate is indeed a binary operation, i.e. whether it defines a function $S \times S \to S$.

S	**Candidate for a binary operation on** S	**Is our candidate a binary operation?**
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	addition	Yes
any vector space V	addition	yes
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	multiplication (i.e. $(x, y) \mapsto xy$	Yes
$\mathbb{Q}$	$(x, y) \mapsto \frac{x}{y}$	No (Why?)
$\mathbb{Q} - \{0\}$	$(x, y) \mapsto \frac{x}{y}$	Yes

S	**Candidate for a binary operation on S**	**Is our candidate a binary operation?**
$\mathbb{Q} - \{0\}$	multplication	Yes
$\mathbb{Q} - \{0\}$	addition	No $(1 + (-1) = 0)$
$\mathbb{Z} - \{0\}$	$(x, y) \mapsto \frac{x}{y}$	No (Where is our "function" trying to send $(1, 2)$?)
$Mat_{m\times n}(\mathbb{Q})$, $Mat_{m\times n}(\mathbb{R})$ $Mat_{m\times n}(\mathbb{C})$	matrix addition	Yes
$Mat_{n\times n}(\mathbb{Q})$, $Mat_{n\times n}(\mathbb{R})$ $Mat_{n\times n}(\mathbb{C})$	matrix multiplication $(A, B) \mapsto AB$	Yes
$Mat_{n\times n}(\mathbb{Q}) - \{0\}$ (the set of nonzero $n \times n$ matrices with entries in $\mathbb{Q}$) for $n \geq 2$	matix multiplication	No (Why?)
The set of $n \times n$ invertible matrices with entries in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	matrix addition	No $(I + (-I) = 0)$
The set of $n \times n$ invertible matrices with entries in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	matrix maltiplication	Yes (See below.)

Our last example in the table deserves more explanation. Recall that a square matrix is invertible if and only if its determinant is nonzero. Also recall that for two $n \times n$ matrices A and B, $\det(AB) = \det(A)\det(B)$. If A and B are both invertible, their determinants are both nonzero, and hence

$$\det(AB) = \det(A)\det(B) \neq 0,$$

i.e. AB is invertible as well. Thus matrix multiplication is a binary operation on the set of all invertible $n \times n$ matrices with entries in $\mathbb{Q}$ (or $\mathbb{R}$ or $\mathbb{C}$).

Another example: Composition of functions. Recall that if X, Y, Z are sets, and $f : X \to Y$ and $g : Y \to Z$ are functions, one has the *composition* $g \circ f : X \to Z$ defined by

$$g \circ f(x) = g(f(x)) \quad \text{for all } x \in X.$$

Note that the expression $g(f(x))$ indeed makes sense: x is in X, and hence $f(x)$ is an element of Y, i.e. an element of the domain of g. We can apply g to $f(x) \in Y$. The result (i.e. $g(f(x))$ belongs to the set Z.

Let X be a set. Given two functions $f, g : X \to X$, the composition $f \circ g$ is again a function $X \to X$. Thus $(f, g) \mapsto f \circ g$ defines a binary operation on

$$\mathrm{Fun}(X, X) := \text{the set of all functions } X \to X.^{\dagger}$$

Suppose $f : X \to Y$ is a function. Recall that we say f is injective (or one-to-one) if whenever $f(x_1) = f(x_2)$, we have $x_1 = x_2$ (or equivalently, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$). We say the function f is surjective (or onto), if its image (i.e. the set $\{f(x) : x \in X\}$) is all of its codomain (i.e. Y). In other words, f is surjective if for every element y of Y, there is some $x \in X$ such that $f(x) = y$. We say f is bijective if it is both injective and surjective.

Exercise 4. (a) Show that if $f : X \to Y$ and $g : Y \to Z$ are injective, then so is the composition $g \circ f$.

[†]The symbol ":=" means "is defined to be equal to".

(b) Show that if $f : X \to Y$ and $g : Y \to Z$ are surjective, then so is the composition $g \circ f$.
(c) Conclude from (a) and (b) that if $f : X \to Y$ and $g : Y \to Z$ are bijective, then so is the composition $g \circ f$.

Let X be a fixed set. It follows from the exercise that $(f, g) \mapsto f \circ g$ indeed defines a binary operation on each of the following sets: (i) the set of all injective functions $X \to X$, (ii) the set of all surjective functions $X \to X$, and (iii) the set of all bijective functions $X \to X$.

Exercise 5. Let S be a set with n elements. Finds the number of all binary operations on S.

2.3. Commutative binary operations. Let $\star$ be a binary operation on a set S. We say $\star$ is *commutative* if for all $x, y \in S$, $x \star y = y \star x$. For example, addition of numbers and matrices is commutative. Multiplication of numbers is commutative. In any vector space, addition is a commutative binary operation. (Indeed, one of the defining axioms of a vector is space is that $v + w = w + v$ for all v, w in the vector space.)

More examples: (i) Define $\star$ on $\mathbb{Z}$ (or $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) by $x \star y = x + y + xy$. The operation $\star$ is commutative. (Why?)
(ii) Let $n \geq 2$. Then multiplication on $Mat_{n\times n}(\mathbb{Q})$, $Mat_{n\times n}(\mathbb{R})$ and $Mat_{n\times n}(\mathbb{C})$) is not commutative. For instance, take A to be the $n \times n$ matrix with 1's on the diagonal, 1 in the $(1, 2)$ entry, and 0's elsewhere. Take $B = A^T$ (the transpose of A). Then a direct computation shows $AB \neq BA$. (Verify this.)

Exercise 6. (a) Let $n \geq 2$. Is matrix multiplication commutative on the set of all invertible elements of $Mat_{n\times n}(\mathbb{Q})$? (Are A and B above invertible?)
(b) Let D be the set of all diagonal $n \times n$ matrices. Show that matrix multiplication is a commutative binary operation on D.

Examples continued: (iii) Composition of functions on the set of all bijections $\{1,2,3\} \to \{1,2,3\}$ is not commutative. Indeed, take f and g to be the following maps:

$$f:\ 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1$$

and

$$g:\ 1 \mapsto 1,\ 2 \mapsto 3,\ 3 \mapsto 2$$

Then

$$f \circ g(1) = f(g(1)) = f(1) = 2,$$

whereas

$$g \circ f(1) = g(f(1)) = g(2) = 3,$$

so that $f \circ g(1) \neq g \circ f(1)$. Hence $f \circ g \neq g \circ f$.[†]

Exercise 7. Let X be any set with more than 2 elements. Show that composition of functions on the set of all bijections $X \to X$ is not commutative.

Exercise 8. Let S be a set with n elements. Finds the number of all commutative binary operations on S.

2.4. Associative binary operations. Let $\star$ be a binary operation on a set S. Note that a binary operation only takes a *pair* of elements of S as its input. Suppose we are given a triple of elements of S, say (x, y, z), and we want to use $\star$ to produce another element. Since $\star$ only takes two elements at a times, we have to do this is in more that one step. Assuming we want x, y, z to appear in the expressions in that order, our choices are $(x \star y) \star z$ and $x \star (y \star z)$. In general, these may not be the same (as we will see in a moment).

DEFINITION. We say a binary operation $\star$ on a set S is associative if for all $x, y, z \in S$, $(x \star y) \star z = x \star (y \star z)$.

[†]Note that by definition, two functions $f, g : X \to Y$ are equal if and only if $f(x) = g(x)$ for all $x \in X$.

Examples: (i) Addition and multiplication of numbers is associative.

(ii) Addition in any vector space is associative. (Indeed, this is one of the defining axioms of a vector space. See your linear algebra book.)

(iii) Addition and multiplication of matrices is associative. For addition this is easy to see (since addition is done entry-wise and one has associativity of addition for numbers). For matrix multiplication, one can verify associativity directly using the definition of matrix multiplication, and again some properties of the arithmetic of numbers. This is not hard, but is a fairly long calculation, and we will skip it. (See the remark below.)

(iv) Let X, Y, Z, W be sets, and $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$ be functions. We claim that $(h \circ g) \circ f = h \circ (g \circ f)$.[†] Indeed, first note that both of these expressions make sense[‡] and are functions $X \to W$. For any $x \in X$,

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

Thus $(h \circ g) \circ f = h \circ (g \circ f)$, as claimed. (Make sure you see what is happenning in every step above.)

In particular, composition of functions on the set of all functions (or all bijective functions) $X \to X$ is associative.

REMARK. Using the connection between matrices and linear transformations that you have seen in linear algebra, one can conclude associativity of matrix multiplication from that of functions. (The interested reader is encouraged to think about this, but for purposes of tests and exam you may ignore this remark.)

Two more examples: (v) Consider the binary operation $\star$ defined on $\mathbb{Z}$ by $x \star y = x + y + xy$. We claim that this operation is associative. Indeed, given $x, y, z \in \mathbb{Z}$, by definition of $\star$,

$$(x \star y) \star z = (x + y + xy) \star z = x + y + xy + z + (x + y + xy)z = xyz + xy + yz + xz + x + y + z,$$

[†] One summarizes this by saying that composition of functions (in general, not just those from a set to itself) is associative.

[‡] For example, $h \circ g$ is a function $Y \to W$, and hence the composition $(h \circ g) \circ f$ makes sense.

$$X \xrightarrow{f} Y \xrightarrow{h \circ g} W$$

and

$$x \star (y \star z) = x \star (y + z + yz) = x + y + z + yz + x(y + z + yz) = xyz + xy + yz + xz + x + y + z.$$

(vi) Consider the binary operation $\star$ defined on $\mathbb{Z}$ by $x \star y = x^2 + y^2$. This operation is not associative:

$$(1 \star 1) \star 2 = 2 \star 2 = 8,$$

whereas

$$1 \star (1 \star 2) = 1 \star 5 = 26.$$

Suppose $\star$ is an associative binary operation on a set S. Let $x, y, z \in S$. Since the two elements $(x \star y) \star z$ and $x \star (y \star z)$ are the same, we might as well drop the brakets and simply write $x \star y \star z$ for this element. In fact, one can prove by induction that given any number of elements $x_1, \cdots, x_n \in S$, the outcome of $x_1 \star x_2 \star \cdots \star x_n$ does not depend on the possible arrangements of brackets, so that we might as well just drop the brackets all together, without causing any ambiguity. The exercise bellow asks you to verify that two specific possible arrangements of brackets for $n = 4$ result in the same outcome.

Exercise 9. Suppose $\cdot$ is an associative binary operation on S. Let $x, y, z, w \in S$. Show that

$$(x \cdot y) \cdot (z \cdot w) = (x \cdot (y \cdot z)) \cdot w.$$

We close this discussion of associativity with a warning. One has to be careful that the notion of associativity is about different arrangements of *brackets*, and not different arrangements of *elements*. Indeed, matrix maltiplication is associative; all that means is that $(AB)C = A(BC)$ (if the products make sense). Of course, $(AB)C$ and $A(CB)$ may be different. To be able to freely rearrange the brackets and the elements in expressions, one needs the operation to be both associative and commutative.

3. What is a group?

3.1. Definition and examples. Just like in MAT224 the goal was to study vector spaces, our goal in this course is to study groups.

DEFINITION. (1) A group is a pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G, such that the following axioms hold:

(i) $\star$ is associative, i.e. for every $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.

(ii) There exists an element $e \in G$ such that for all $a \in G$, $a \star e = e \star a = a$. (An element e satisfying this property is called an identity element of $(G, \star)$.)

(iii) For every $a \in G$, there is an element $b \in G$ such that $a \star b = b \star a = e$. (An element b satisfying this property is called an inverse of a.)

(2) We say a group $(G, \star)$ is commutative or abelian if the binary operation $\star$ in commutative, i.e. for all $a, b \in G$, $a \star b = b \star a$.

For example, $(\mathbb{Z}, +)$ is an abelian group. Note that the number 0 satisfies the defining property of an identity element:

$$0 + n = n + 0 = n \quad \text{for all } n \in \mathbb{Z},$$

and for every integer n, $-n$ is an inverse of n:

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

Similarly, $(\mathbb{Q}, +)$ is an abelian groups. On the other hand, $(\mathbb{Z}_{>0}, +)$ is not a group, since there is no identity element, i.e. there is no positive integer e such that for all $n \in \mathbb{Z}_{>0}$, $e + n = n + e = n$.

Before we give more examples, let us prove a proposition. Note that in the definition, we are not requiring identity and inverses to be unique; the definition speaks only of existence of them. The next proposition tells us that indeed these are unique. To state the proposition, it is convenient to have the following definition: If $*$ is a binary operation on a set S, even if $(S, *)$ is not a group, we say an element $e \in S$ is an identity element if for all $a \in S$, $e * a = a * e = a$.

PROPOSITION 2. Let G be a set, and $\star$ be a binary operation on G.[†]

[†]The proposition does not assume *yet* that $(G, \star)$ is a group.

(a) If an identity element exists, it is unique. In particular, idenity element in a group is unique.

(b) Suppose $(G, \star)$ is a group. Then every element $a \in G$ has a unique inverse.

PROOF. (a) Suppose e and e' are both idenitity elements. Note that this means $e \star a = a \star e = a$ and $e' \star a = a \star e' = a$ for all $a \in G$. Consider the element $e \star e'$ of G. On the one hand, since e is an idenitity, this element is equal to e'. On the other hand, since e' is an identity, this element is equal to e. Thus $e = e'$, proving the assertion.
(b) Suppose b, c are both inverses of a. Note that this means $a \star b = b \star a = e$ and $a \star c = c \star a = e$. We have

$$c = c \star e = c \star (a \star b) = (c \star a) \star b = e \star b = b.$$

(Justify every equality along the way.) □

Thus from now on, we speak of *the* idenitity element of a group (as opposed to *an* identity). Similarly, for every element a of a group, we speak of *the* inverse of a. We denote this inverse by a^{-1}.† The inverse a^{-1} of a is charaterized by the following property: It is the unique element of the group satisfying $a \star a^{-1} = a^{-1} \star a = e$.

A piece of terminology and notation before proceeding with examples: Often, we say "G is a group under $\star$" as a slightley less formal substitute of the expression "$(G, \star)$ is a group". We might even simply speak of the group G, with no mention of the binary operation, if it does not lead to any confusion (e.g. if the operation is obvious from the context).

More examples: (1) We already discussed that $\mathbb{Z}$ and $\mathbb{Q}$ under addition are abelian groups. Same is true for $\mathbb{R}$ and $\mathbb{C}$.

(2) $Mat_{m\times n}(\mathbb{Z})$, $Mat_{m\times n}(\mathbb{Q})$, $Mat_{m\times n}(\mathbb{R})$, and $Mat_{m\times n}(\mathbb{C})$ form abelian groups under addition. In each of these, the idenity is the zero matrix, and the inverse of a matrix A is the matrix $-A$.

†Unless the notation can lead to confusion, e.g. in $(\mathbb{Q}, +)$.

(3) $\mathbb{Q}$ under multiplication is not a group. Indeed, the identity element for multiplication on $\mathbb{Q}$ is 1. But then 0 does not have an inverse, as there is no $b \in \mathbb{Q}$ such that $0b = 1$. Similarly, $\mathbb{R}$ and $\mathbb{C}$ are not groups under multiplication.

(4) $\mathbb{Q} - \{0\}$ is a group under multiplication. Indeed, first note that multiplication is indeed a binary operation on $\mathbb{Q} - \{0\}$. The associativity axiom clearly holds. The number 1 it the identity, and the inverse of $a \in \mathbb{Q} - \{0\}$ is $\frac{1}{a}$ (i.e. the reciprocal of a). We usually use the notation $\mathbb{Q}^\times$ for the group $\mathbb{Q} - \{0\}$ under multiplication. Similarly, $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are groups under multiplication, and are denoted by $\mathbb{R}^\times$ and $\mathbb{C}^\times$. Note that $\mathbb{Q}^\times$, $\mathbb{R}^\times$ and $\mathbb{C}^\times$ are all abelian.

(5) Consider $\mathbb{Z}$ under multiplication. The identity element is 1. Since zero does not have an inverse, $\mathbb{Z}$ is not a group under multiplication. Note that 2 also does not have an inverse, as there is no $b \in \mathbb{Z}$ such that $2b = 1$. (In fact, the only elements of $\mathbb{Z}$ with a multiplicative inverse are ± 1 (why?).) Thus in contrast to the situation for $\mathbb{Q}$, $\mathbb{Z} - \{0\}$ is still not a group under multiplication.

(6) $Mat_{n\times n}(\mathbb{Q})$, $Mat_{n\times n}(\mathbb{R})$ and $Mat_{n\times n}(\mathbb{C})$ under matrix multiplication are not groups. (Why?)

(7) The set of all $n \times n$ invertible matrices with entries in $\mathbb{Q}$ (resp. $\mathbb{R}$ and $\mathbb{C}$) forms a group under matrix multiplication. Tthis group is referred to as the *general linear group* of degree n over $\mathbb{Q}$ (resp. over $\mathbb{R}$ and $\mathbb{C}$), and is denoted by $GL_n(\mathbb{Q})$ [†] (resp. $GL_n(\mathbb{R})$, $GL_n(\mathbb{C})$).

(8) The set of all symmetries of a plane figure forms a group under composition. Of special interest to us, are the groups of symmetries of regular[‡] polygons. The group of all symmetries of regular n-gon (i.e. regular polygon with n sides) is denoted by D_n.

(9) Let X be any set. The set of all bijections $X \to X$ forms a group under composition of functions. The identity element of this group is the identity function on X, i.e. the function $e : X \to X$ mapping $x \mapsto x$ for all $x \in X$. Given a bijection $f : X \to X$, the inverse element of f in this group is simply the inverse function $f^{-1} : X \to X$ (which exists since f is a bijection).

(10) Let n be a positive integer. An important special case of the previous example is the group of all bijections

$$\{1, \cdots, n\} \to \{1, \cdots, n\}.$$

[†]Some books use the notation $GL(n, \mathbb{Q})$ instead.

[‡]A polygon is regular if all its sides have equal lengths.

This group is referred to as the *symmetric group of degree* n, as is denoted by S_n. It has $n!$ elements (why?). For instance, let us explicitly write all element of S_3. There are 6 bijections $\{1,2,3\} \to \{1,2,3\}$, which for now we denote by $e, f_1, f_2, f_3, g_1, g_2$:[§]

i	1	2	3
$e(i)$	1	2	3

i	1	2	3
$f_1(i)$	1	3	2

i	1	2	3
$f_2(i)$	3	2	1

i	1	2	3
$f_3(i)$	2	1	3

i	1	2	3
$g_1(i)$	2	3	1

i	1	2	3
$g_2(i)$	3	1	2

The identity of S_3 is the function e. We have $e^{-1} = e$ (note the identity element is always its own inverse), $f_i^{-1} = f_i$, $g_1^{-1} = g_2$, and $g_2^{-1} = g_1$.

(11) Let V be any vector space. Then V is an abelian group under $+$. (See the defining axioms of a vector space.) One refers to this as the "underlying additive group" of a vector space.

We finish this discussion with a useful proposition.

PROPOSITION 3. Let $(G, \star)$ be a group. We have:

(a) For every $a \in G$, $(a^{-1})^{-1} = a$.

(b) For every $a, b \in G$, $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

(c) If $a, b, c \in G$ and $a \star b = a \star c$, then $b = c$. (This is usually referred to as "left cancellation".)

(d) If $a, b, c \in G$ and $b \star a = c \star a$, then $b = c$. (This is usually referred to as "right cancellation".)

PROOF. (a) a^{-1} is the inverse of a, i.e.

$$a^{-1} \star a = a \star a^{-1} = e.$$

Thus a satisfies the characterizing property of the inverse of a^{-1}.

(b) We have

$$(a \star b) \star (b^{-1} \star a^{-1}) = ((a \star b) \star b^{-1}) \star a^{-1} = (a \star (b \star b^{-1}) \star a^{-1} = (a \star e) \star a^{-1} = a \star a^{-1} = e.$$

[§]We named these functions differently in class.

Similarly, one can see

$$(b^{-1} \star a^{-1}) \star (a \star b) = e.$$

It follows that $b^{-1} \star a^{-1}$ is the inverse of $a \star b$, as desired.

(c) Let $a \star b = a \star c$. Then

$$a^{-1} \star (a \star b) = a^{-1} \star (a \star c).$$

Using associativity we get

$$(a^{-1} \star a) \star b = (a^{-1} \star a) \star c,$$

But $a^{-1} \star a = e$, so that we have $e \star b = e \star c$. Thus $b = c$.

(d) You prove this on your assignment. □

3.2. Order.

DEFINITION (Order of a group). Let G be a group. We say G is finite (resp. infinite) if G has finitely (resp. infinitely) many elements. By the order of G we mean the number of elements (i.e cardinility) of G.

The order of a group G is usually denoted by $|G|$. Some examples of infinite groups are $\mathbb{Z}$ (under addition), $\mathbb{R}^\times$, and $GL_n(\mathbb{Q})$. Some examples of finite groups are the groups D_n and S_n. A regular n-gon has $2n$ symmetries: n rotations and n reflections. (Draw pictures for $n = 3, 4, 5, 6$ to see this.) Thus $|D_n| = 2n$. We call D_n the *Dihedral group of order* $2n$. The group S_n has $n!$ elements, i.e. has order $n!$.

There is also a notion of order for elements of a group.

DEFINITION (Order of an element). Let $(G, \star)$ be a group with identity element denoted by e. We say an element $g \in G$ has finite order if there there is a positive integer n such that

$$\underbrace{g \star g \star g \cdots \star g}_{n \text{ appearances of } g} = e. \tag{1}$$

If there is no such n, we say g has infinite order. If g has finite order, the smallest positive integer n for which Eq. (1) holds is called the order of g.

The order of an element g is usually denoted by $|g|$.

Examples: (1) The identity element of a group has order 1.

(2) The only element of $\mathbb{Z}$ of finite order is 0. Same is true for $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(3) The reflections in D_n have order 2. This is because if r is a reflection, $r \neq e$, but $r \circ r = e$.

(4) Denoting the elements of S_3 by $e, f_1, f_2, f_3, g_1, g_2$ as in Example (10) of Paragraph 3.1, each of the f_i has order 2, where as the g_i have order 3. (Work out the details. You'll see that for example, $g_1 \neq e$, $g_1 \circ g_1 \neq e$, but $g_1 \circ g_1 \circ g_1 = e$.)

We now introduce a convenient piece of notation. If it won't lead to any confusion, often we shorten our expressions as follows: If G is a group under the binary operation $\star$ (or $\cdot$, $*$, etc.) and $g, h \in G$, rather than writing $g \star h$ (or $g \cdot h$, etc.), we may drop the operation symbol and simply write gh. Also, given $g \in G$ and $n \in \mathbb{Z}_{>0}$, we may abbreviate the element

$$\underbrace{g \star g \star g \cdots \star g}_{n \text{ appearances of } g}$$

by simply g^n. Since this notation convention mimicks that of the usual multiplication of numbers, we may refer to this as the *multiplicative notation*. For instance, adopting the multiplicative notation, the order of $g \in G$ is the smallest positive integer n for which $g^n = e$.

The goal of the following exercise is to extend the definition of g^n to negative exponents, and show that the usual "laws of exponents" are valid in any group.

Exercise 10. Let G be a group. Let $g \in G$.

(a) Let m, n be positive integers. Show that $g^m g^n = g^{m+n}$ and $(g^n)^m = g^{nm}$.

(b) For any integer $n > 0$, show that $(g^n)^{-1} = (g^{-1})^n$.

(c) For any integer $n > 0$, define g^{-n} to be $(g^n)^{-1}$ (or equivalently $(g^{-1})^n$). Also, define g^0 to be the identity element. Show that for every $m, n \in \mathbb{Z}$, $g^m g^n = g^{m+n}$ and $(g^n)^m = g^{nm}$.

PROPOSITION 4. Let G be a group, $g \in G$, and $|g| = d$. Then for any integer n, $g^n = e$ if and only if $d \mid n$.

PROOF. First note that if $d \mid n$, then

$$g^n = (g^d)^{\frac{n}{d}} = e^{\frac{n}{d}} = e,$$

giving the result in one direction. Conversely, suppose $g^n = e$. Our goal is to show that $d \mid n$. By the division algorithm (Proposition 1, here we are dividing n by d) there are integers q, r such that $n = qd + r$ and $0 \leq r < d$. Suppose $r \neq 0$, so that $0 < r < d$. We have

$$g^r = g^{n-qd} = g^n (g^d)^{-q} = ee = e.$$

This contradicts the defining property of d. The contradiction proves $r = 0$, and hence $d \mid n$. □

Example: Let $\rho_{\frac{2\pi}{6}} \in D_6$ be rotation by $\frac{2\pi}{6}$. One easily checks $|\rho_{\frac{2\pi}{6}}| = 6$. The previous proposition asserts that $\rho_{\frac{2\pi}{6}}^n = e$ if and only if $6 \mid n$.

PROPOSITION 5. Let G be a group, $g \in G$, and $|g| = d$. Then for any integer k, $|g^k| = \frac{d}{\gcd(d,k)}$.

PROOF. This was one of the problems on Assignment 2. For the sake of completeness we include the proof here as well. Let $|g^k| = D$. On the one hand,

$$(g^k)^{\frac{d}{\gcd(d,k)}} = g^{\frac{kd}{\gcd(d,k)}} = (g^d)^{\frac{k}{\gcd(d,k)}} = e^{\frac{k}{\gcd(d,k)}} = e.$$

By Proposition 4, this imply $D \mid \frac{d}{\gcd(d,k)}$. On the other hand, we have $g^{kD} = (g^k)^D = e$. Again by Proposition 4, this gives $d \mid kD$. Thus $\frac{d}{\gcd(d,k)} \mid \frac{k}{\gcd(d,k)} D$. Since $\gcd(\frac{d}{\gcd(d,k)}, \frac{k}{\gcd(d,k)}) = 1$, it follows $\frac{d}{\gcd(d,k)} \mid D$. Combining with $D \mid \frac{d}{\gcd(d,k)}$ we get $D = \frac{d}{\gcd(d,k)}$ as desired. □

4. Subgroups

DEFINITION. Let $(G, \star)$ be a group (with identity element denoted by e, as usual). Let H be a subset of G. We say H is a subgroup of G if it satisfies the following three properties:

(i) H is closed under the operation, i.e. if $g, h \in H$, then $g \star h \in H$.

(ii) $e \in H$

(iii) H is closed under taking inverses, i.e. if $h \in H$, then $h^{-1} \in H$ as well.

Note that the first requirement ensures that $\star$ gives[†] a binary operation on H as well. Of course, this operation is associative: If $x, y, z \in H$, then $x \star (y \star z) = (x \star y) \star z$, as this equality indeed holds for all x, y, z in G. The second requirement ensures that $(H, \star)$ has an identity element, namely e (the identity of $(G, \star)$). Finally, the third requirement ensures that inverses exist in $(H, \star)$. Thus a subgroup of $(G, \star)$ is itself a group under $\star$.

Notation. We write $H \leq G$ to signify that H is a subgroup of G.

Examples: (1) Let G be any group. Examples of subgroups of G are $\{e\}$ and G. The former is usually referred to as *the trivial subgroup*.

(2) Let $n \in \mathbb{Z}$. Define $n\mathbb{Z}$ to be the set of all multiples of n, i.e.

$$n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}.$$

Then $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.[‡]

(3) Let $\mathbb{Q}_{>0}$ be the set of all positive rational numbers. Then $\mathbb{Q}_{>0}$ is a subgroup of $\mathbb{Q}^\times$. (Remember $\mathbb{Q}^\times$ means nonzero rational numbers under multiplication.) Similarly, $\mathbb{R}_{>0}$ (positive reals) is a subgroup of $\mathbb{R}^\times$.
Note that the set of negative rationals on the other hand, does not form a subgroup of $\mathbb{Q}^\times$. Indeed, it is not closed under the operation (and also does not contain the identity element).

(4) The set of all rotational symmetries in D_n forms a subgroup. Indeed, composition of two rotations is a rotation, the identity symmetry is a rotation (by 0), and finally, the inverse of a rotation is also a rotation. Being a subgroup of D_n, the set of all rotational symmetries itself is a group under composition. Its order is n, as there are n rotations in D_n.

(5) *The groups μ_N of N-th roots of unity*. Let N be a positive integer. Let μ_N be the set of all the N-th roots of unity in $\mathbb{C}$, i.e.

$$\mu_N := \{\alpha \in \mathbb{C} : \alpha^N = 1\}.$$

[†] or restricts to, to be more precise

[‡] As you show on Assignment 2, these are in fact the only sungroups of $\mathbb{Z}$.

Note that $0 \notin \mu_N$, so that $\mu_N \subset \mathbb{C}^\times$. We claim that μ_N is a subgroup of $\mathbb{C}^\times$. Indeed, if $\alpha, \beta \in \mu_N$, then

$$(\alpha\beta)^N = \alpha^N \beta^N = 1 \cdot 1 = 1,$$

so that $\alpha\beta \in \mu_N$. This shows μ_N is closed under multiplication. It is clear that $1 \in \mu_N$, verifying Property (ii) of the definition. Finally, if $\alpha \in \mu_N$, then $\frac{1}{\alpha}$ (which is the inverse of α in $\mathbb{C}^\times$) is also an N-th root of unity, as

$$(\frac{1}{\alpha})^n = \frac{1}{\alpha^n} = 1.$$

Thus μ_N is closed under taking inverses as well.

Being a subgroup of $\mathbb{C}^\times$, μ_N itself is a group under the usual multiplication of numbers. Recall that if we set $\zeta = e^{i\frac{2\pi}{N}} = \cos(\frac{2\pi}{N}) + i\sin(\frac{2\pi}{N})$, the (distinct) N-th roots of unity are

$$1, \zeta, \zeta^2, \ldots, \zeta^{N-1}.$$

(Note that $\frac{1}{\zeta} = \zeta^{N-1}$) In other words,

$$\mu_N = \{1, \zeta, \zeta^2, \ldots, \zeta^{N-1}\}.$$

Thus $|\mu_N| = N$. As an example, the Cayley table of μ_3 is given below. In the table, $\zeta = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ (and hence $\zeta^2 = e^{\frac{4\pi i}{3}} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$).

$\cdot$	1	ζ	ζ^2
1	1	ζ	ζ^2
ζ	ζ	ζ^2	1
ζ^2	ζ^2	1	ζ

Is the table consistent with Problem 4 of Assignment 1?

(6) Let K be any of $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Define

$$SL_n(K) := \{A \in GL_n(K) : \det(A) = 1\}.$$

In other words, $SL_n(K)$ is the set of all $n \times n$ matrices of determinant 1 with entries in K. Then $SL_n(K)$ is a subgroup of the general linear group $GL_n(K)$. (See Example (7) of Paragraph 3.1 for definition of the general linear groups.) Indeed, if $A, B \in SL_n(K)$, then

$$\det(AB) = \det(A)\det(B) = 1$$

and hence $AB \in SL_n(K)$. The identity matrix has determinant 1 and hence is in $SL_n(K)$. Finally, if $A \in SL_n(K)$, then $\det(A^{-1}) = \frac{1}{\det(A)} = 1$ and hence $A^{-1} \in SL_n(K)$.
The subgroup $SL_n(K)$ (which is itself a group) is called the *special linear group* over K of degree n.

(7) The subset

$$S = \{A \in GL_n(\mathbb{Q}) : A \text{ has all entries in } \mathbb{Z}\}$$

is not a subgroup of $GL_n(\mathbb{Q})$. Indeed, it is not closed under taking inverses. For instance, consider the diagonal matrix with diagonal entries $2, 1, 1, \ldots, 1$. It is invertible and has integer entries, hence it is in S. But its inverse is not in S. (The inverse is the diagonal matrix with $1/2, 1, 1, \ldots, 1$ on the diagonal.)

(8) Let

$$\begin{aligned} SL_n(\mathbb{Z}): &= \{A \in GL_n(\mathbb{Q}) : A \text{ has all entries in } \mathbb{Z} \text{ and moreover } \det(A) = 1\} \\ &= \{A \in SL_n(\mathbb{Q}) : A \text{ has all entries in } \mathbb{Z}\}. \end{aligned}$$

Then $SL_n(\mathbb{Z})$ is indeed a subgroup of $SL_n(\mathbb{Q})$. Indeed, that $SL_n(\mathbb{Z})$ is closed under multiplication and contains the identity matrix are clear. As for inverses, recall that by the adjunct formula, for any invertible matrix A, A^{-1} is $\frac{1}{\det A}$ times the adjunt matrix of A. If A has (all) entries in $\mathbb{Z}$, so will the adjunct matrix (see the definition of the adjunct matrix). If A moreover has determinant 1, then A^{-1} will have entries in $\mathbb{Z}$ as well.

For instance,

$$\begin{bmatrix} 4 & 7 \\ 5 & 9 \end{bmatrix} \in SL_2(\mathbb{Z}).$$

Its inverse is

$$\begin{bmatrix} 9 & -7 \\ -5 & 4 \end{bmatrix}.$$

(Recall the formula for inverse of an invertible 2×2 matrix.)

(9) Fix a positive integer N. Define $\Gamma_0(N)$ to be the following subset of $SL_2(\mathbb{Z})$:

$$\Gamma_0(N) := \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : N \mid c \}$$

For instance,

$$\begin{bmatrix} 5 & 4 \\ 6 & 5 \end{bmatrix} \in \Gamma_0(3).$$

We claim that $\Gamma_0(N) \leq SL_2(\mathbb{Z})$. Indeed, let $A, B \in \Gamma_0(N)$. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} r & s \\ t & u \end{bmatrix}.$$

Then

$$AB = \begin{bmatrix} * & * \\ cr + dt & * \end{bmatrix}.$$

Since $N \mid c, t$ (why?), $N \mid cr + dt$ as well. Hence $AB \in \Gamma_0(N)$. Note that

$$A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Since N divides c, it also divides $-c$ and hence $A^{-1} \in \Gamma_0(N)$. That identity lives in $\Gamma_0(N)$ is clear (but you should still quickly justify it on the assessments).

(10) As our final example, we note that some of the groups we saw in earlier sections are indeed subgroups of each other:

$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C},$$

$$\mathbb{Q}^\times \leq \mathbb{R}^\times \leq \mathbb{C}^\times,$$

and

$$GL_n(\mathbb{Q}) \leq GL_n(\mathbb{R}) \leq GL_n(\mathbb{C}).$$

Exercise 11. Let $K \leq H$ and $H \leq G$. Show that $K \leq G$.

Exercise 12. Let $K \leq G$, $H \leq G$, and $K \subset H$ (K contained in H). Show that K is a subgroup of H.

Exercise 13. Show that if $m \mid n$, then $n\mathbb{Z} \leq m\mathbb{Z}$.

Exercise 14. Show that if $m \mid n$, then $\Gamma_0(n) \leq \Gamma_0(m)$.

Exercise 15. Show that if $m \mid n$, then $\mu_m \leq \mu_n$. (Compare with the previous two exercises.)

5. Digression: Equivalence relations and partitions

5.1. Equivalence relations.

DEFINITION. Let X be a set. We say a relation $\sim$ on X is an equivalence relation if the following conditions are satisfies:

(i) For every $x \in X$, $x \sim x$.

(ii) If $x \sim y$, then $y \sim x$.

(iii) If $x \sim y$ and $y \sim z$, then $x \sim z$.

A relation that satisfies (i) (resp. (ii), (iii)) is said to be reflexive (resp. symmetric, transitive). Thus an equivalence relation is a relation that is reflexive, symmetric, and transitive. For instance, $\leq$ (the usual less than or equal to) on $\mathbb{R}$ is not symmetric, and hence not an equivalence relation. Similarly, $\subset$ (being a (not necesarily proper) subset) is a relation on the collection of all subsets of a given set S, but is not an equivalence relation since it is not symmetric. Note that both $\leq$ and $\subset$ are indeed reflexive and transitive.

Fix an integer $n \geq 1$. Recall that for $a, b \in \mathbb{Z}$, we write $a \equiv b \pmod{n}$ (and say a is congruent to b mod n) if $n \mid a - b$. This defines a relation on $\mathbb{Z}$, which we refer to as congruence mod n. The properties listed in Exercise 1 tell us that congruence mod n is an equivalence relation on $\mathbb{Z}$.

As another example, consider the relation $\sim$ on $\mathbb{R}^2 - \{(0,0)\}$ (or on $\mathbb{R}^2$) defined by

$$v \sim v' \text{ if and only if } v' = cv \text{ for some nonzero real number } c. \tag{2}$$

We claim that this is an equivalence relation. Indeed, $v = 1v$ so that $\sim$ is reflexive. If $v \sim v'$, $v' = cv$ for some nonzero c. But then $v = \frac{1}{c}v'$, and hence $v' \sim v$. This proves symmetry. As for transitivity, let $v \sim v'$ and $v' \sim v''$. Then there are nonzero c, c' such that $v' = cv$ and $v'' = c'v'$. It follows $v'' = c'cv$, and hence $v \sim v''$. (Also note that $c'c$ is nonzero.)

Exercise 16. Define $\sim$ on $\mathbb{R}^2$ by

$$(x, y) \sim (x', y') \text{ if and only if } x^2 + y^2 = x'^2 + y'^2.$$

Show that $\sim$ is an equivalence relation on $\mathbb{R}^2$.

5.2. Partitions. Let X be a set. By a partition of X we mean a collection of non-empty, non-overlapping subsets of X whose union is all of X. For instance,

$$\{0\}, \ \mathbb{R}_{>0} := \{x \in \mathbb{R} : x > 0\}, \qquad \text{and} \qquad \mathbb{R}_{<0} := \{x \in \mathbb{R} : x < 0\}$$

form a partition of $\mathbb{R}$. More formally, a partition of X is a collection of subsets P_α of X (α in some *index set* I used to index our subsets) such that

(i) each P_α is non-empty,
(ii) $P_\alpha \cap P_\beta = \emptyset$ if $\alpha \neq \beta$, and
(iii) $\bigcup_{\alpha \in I} P_\alpha = X$.

Note that conditions (ii) and (iii) say that every $x \in X$ belongs to exactly one of the P_α.

Thus for instance,

$$\{1, 2\}, \{3\}, \{4\} \tag{3}$$

is a partition of $\{1,2,3,4\}$. Note that

$$\{1\}\,,\ \{2\}\,,\ \{3\}\,,\ \{4\}$$

is another partition of $\{1,2,3,4\}$, as is

$$\{1,2,3,4\}$$

itself.

Let $\mathcal{P} = \{P_\alpha\}_{\alpha\in I}$ be a partition of X. We can define a relation $\sim_{\mathcal{P}}$ on X as follows: For any $x, y \in X$, set

$$x \sim_{\mathcal{P}} y \text{ if and only if there is } \alpha \in I \text{ such that } x, y \in P_\alpha.$$

In other words, we set $x \sim_{\mathcal{P}} y$ if and only if x and y belong to *the same* P_α. It is easy to see that $\sim_{\mathcal{P}}$ is an equivalence relation on X. For instance, if $\mathcal{P}$ is the partition Eq. (3) of $\{1,2,3,4\}$, we have

$$1 \sim_{\mathcal{P}} 1,\ 1 \sim_{\mathcal{P}} 2,\ 2 \sim_{\mathcal{P}} 1,\ 2 \sim_{\mathcal{P}} 2,\ 3 \sim_{\mathcal{P}} 3,\ 4 \sim_{\mathcal{P}} 4 \tag{4}$$

(and these are the only pairs in relation under $\sim_{\mathcal{P}}$).

5.3. Equivalence classes. In the previous paragraph we saw that one can use a partition of a set X to define an equivalence relation on X. Can one reverse this procedure?

Let us go back to the example of $X = \{1,2,3,4\}$ and the partition $\mathcal{P}$ given in Eq. (3). The relation $\sim_{\mathcal{P}}$ defined on X is described in Eq. (4). Note that

$$\{x \in X : 1 \sim_{\mathcal{P}} x\} = \{x \in X : 2 \sim_{\mathcal{P}} x\} = \{1,2\},$$

$$\{x \in X : 3 \sim_{\mathcal{P}} x\} = \{3\},$$

and

$$\{x \in X : 4 \sim_{\mathcal{P}} x\} = \{4\}.$$

Thus the sets of the form $\{x \in X : a \sim_{\mathcal{P}} x\}$ (for fixed a) *recover* the partition $\mathcal{P}$ for us from the equivalence relation $\sim_{\mathcal{P}}$.

Let us go back to the general picture. Suppose X is any set, and $\sim$ is an equivalence relation on X. For every $a \in X$, define the *equivalence class of* a (with respect to $\sim$) to be

$$[a] := \{x \in X : a \sim x\}.$$

Note that equivalence classes are all nonempty, as $a \in [a]$ (by reflexivity of $\sim$).

LEMMA 1. Let $\sim$ be an equivalence relation on a set X. For any $a, b \in X$, $a \sim b$ if and only if $[a] = [b]$.

PROOF. $\Leftarrow$: Suppose $[a] = [b]$. It follows that $b \in [a]$ (why?), and hence $a \sim b$ as desired.
$\Rightarrow$: Now suppose $a \sim b$. Note that by symmetry, $b \sim a$ as well. Suppose $x \in [a]$. This means $a \sim x$. Putting together with $b \sim a$, transitivity implies $b \sim x$, which is to say $x \in [b]$. This proves $[a] \subset [b]$. Similarly one can prove $[b] \subset [a]$. □

THEOREM 1. Let $\sim$ be an equivalence relation on a set X. Then the distinct equivalence classes of $\sim$ form a partition of X.

Before the proof, note that in the example of $\sim_{\mathcal{P}}$ for $\mathcal{P}$ given by (3) on $\{1, 2, 3, 4\}$, the distinct equivalence classes are $[1] = [2] = \{1, 2\}$, $[3] = \{3\}$, and $[4] = \{4\}$. They do indeed partition $\{1, 2, 3, 4\}$. (In fact, as pointed out earlier, they just give $\mathcal{P}$ back. See the exercise below.)

PROOF OF THEOREM 1. We already noted that the equivalence classes are nonempty (as $a \in [a]$). Also, the union of all the equivalence classes is indeed all of X, as each $a \in X$ belongs to an equivalence class (namely to $[a]$). It remains to show that the distinct equivalence classes have empty intersection. Suppose $[a] \cap [b] \neq \emptyset$. We need to show that $[a] = [b]$. Let c be in the intersection of $[a]$ and $[b]$. Then $a \sim c$ and $b \sim c$. By symmetry and transitivity, $a \sim b$, and hence by the previous lemma $[a] = [b]$. □

Let $\sim$ be an equivalence relation on X. Let C be an equivalence class of $\sim$. We call any a for which $C = [a]$ a *representative* of C. Note that by the previous theorem, the representatives of C are exactly the elements of C. For instance, in the example of $\sim_{\mathcal{P}}$ for $\mathcal{P}$ given by Eq. (3) on $\{1, 2, 3, 4\}$, the representatives of the class $\{1, 2\}$ are 1 and 2.

Exercise 17.[†] Let X be a set. In the previous paragraph we defined a map

$$\text{partitions of } X \ \to \ \text{equivalence relations on } X \qquad \mathcal{P} \mapsto \sim_{\mathcal{P}} . \tag{5}$$

In this paragraph, we saw that given any equivalence relation $\sim$ on X, the distinct equivalence classes of $\sim$ form a partition of X. In other words, we have a map

$$\text{equivalence relations on } X \ \to \ \text{partitions of } X \tag{6}$$

sending

$$\text{an equivalence relation } \sim \ \mapsto \ \text{partition formed by the distinct equivalence classes of } \sim.$$

Show that the two maps (5) and (6) are inverses of one another.

6. The groups $\mathbb{Z}/n$ and $U(n)$

Fix an integer $n \geq 1$. As we discussed, congruence mod n is an equivalence relation on $\mathbb{Z}$. The equivalence classes of this relation are usually called *residue classes* mod n. Note that the residue class $[a]$ of an integer a mod n is

$$\{b \in \mathbb{Z} : a \equiv b \pmod{n}\} = \{a + nk : k \in \mathbb{Z}\}.$$

In other words,

$$[a] = \{\ldots,\ a-2n,\ a-n,\ a,\ a+n,\ a+2n,\ldots\}.$$

By Lemma 1, $[a] = [b]$ if and only if $a \equiv b \pmod{n}$. Thus $[0], [1], \ldots, [n-1]$ are all distinct. On the other hand, by the division algorithm (Proposition 1), for any $a \in \mathbb{Z}$, a is congruent to one of the numbers $0, 1, \ldots, n-1$, and hence $[a]$ is one of $[0], [1], \ldots, [n-1]$. It follows that $[0], [1], \ldots, [n-1]$ are all the (distinct) residue classes mod n.

Notation: We denote the set of all residue classes mod n by $\mathbb{Z}/n$. ("/" is to be read as "mod".)

[†] You can ignore this exercise for the purposes of tests and exam.

Thus

$$\mathbb{Z}/n = \{[0], [1], \ldots, [n-1]\}.$$

One has to be careful about the notation for residue classes: There is always a *modulus* n in the background, even though the dependence on n may not be clear from the notation $[a]$. For instance, working mod 3,

$$[2] = \{\ldots, -1, 2, 5, 8, \ldots\},$$

where as mod 4,

$$[2] = \{\ldots, -2, 2, 6, 10, \ldots\}.$$

We have

$$\mathbb{Z}/4 = \{[0], [1], [2], [3]\} = \{[4], [17], [22], [-1]\},$$

as $[0] = [4]$, $[1] = [17]$, $[2] = [22]$, and $[3] = [-1]$.

Back to the general case of residue classes mod n. Now that we have defined the set $\mathbb{Z}/n$, we will define two binary operations on it; we will refer to these operations as addition and multiplication. This discussion is very subtle, so one is warned to be careful. We will be using the additon and multiplication on $\mathbb{Z}$ to define our addition and multiplication on $\mathbb{Z}/n$. Suppose C and C' are two residue classes mod n (possibly the same). We will define $C + C'$ and $C \cdot C'$. We *choose* a representative $a \in C$ (i.e. a number a such that $[a] = C$), and a representative $b \in C'$. We define

$$C + C' := [a + b]$$

and

$$C \cdot C' = [ab].$$

Of course, and this is the crucial part, for this to make sense, one needs to know that the classes $[a+b]$ and $[ab]$ do not depend on *the choice of the representatives* a and b. In other words, one needs to have the following:

$$\text{If } [a] = [a'] \text{ and } [b] = [b'] \text{ ,}^{\dagger} \text{ then } [a + b] = [a' + b'] \text{ and } [ab] = [a'b'].$$

[†] i.e. if a, a' represent the same class, and so do b, b'

But this is indeed the case. Translating the statement back to the language of congruences, the statement says:

$$\text{If } a \equiv a' \pmod{n} \text{ and } b \equiv b' \pmod{n}, \text{ then } a+b \equiv a'+b' \text{ and } ab \equiv a'b' \pmod{n}.$$

This is indeed true. (See Exercise 2.) Thus we have defined binary operations $+$ and $\cdot$ on $\mathbb{Z}/n$.

Let us look at an example. In $\mathbb{Z}/4$, let us find the sum and product of $[2]$ and $[3]$. By taking 2 and 3 as the representatives of these classes, we have $[2]+[3] = [2+3] = [5]$ and $[2][3] = [2\cdot 3] = [6]$. Note that we could have carried out these calculations by choosing other representatives for $[2]$ and $[3]$. For instance, take $-2 \in [2]$ and $-1 \in [3]$. Using these representatives we have $[2]+[3] = [-2-1] = [-3]$ and $[2]\cdot[3] = [(-2)(-1)] = [2]$. Are our answers different from the original calculations? No: $[5] = [-3]$ and $[6] = [2]$.

With binary operations addition and multiplication defined on $\mathbb{Z}/n$, it is natural to ask whether we have groups.

PROPOSITION 6. (a) $\mathbb{Z}/n$ is an abelian group under addition.
(b) For $n \geq 2$, $\mathbb{Z}/n$ does not form a group under multiplication.

PROOF. Note that both operations $+$ and $\cdot$ on $\mathbb{Z}/n$ are associative:

$$[a]+([b]+[c]]) = [a]+[b+c] = [a+(b+c)] = [(a+b)+c] = [a+b]+[c] = ([a]+[b])+[c]$$

and

$$[a]+[b] = [a+b] = [b+a] = [b]+[a].$$

Similarly one checks these for multiplication. (As you can see, the associativity and commutativity are essentially a consequence of these properties of addition and multiplication on $\mathbb{Z}$.)
As for identity elements, $[0]$ is the idenity of addition: $[a]+[0] = [a+0] = [a]$. Similarly, $[1]$ is the identity of multiplication. Finally, under addition, the inverse of $[a]$ is $[-a]$ $(= [n-a])$, as

$$[a]+[-a] = [a-a] = [0].$$

Thus $\mathbb{Z}/n$ is an abelian group under addition. Under multiplication however, if $n \geq 2$, $[0]$ does not have an inverse. Indeed, suppose there is $[b] \in \mathbb{Z}/n$ such that $[0][b] = [1]$. This means $[0b] = [1]$, which is equivalent to $0b \equiv 1 \pmod{n}$, which is absurd. Thus $\mathbb{Z}/n$ is not a group under multiplication. □

From now on, if we talk about the group $\mathbb{Z}/n$ with no mention of the operation, we mean under addition. (Similar to us talking about the groups $\mathbb{Z}$ or $\mathbb{Q}$.) We have $|\mathbb{Z}/n| = n$.

As it was pointed out in the proof of the last proposition, multiplication on $\mathbb{Z}/n$ does pass the tests of associativity and existence of identity. It fails the axiom of inverses. We were in similar situations when studying $Mat_{n\times n}(\mathbb{Q})$ and $\mathbb{Q}$ under multiplication. In those instances, we resolved the issue by only considering the elements that do have multiplicative inverses. This approach lead to the groups $GL_n(\mathbb{Q})$ and $\mathbb{Q}^\times$. In the case of multiplication on $\mathbb{Z}/n$, we will do the same. We will need a result from arithmetic:

Exercise 18. Suppose $a \equiv b \pmod{n}$. Show that $gcd(a, n) = gcd(b, n)$.

We say a residue class mod n is coprime to n if the gcd of any (and hence all, thanks to the above exercise) of its representatives and n is 1. Residue classes mod 8 that are coprime to 8 are $[1], [3], [5], [7]$.

Notation: Denote by $U(n)$ (read units mod n) the subset of $\mathbb{Z}/n$ consisting of all residue classes coprime to n. Thus for instance,

$$U(8) = \{[1], [3], [5], [7]\}.$$

Note that if $[a], [b] \in U(n)$, then $gcd(a, n) = gcd(b, n) = 1$, and hence $gcd(ab, n) = 1$ (why?). Thus $[a][b] = [ab] \in U(n)$. This shows that the subset $U(n)$ of $\mathbb{Z}/n$ is closed under multiplication, so that multiplication on $\mathbb{Z}/n$ restricts to a binary operation on $U(n)$.

PROPOSITION 7. $U(n)$ is an abelian group under multiplication.

PROOF. We already know the operation is commutative and associative. Note that $[1] \in U(n)$ and is our identity element. What remains is the axiom of inverses. Suppose $[a] \in U(n)$. This

means $\gcd(a, n) = 1$. Thus by Problem 3(d) of Assignment 2, there are integers x, y such that $ax + ny = 1$. Note that this equality implies $\gcd(x, n) = 1$ as well, and hence $[x] \in U(n)$. The same equality also implies $ax \equiv 1 \pmod{n}$. But this means $[ax] = [1]$ (these being residue classes mod n), and hence by definition of multiplication on residues $[a][x] = [1]$. Thus $[x]$ (which we already saw is in $U(n)$) is the inverse of $[a]$. (Note that by commutativity, $[x][a] = [1]$ as well.) □

If we speak of the group $U(n)$ with no specific mention of the operation, we mean under multiplication. As an example, the Cayley table of $U(8)$ is included below.

$\cdot$	$[1]$	$[3]$	$[-3]$	$[-1]$
$[1]$	$[1]$	$[3]$	$[-3]$	$[-1]$
$[3]$	$[3]$	$[1]$	$[-1]$	$[-3]$
$[-3]$	$[-3]$	$[-1]$	$[1]$	$[3]$
$[-1]$	$[-1]$	$[-3]$	$[3]$	$[1]$

Let us recall the definition of Euler's φ function[†]: For any positive integer n, $\varphi(n)$ is the number of positive integers $\leq n$ that are coprime to n. Thus for instance, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 3$, and $\varphi(6) = 2$. For any prime number p, $\varphi(p) = p - 1$ (why?). Note that $|U(n)| = \varphi(n)$.

Exercise 19. Show that $[a] \in \mathbb{Z}/n$ has an inverse under multiplication if and only if $[a] \in U(n)$. (Note that the "if" part is already done in the proof of $U(n)$ being a group. The exercise asserts that the elements of $U(n)$ are exactly all the invertible elements of $\mathbb{Z}/n$ under multiplication. Usually invertible elements under multiplication are referred to as *units*, hence the notation $U(n)$.)

7. Cyclic groups

The material of this section except for Theorem 2 have already appeared in Assignments 2 and 3.

[†]sometimes called Euler's totient function

7.1. The subgroup generated by an element. Let G be a group. For each element $g \in G$, the subset

$$\langle g \rangle := \{g^n : n \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}.$$

of G is a subgroup. It is called the subgroup generated by g. For instance, the subgroup generated by $[3]$ in $U(8)$ is $\{[1], [3]\}$.

The following proposition summarizes some results we have already seen on the assignments. For the sake of completeness we include the proofs here as well.

PROPOSITION 8. (a) If $|g| = \infty$, the elements $\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots$ are all distinct.
(b) If $|g| = n < \infty$, then $e, g, \ldots, g^{n-1}$ are all distinct and $\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$.
(c) $|\langle g \rangle| = |g|$ (finite or infinite)

PROOF. (a) Suppose $g^i = g^j$ for some $i < j$. Then $g^{j-i} = e$, contradicting that g has infinite order.
(b) Suppose $g^i = g^j$ for some $0 \leq i < j \leq n-1$. Then $g^{j-i} = e$, where $0 < j - i \leq n-1$. This contradicts $|g| = n$ (why?). Thus $e, g, \ldots, g^{n-1}$ are all distinct. Given any $m \in \mathbb{Z}$, by the division algorithm we have $m = nq + r$ for some integers q, r, the latter satisfying $0 \leq r < n$. Then

$$g^m = g^{nq+r} \overset{\text{why}}{=} g^r \in \{e, g, \ldots, g^{n-1}\},$$

as desired.
(c) This follows from (a) and (b). □

Exercise 20. Let g be an element of a group G.

(a) Show that if a subgroup H of G contains g, then H contains $\langle g \rangle$.

(b) Show that $\langle g \rangle$ is the intersection of all subgroups of G which contain g.

7.2. Cyclic groups: Definition and recollections from Assignments 2 and 3.

DEFINITION. We say a group G is cyclic if there is an element $g \in G$ such that $\langle g \rangle = G$. If $\langle g \rangle = G$, we call g a generator of G.

For example, the following groups are cyclic:

- $\mathbb{Z}$ (with generators 1 and -1)
- $\mathbb{Z}/n$: A generator is $[1]$.
- μ_n: A generator is $e^{\frac{2\pi i}{n}}$.

Also, given any g in any group G, the subgroup $\langle g \rangle$ (which is a group in its own right) is cyclic.

Exercise 21. Show that every cyclic group is abelian.

Of course, not every abelian group is cyclic. For instance, direct calculation of the subgroups of $U(8)$ that are generated by each element (i.e. the cyclic subgroups) shows that $U(8)$ is not cyclic.

PROPOSITION 9. Let G be a group of (finite) order n. Let $g \in G$. Then $\langle g \rangle = G$ if and only if $|g| = n$. In particular, G is cyclic if and only if it has an element of order n.

PROOF. Suppose $\langle g \rangle = G$. Then by Proposition 8, $|g| = |G| = n$. Conversely, suppose $|g| = n$. Then the subgroup generated by g has n elements. Since G has only n elements, we must have $\langle g \rangle = G$.
The second assertion in the proposition is immediate from the first. □

Let G be a cyclic group of order n. Suppose g is a generator of G. Then by Proposition 8, the distinct elements of G are

$$g, g^2, \cdots, g^n = e.$$

By Proposition 9, generators of G are exactly the elements of order n. It follows that the generators of G are the elements g^k, where $1 \leq k \leq n$ is relatively prime to n (why?). In particular, we obtain:

COROLLARY 1. A cyclic group of order n has $\varphi(n)$ generators (φ being Euler's function).

Exercise 22. Let G be a finite group. Show that for any n, the number of elements of G that have order n is divisible by $\varphi(n)$.

7.3. The fundamental theorem of cyclic groups. Recall from Assignment 2 that every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some integer n. Note that $n\mathbb{Z}$ is the subgroup of $\mathbb{Z}$ generated by n, so that the result is saying that every subgroup of $\mathbb{Z}$ is cyclic. The first part of the following theorem asserts that the same is true for any cyclic group.

THEOREM 2 (Fundamental theorem of cyclic groups). Suppose G is a cyclic group. Then:

(a) Every subgroup of G is cyclic.

(b) Suppose in addition that G is finite. Then the order of every subgroup of G divides $|G|$. Moreover, for every positive divisor d of $|G|$, G has a unique subgroup of order d.

Before we prove the result, let us look at an example. The group $\mathbb{Z}/6$ is cyclic. Let us find the cyclic subgroups of $\mathbb{Z}/6$:

$$\langle [0] \rangle = \{[0]\}, \quad \langle [1] \rangle = \mathbb{Z}/6,$$

$$\langle [2] \rangle = \langle [4] \rangle = \{[0], [2], [4]\},$$

and

$$\langle [3] \rangle = \{[0], [3]\}.$$

By Part (a) of the theorem, these are *the only* the subgroups of $\mathbb{Z}/6$, so that $\mathbb{Z}/6$ has (exactly) 4 subgroups, namely $\{[0]\}$, $\mathbb{Z}/6$, $\{[0], [2], [4]\}$, and $\{[0], [3]\}$. Note that these have orders 1,6,3, and 2. All these orders divide $|\mathbb{Z}/6| = 6$. Moreover, every divisor of 6 is the order of exactly one subgroup of $\mathbb{Z}/6$ (as expected in view of the theorem).

PROOF OF THEOREM 2. Throughout, let g be a generator of G.

(a) Let H be a subgroup of G. If H is the trivial subgroup, then $H = \langle e \rangle$ and we are done. Suppose H is not the trivial subgroup. It follows that the set

$$\{m > 0 : g^m \in H\}$$

is non-empty (why?). Let k be the smallest number in this set. (In other words, k is the smallest positive integer such that $g^k \in H$.) We claim that $H = \langle g^k \rangle$. First note that since H is a subgroup that contains g^k, $\langle g^k \rangle \subset H$ (make sure you are okay with this). It remains to show that $H \subset \langle g^k \rangle$. Given any $h \in H$, there is $m \in \mathbb{Z}$ such that $h = g^m$ (why?). By the division algorithm, we can write $m = kq + r$, where $0 \leq r < k$. Note that $g^r = g^m g^{-kq}$. Since $g^m, g^k \in H$ and H is a subgroup, we get $g^r \in H$. On recalling $0 \leq r < k$ and the definition of k, it follows $r = 0$, so that $g^m = g^{kq} \in \langle g^k \rangle$. Thus $H \subset \langle g^k \rangle$ as desired.

(b) Suppose $|G| = n$. Let H be a subgroup of G. By Part (a) we know H is cyclic. Thus $H = \langle g^k \rangle$ for some integer k. We have

$$|H| \overset{\text{why}}{=} |g^k| \overset{\text{why}}{=} \frac{n}{\gcd(n,k)} \mid n.$$

This proves the first assertion.

Now suppose d is any positive divisor of n. We have to show that G has a unique subgroup of order d. Note that

$$|\langle g^{n/d}\rangle| = |g^{n/d}| = \frac{n}{gcd(n, n/d)} = \frac{n}{n/d} = d.$$

This proves the existence part: G does indeed have a subgroup of order d, namely the subgroup $\langle g^{n/d}\rangle$. It remains to show the uniqueness. Suppose $H' \leq G$ is also a subgroup of order d. We must show $H' = \langle g^{n/d}\rangle$. Note that since both H' and $\langle g^{n/d}\rangle$ have order d, it is enough to show that one of them is contained in the other. Let $H' = \langle g^{\ell}\rangle$. (How do we know such ℓ exists?) Then

$$d = |H| = |g^{\ell}| = \frac{n}{gcd(n, \ell)}.$$

It follows $\frac{n}{d} = gcd(n, \ell) \mid \ell$. Thus $g^{\ell} \in \langle g^{\frac{n}{d}}\rangle$ (why?) and $H' \subset \langle g^{\frac{n}{d}}\rangle$ as desired. □

Examples: (1) The group $\mathbb{Z}/30$ is cyclic and of order 30. By the fundamental theorem it has 8 (= the number of positive divisors of 30) subgroups, one of each order 1, 2, 3, 5, 6, 10, 15, and 30. Let us try to find the subgroup of order 6. Since $[1]$ has order 30, $[5] = 5[1]$ has order $\frac{30}{5} = 6$. The subgroup

$$\langle [5]\rangle = \{[0], [5], [10], [15], [20], [25]\}$$

is the (unique) subgroup of order 6. Note that, being a cyclic group of order 6, $\langle [5]\rangle$ has $\varphi(6) = 2$ generators. One generator is of course $[5]$. The other generator is $5[5] = [25]$. (See Problem 5 of Assignment 3 or the discussion prior to Corollary 1.)

(2) Consider the group μ_{30}, which is also cyclic of order 30. By the fundamental theorem, it has a unique subgroup of order 6. Call this subgroup H and let us try to find it. Let ζ be a generator of μ_{30}, say $e^{\frac{2\pi i}{30}}$. (Any other generator can be used. How many generators does μ_{30} have?) Then

$$\begin{aligned} H &= \langle \zeta^5\rangle = \{1, \zeta^5, \zeta^{10}, \zeta^{15}, \zeta^{20}, \zeta^{25}\} \\ &= \{1, e^{\frac{2\pi i}{6}}, e^{2\cdot\frac{2\pi i}{6}}, e^{3\cdot\frac{2\pi i}{6}}, e^{4\cdot\frac{2\pi i}{6}}, e^{5\cdot\frac{2\pi i}{6}}\}. \end{aligned}$$

We recognize that this is exactly the group μ_6 of 6-th roots of unity! Indeed, to find H, we did not have to go through the above calculation: μ_6 is a subgroup of μ_{30} and has order 6, so that by the (uniqueness part of the) fundamental theorem, H must be equal to μ_6. Similarly, μ_{10} is the unique

subgroup of μ_{30} of order 10. The subgroups of μ_{30} are:

$$\mu_1,\ \mu_2,\ \mu_3,\ \mu_5,\ \mu_6,\ \mu_{10},\ \mu_{15}, \text{ and } \mu_{30}.$$

8. Symmetric groups

8.1. The order of S_n. Let n be a positive integer. Recall that the set of all bijections

$$\{1, \cdots, n\} \to \{1, \cdots, n\}$$

forms a group under composition of functions. As mentioned earlier, this group is called the symmetric group of degree n, and is denoted by S_n. Elements of S_n are called *permutations* of the set $\{1, \cdots, n\}$. In other words, a permutation[†] of $\{1, \cdots, n\}$ is by definition a bijective function

$$\{1, \cdots, n\} \to \{1, \cdots, n\}.$$

It is easy to see that $|S_n| = n!$. Indeed, to define a bijection σ from $\{1, \cdots, n\}$ to itself, one can choose $\sigma(1)$ arbitrarily, then $\sigma(2)$ can be any element but $\sigma(1)$, $\sigma(3)$ can be anything but $\sigma(1)$ and $\sigma(2)$, and so on. It follows that there are

$$n \cdot (n-1) \cdot (n-2) \cdots 1$$

permutations of $\{1, \cdots, n\}$.

REMARK. More generally, for any nonempty set X, by a permutation of X one means a bijective function $X \to X$. The set of all permutations of X form a group under composition of functions. This group is called the symmetric group on X. If X is finite and has n elements, the symmetric group on X has $n!$ elements.

8.2. Cycles. Since S_n is a finite group, every element of S_n has finite order. In other words, for every permutation σ of $\{1, \cdots, n\}$ there is a positive integer m such that σ^m ($=\sigma \circ \sigma \circ \cdots$) is the identity function. Our goal in this section and the next is to give an efficient notation for permutations which will enable us to calculate the order of a permutation very quickly.

[†]This interpretation of a permutation might not be in line with what you have seen in earlier courses, but has the advantage that now permutations can be composed, whereas if you think of permutations simply as arrangements of numbers, it is not clear how to define a natural binary operation on them.

First, a general piece of terminology: One says a function $f : X \to X$ fixes an element $x \in X$ if $f(x) = x$. If x is not fixed by f, we say f acts nontrivially on x. For instance, the function $f : [0,1] \to [0,1]$ defined by $f(x) = 1 - x$ fixes $\frac{1}{2}$ and no other element of $[0,1]$. In other words, f acts nontrivially on every $x \in [0,1] - \{\frac{1}{2}\}$.

Let $a_1, \cdots, a_\ell$ be distinct numbers from $1, \cdots, n$. The permutation of $\{1, \cdots, n\}$ which maps

$$a_\ell \mapsto a_1,\ a_1 \mapsto a_2,\ a_2 \mapsto a_3, \cdots,\ a_{\ell-1} \mapsto a_\ell,$$

and fixes all the other numbers is called a *cycle* and is denoted by $(a_1 a_2 \cdots a_\ell)$. The number ℓ is called the *length* of the cycle. By an ℓ-cycle we mean a cycle of length ℓ.

Thus for instance, the cycle $(124) \in S_5$ is the permutation that maps $1 \mapsto 2$, $2 \mapsto 4$, $4 \mapsto 1$, $3 \mapsto 3$, and $5 \mapsto 5$. Note that (241) and (412) refer to the exact same element of S_5. More generally,

$$(a_1 a_2 \cdots a_\ell) = (a_2 \cdots a_\ell a_1) = (a_3 \cdots a_\ell a_1 a_2) = \cdots = (a_\ell a_1 a_2 \cdots a_{\ell-1}). \tag{7}$$

Note that $(1) \in S_n$ maps $1 \mapsto 1$ and fixes every other number. In other words, (1) is the identity permutation. Similarly, $(1) = (2) = \cdots = (n)$ is the simply the idenity of S_n.

Being permutations, cycles can be composed and the composition is a permutation (but not necessarily a cycle). For instance, let us try to find $(132) \circ (215)$ in S_5. Let $\sigma = (132)$ and $\delta = (215)$. Then

$$\sigma \circ \delta(1) = \sigma(\delta(1)) = \sigma(5) = 5 \qquad \text{and} \qquad \sigma \circ \delta(2) = \sigma(\delta(2)) = \sigma(1) = 3.$$

Similarly one finds $\sigma \circ \delta(3) = 2$, $\sigma \circ \delta(4) = 4$, and $\sigma \circ \delta(5) = 1$. Usually one drops the symbol $\circ$ for convenience and simply for example writes $\sigma\delta(1) = 5$. Note that thinking of (132) and (215) as elements of S_6 (and denoting them again by σ and δ) our previous calculations are still valid. Now in addition one has $\sigma\delta(6) = 6$.

One easily checks $(12)(13) = (132)$ and $(13)(12) = (123)$. Since $(123) \neq (132)$ (look at where they send 1 for instance), we see that S_n is not abelian for $n \geq 3$.

Let $\sigma = (a_1 a_2 a_3 a_4)$. Then $\sigma^2(a_1) = \sigma(\sigma(a_1)) = \sigma(a_2) = a_3$. A similar calculation shows $\sigma^2(a_2) = a_4$, $\sigma^2(a_3) = a_1$, and $\sigma^2(a_4) = a_2$. More generally, let $\sigma = (a_1 a_2 \cdots a_\ell)$. Writing the numbers $a_1, a_2, \cdots, a_\ell$ around a circle clockwise, σ sends each number to the next number clockwise;

σ^2 sends every number to the second next number clockwise. In general, σ^r sends every number to the next r-th number clockwise (and of course, fixes numbers not in $\{a_1, a_2, \cdots, a_\ell\}$).

PROPOSITION 10. Let $\sigma = (a_1 a_2 \cdots a_\ell)$. Then $|\sigma| = \ell$ and $\sigma^{-1} = (a_\ell \cdots a_2 a_1)$.

PROOF. From the preceding discussion we see that (i) for $0 < r < \ell$, $\sigma^r(a_1) \neq a_1$, and (ii) $\sigma^\ell = e$. Thus $|\sigma| = \ell$. For the assertion about the inverse, one easily sees

$$(a_1 a_2 \cdots a_\ell)(a_\ell \cdots a_2 a_1)$$

fixes each of the a_i (and of course everything else), and hence is the identity. □

Exercise 23. Consider the elements $\sigma = (a_1 \cdots a_\ell)$ and $\delta = (b_1 \cdots b_k)$ of S_n. Suppose $\sigma = \delta \neq e$ (thus $k, \ell > 1$). Show that $\ell = k$ and that there is i such that

$$b_1 = a_i,\ b_2 = a_{i+1},\ \cdots,\ b_\ell = a_{i-1}.$$

(Here we set $a_0 = a_\ell$.)

Let $\sigma, \delta \in S_n$. We say σ and δ are *disjoint* if there is no i on which both σ and δ act nontrivially, i.e. if

$$\{i : \sigma(i) \neq i\} \cap \{i : \delta(i) \neq i\} = \emptyset.$$

In other words, we say σ and δ are disjoint if for every i, either $\sigma(i) = i$ or $\delta(i) = i$ (or both). For cycles $(a_1 \cdots a_\ell)$ and $(b_1 \cdots b_k)$ of length > 1, being disjoint is equivalent to that

$$\{a_1, \cdots, a_\ell\} \cap \{b_1, \cdots, b_k\} = \emptyset.$$

Thus for instance, (156) and (2347) are disjoint.

Intuitively, disjoint permutations permute disjoint sets of numbers, and as such it shouldn't matter in which order they are applied. In other words, they should commute. Let us formally prove this:

PROPOSITION 11. Disjoint permutations (and in particular disjoint cycles) cummute. In other words, if σ and δ are disjoint permutations (in particular disjoint cycles), then $\sigma\delta = \delta\sigma$.

PROOF. We shall show that $\sigma\delta(i) = \delta\sigma(i)$ for every i. Indeed, if i is fixed by both σ and δ, then $\sigma\delta(i) = \delta\sigma(i) = i$. Suppose one of σ or δ, say σ, doesn't fix i. Then δ must fix i (by disjointness),

so that $\sigma\delta(i) = \sigma(i)$. Now note that since σ doesn't fix i, it cannot fix $\sigma(i)$ either: If $\sigma(\sigma(i)) = \sigma(i)$, then σ is mapping i and $\sigma(i)$ to $\sigma(i)$, which is absurd since σ is injective. (Where in this argument is the assumption that σ doesn't fix i used?) Since σ doesn't fix $\sigma(i)$, by disjointness δ must fix $\sigma(i)$. Thus $\delta\sigma(i) = \delta(\sigma(i)) = \sigma(i)$. □

PROPOSITION 12. Let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be (pairwise) disjoint cycles. Then

$$|\sigma_1\sigma_2\cdots\sigma_r| = \text{the least common multiple of } |\sigma_1|,\ |\sigma_2|, \cdots,\ |\sigma_r|.$$

PROOF. Denote the length of σ_i by ℓ_i (thus $|\sigma_i| = \ell_i$) and let L be the least common multiple of $\ell_1, \ldots, \ell_r$. First note that since $\ell_i \mid L$, $\sigma_i^L = e$, and by the previous proposition (since the σ_i are disjoint)

$$(\sigma_1\sigma_2\cdots\sigma_r)^L = \sigma_1^L\sigma_2^L\cdots\sigma_r^L = e.$$

It remains to show that if $0 < k < L$, $(\sigma_1\sigma_2\cdots\sigma_r)^k \neq e$. By the minimality property of L, $\ell_i \nmid k$ for some i. Since the σ_i commute, we may assume $i = 1$. Let a be one of the numbers which σ_1 does not fix (i.e. one of the numbers that "appear" in σ_1). By disjointness, a is fixed by $\sigma_2, \cdots, \sigma_r$, and hence

$$(\sigma_1\sigma_2\cdots\sigma_r)^k(a) = (\sigma_1^k\sigma_2^k\cdots\sigma_r^k)(a) = \sigma_1^k(a).$$

Since $\ell_1 \nmid k$, $\sigma_1^k(a) \neq a$ and hence $(\sigma_1\sigma_2\cdots\sigma_r)^k \neq e$. □

Thus for instance, since the cycles (13), (245) and (6789) are disjoint, the order of $(13)(245)(6789)$ is 12 (=the least common multiple of 2,3,4). One should be careful that the disjointness assumption is crucial in the result. For instance, $(12)(23) = (123)$ and has order 3.

8.3. Cycle decomposition. In view of Proposition 12, if we could express a permutation as a product (i.e. composition) of disjoint cycles, then we could simply read off the order by looking at the lengths of the cycles. This raises the following question: Can we express every permutation as a product of disjoint cycles? We shall see that the answer is yes, and in fact this can be done in an essentially unique way. (As unique as one can hope for, see below.)

Suppose $\sigma \in S_n$. A *cycle decomposition* of σ is an expression of σ as a product

$$\sigma = \delta_1\delta_2\cdots\delta_r$$

of cycles $\delta_1, \cdots, \delta_r$ such that every $i \in \{1, \cdots, n\}$ appears in exactly one of the the δ_i. For instance, consider $\sigma \in S_7$ defined by

$$\sigma(1) = 2,\ \sigma(2) = 4,\ \sigma(3) = 3,\ \sigma(4) = 1,\ \sigma(5) = 6,\ \sigma(6) = 7,\ \sigma(7) = 5. \tag{8}$$

One easily can check that $(124)(3)(567) = \sigma$. Thus $(124)(3)(567)$ is a cycle decomposition of σ. Note that the cycles appearing in a cycle decomposition are disjoint (as every $i \in \{1, \cdots, n\}$ appears in exactly one of the the cycles in the decomposition.)

The following result answers the question posed at the beginning of this paragraph.

PROPOSITION 13 (Existence and uniqueness of cycle decomposition). Every permutation $\sigma \in S_n$ has a cycle decomposition. Moreover, the decomposition is unique up to rearranging the factors. That is, if

$$\delta_1 \cdots \delta_r = \delta'_1 \cdots \delta'_s$$

are both cycle decompositions of σ, then $r = s$ and the cycles $\delta_1, \ldots$ are exactly the cycles $\delta'_1, \ldots$ possibly in a different order[†].

Let us make a few remarks before we proceed:

(1) Consider the element $\sigma \in S_7$ defined in Eq. (8). We saw $\sigma = (124)(3)(567)$. Since disjoint cycles commute, σ is also equal to $(567)(124)(3)$. The uniqueness assertion is that up to rearrangements of this form this is the only way of expressing σ as a product of disjoint cycles in which each of the numbers $1, \cdots, 7$ appear one time.

(2) The assertion is clear for $\sigma = e$. Indeed, $(1)(2)\cdots(n)$ is a cycle decomposition of e, and up to rearranging the 1-cycles this is the unique cycle decomposition, as any product of disjoint cycles one of which is of length > 1 is not identity. (So any cycle decomposition has to be a product of 1-cycles.)

(3) Proposition 13 can be equivalently formulated as follows: Every $\sigma \in S_n$ that is not identity can be expresses as a product of disjoint cycles of length > 1, and moreover this can be done in a unique way up to rearranging the factors.

As to why Proposition 13 is true, we'll be satisfied with an informal argument. Writing a formal proof here can be (especially notationally) painful (but not hard) and doesn't really add

[†] i.e. there is a permutation π of $\{1, \ldots, r\}$ such that $\delta'_i = \delta_{\pi(i)}$ for each i.

any new insight. For existence, we shall give an algorithm that finds a cycle decomposition. The algorithm is best described on an example. Consider the permutation $\sigma \in S_{10}$ defined by

(9)

$$\sigma(1) = 4,\ \sigma(2) = 6,\ \sigma(3) = 3,\ \sigma(4) = 2,\ \sigma(5) = 8,\ \sigma(6) = 1,\ \sigma(7) = 9,\ \sigma(8) = 10,\ \sigma(9) = 7,\ \sigma(10) = 5.$$

We start with any number in $\{1, \cdots, 10\}$, say 1. We start a cycle $(1$. Note that if this cycle is one of the cycles in a decomposition of σ, the number next to 1 in it *must* be $\sigma(1)$ (as the other cycles not affect where 1 is mapped). We write $\sigma(1)$, i.e. 4, next to 1 in our cycle; at this point we have $(14$. Again, if this is to be a cycle in a cycle decomposition, the number next to 4 in it must by $\sigma(4) = 2$. Thus we add 2 to our cycle and get $(142$. Now we add $\sigma(2) = 6$ to the cycle. At this stage our cycle looks like $(1426$. Next, we find $\sigma(6)$. We note that $\sigma(6) = 1$. Thus we close the cycle: (1426). This will be one of the cycles in our decomposition. Now we find a number that did not appear in this cycle, say 3 (the smallest one, but any of them will do). We open a new cycle $(3$. Since $\sigma(3) = 3$, we close the cycle: (3). Now we look for a number that hasn't appeared in any of our 2 cycles so far, say 5. We start a new cycle $(5$. We have $\sigma(5) = 8$, so we write 8 next to 5; we get $(58$. Since $\sigma(8) = 10$, we write 10 next to 8: $(58\ 10$. Finally, since $\sigma(10) = 5$, we close the cycle: $(58\ 10)$. Now we open a new cycle $(7$, then add 9 to it (why?) and get $(79$, and then close the bracket (why?). Our cycle decomposition is

$$(1426)(3)(58\ 10)(79).$$

One can show that the algorithm above always terminates in a cycle decomposition. Note that in the process if you see that the cycles you calculated are not disjoint there must be a mistake somewhere.

The uniqueness assertion should be easy to believe. In the example above, if $\delta_1\delta_2\cdots$ is a cycle decomposition of σ, the number 1 must appear in exactly in one of the δ's, say δ_i. Then $\delta_i = (1\cdots)$ (by Eq. (7)). Since the δ's are disjoint, $\sigma(1) = \delta_i(1)$, so that δ_i must look like $(14\cdots)$. Continuing the same reasoning, we see δ_i must be (1426).

Suppose a permutation $\sigma \in S_n$ has cycle decomposition $\delta_1 \cdots \delta_r$, where δ_i has length (order) ℓ_i and $\ell_1 \geq \cdots \geq \ell_r$. We then say σ is of cycle decomposition type (or cycle type) $\ell_1, \cdots, \ell_r$. For instance, the permutation $\sigma \in S_{10}$ defined in Eq. (9) is of cycle decomposition type 4,3,2,1. By Proposition 12, the order of a permutation only depends on its cycle decomposition type. For

instance, every element of S_{10} of type 4,3,2,1 (and in particular our σ from the example) has order 12.

Convention: It is customary that usually one doesn't write the 1-cycles in the cycle decomposition. Thus for instance, one usually says the cycle deomposition of σ as in Eq. (9) is $(1426)(58\,10)(79)$. Of course, the identity is exempted from this rule, as its cycle decomposition only consists of 1-cycles. When speaking of the cycle type however, we will continue to include the 1-cycles.

Example: Let us try to find the order of $(1273)(4263)(7651) \in S_8$ (or in any S_n with $n \geq 7$). Note that the cycles in the product are not disjoint, so that we can not immediately use Proposition 12. We first find the cycle decomposition. Following our algorithm, we open a cycle $(1$. Now we have to find the image of 1 under our permutation. Note that 1 goes to 7 by the cycle on the right, 7 is fixed by the middle cycle, and then 7 is mapped to 3 by the cycle on the left. It follows the composition maps $1 \mapsto 3$. Thus we write $(13$. Next,

$$3 \overset{(7651)}{\longmapsto} 3 \overset{(4263)}{\longmapsto} 4 \overset{(1273)}{\longmapsto} 4.$$

Thus we write $(134$, and so on. In the end we see $(1273)(4263)(7651) = (1347)(265)$ and hence has order 12.

Example: Consider the group S_5. It has $5! = 120$ elements. Thus by what we have learned so far in the course, each of its elements has order ≤ 120. Let us see what numbers actually occur as the orders of elements of S_5. As we discussed, the order of each element only depends on its cycle type. Possible types are:

(i) 5: These are the five cycles. They have order 5.

(ii) 4,1: These are the 4-cycles. They have order 4.

(iii) 3,2: These are products of a disjoint 3-cycle and a 2-cycle. They have order 6.

(iv) 3,1,1: These are the 3-cycles. They have order 3.

(v) 2,2,1: These are products of two disjoint 2-cycles. They have order 2.

(vi) 2,1,1,1: These are the 2-cycles. They have order 2.

(vii) 1,1,1,1,1: Product of five 1-cycles. This is the cycle type of only the identity element.

Thus the only numbers that appear as the order of an element of S_5 are 1,2,3,4,5,6. (Compare with the cyclic groups which have an element of each order dividing the order of the group.)

One can take the above example further and ask how many elements of say order 5 the group S_5 has. In other words, how many 5-cycles are there in S_5? By Eq. (7) we can fix 1 to be the first number in the cycle. By Exercise 23, each way of writing the numbers 2,3,4,5 to complete our cycle will result in a different 5-cycle. Thus the number of 5-cycles (= the number of elements of order 5) is $4! = 24$.

Let us also find the number of elements of S_5 of order 2. These are permutations of types 2,2,1 or 2,1,1,1. There are $\binom{5}{2} = 10$ elements of the latter type. (Note that $(ab) = (ba)$, so that by simply choosing the two numbers appearing in a 2-cycle the 2-cycle is determined.) The number of elements of type 2,2,1 is

$$\binom{5}{2} \cdot \binom{3}{2} \cdot \frac{1}{2} = 15.$$

(The first factor chooses the first 2-cycle, the second factor chooses the second 2-cycle, and the division by 2 is done since $(ab)(cd) = (cd)(ab)$ for distinct a, b, c, d.) Thus there are 25 elements of order 2 in S_5. By similar arguments, one can see that there are

$$\binom{5}{4} \cdot 3! = 30$$

elements of order 4, and

$$\binom{5}{3} \cdot 2 = 20$$

elements of each order 6 and 3. Of course, there is only 1 element of order 1, namely the identity. (Note that the numbers we calculated indeed add up to 120!)

8.4. Alternating groups. Our goal in this section is to define a notion of parity (i.e. even and odd) for permutations. We start by recalling a result from Assignment 4.

LEMMA 2. Let $n \geq 2$. Every element of S_n can be expresses as a product of 2-cycles.

PROOF. First note that the identity element can be written as $(12)(12)$. It remains to prove the statement for non-identity elements. By Proposition 13 every non-identity element can be expressed as a product of disjoint cycles of length > 1, so that it is enough to show that cycles of length > 1 can be written as products of 2-cycles. Let $\ell > 1$. One easily sees

$$(a_1 a_2 \cdots a_\ell) = (a_1 a_2)(a_2 a_3)(a_3 a_4) \cdots (a_{\ell-1} a_\ell). \tag{10}$$

(Alternatively, $(a_1 a_2 \cdots a_\ell) = (a_1 a_\ell)(a_1 a_{\ell-1}) \cdots (a_1 a_2)$.) □

Note that the 2-cycles in the lemma are not necessarily disjoint. Also note that the proof actually gives an algorithm for writing a permutation as a product of 2-cycles. Indeed, we first express the given permutation as a product of disjoint cycles, and then write each cycle as a product of 2-cycles using one of the two methods described in the proof. For instance, the permutation defined in Eq. (9) is

$$(1426)(58\ 10)(79) = (14)(42)(26)(58)(8\ 10)(79).$$

Of course, a permutation can be expressed as a product of 2-cycles in more than one way. For instance, the permutation of Eq. (9) can also be written as

$$(16)(14)(42)(13)(79)(5\ 10)(58)(13).$$

The following result tells us that even though the same permutation can be expressed as a product of 2-cycles in many ways, the parity of the 2-cycles involved remains invariant.

LEMMA 3. Let $\sigma \in S_n$. Suppose

$$\sigma = \tau_1 \cdots \tau_\ell = \delta_1 \cdots \delta_k,$$

where the τ_i and δ_i are 2-cycles. Then $\ell \equiv k \pmod 2$.

We will skip the proof of this result. The interested reader can find a proof in the textbook. The result asserts for instance that since the permutation of Eq. (9) is equal to $(14)(42)(26)(58)(8\ 10)(79)$, in *any* expression of this permutation as a product of 2-cycles there will be an even number of factors. As another example, since $e = (12)(12)$ is a product of two 2-cycles, no matter how we write e as a product of 2-cycles, there will always be an even number of 2-cycles. On the other hand, in any expression of the permutation (1234) as a product of 2-cycles, there will be an odd number of 2-cycles, as $(1234) = (12)(23)(34)$.

Now we define the notion of parity for permutations.

DEFINITION. Let $n \geq 2$. Let $\sigma \in S_n$. We say σ is even if it can be written as a product of an even number of 2-cycles. We say σ is odd if it can be written as a product of an odd number of 2-cycles.

Note that every permutation is either even or odd (by Lemma 2), and not both (by Lemma 3). We define the *sign* of a permutation σ (denoted by $sgn(\sigma)$) to be

$$sgn(\sigma) := \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

In other words, if $\sigma = \tau_1 \cdots \tau_\ell$ where the τ_i are 2-cycles, then $sgn(\sigma) = (-1)^\ell$. Thus for instance, the identity is an even permutation, whereas any 2-cycle is an odd permutation. More generally, in view of Eq. 10 an ℓ-cycle is odd (resp. even) if ℓ is even (resp. odd).

Example: The permutation $\sigma = (234)(1234)(24536)(1456)$ is even. Indeed, 3-cycles and 5-cycles are even, whereas 4-cycles are odd, so that σ can be expressed as a product of an

$$\text{even} + \text{odd} + \text{even} + \text{odd} = \text{even}$$

number of permutations.

Exercise 24. Let $n \geq 2$.
(a) Show that all permutations of the same cycle decomposition type have the same parity.
(b) Which cycle decomposition types in S_6 correspond to even permutations?

PROPOSITION 14. (a) The product of two permutations with the same parity (i.e. both even or both odd) is even, and the product of an odd and an even permutation is odd.
(b) A permutation and its inverse have the same parity.

PROOF. (a) Let σ be a product of ℓ 2-cycles and δ be a product of k 2-cycles. Then $\sigma\delta$ is a product of $\ell + k$ 2-cycles. If $\ell \equiv k \pmod 2$, $\ell + k$ is even. Otherwise $\ell + k$ is odd.
(b) If $\sigma = \tau_1 \cdots \tau_\ell$ where the τ_i are 2-cycles, then $\sigma^{-1} = \tau_\ell \cdots \tau_1$. In particular, σ and σ^{-1} have the same parity. □

Let $n \geq 2$. Let A_n be the subset of S_n consisting of all the even permutations. We already noted that e is even, so $e \in A_n$. By Part (a) of the previous proposition, A_n is closed under the group operation. By Part (b) A_n is also closed under taking inverses. It follows that A_n is a subgroup of S_n. We call A_n the *Alternating group of degree* n.

The map $\sigma \mapsto (12)\sigma$ gives a bijection

$$A_n = \text{the set of all even elements of } S_n \longrightarrow \text{ the set of all odd elements of } S_n.$$

It follows that exactly half the elements of S_n are even, i.e. $|A_n| = \frac{1}{2}n!$.

Example: The subgroup A_4 of S_4 has order 12. Let us find all the elements of A_4 by going through the cycle types and recongnizing the ones corresponding to the even elements. The 4-cycles in S_4 are odd. The 3-cycles (i.e. elements of type 3,1) are even. Elements of type 2,2 are even. Elements of type 2,1,1 are odd. Finally, identity is even. Thus A_4 consists of the 3-cycles (of which there are $\binom{4}{3} \cdot 2 = 8$), the elements of type 2,2 (of which there are $\binom{4}{2}\frac{1}{2} = 3$), and the identity. (Note that $8 + 3 + 1 = 12$.)

9. Homomorphisms

9.1. Definition and examples.

DEFINITION. Let G and H be groups. Denote the operation in G by $\star$ and the operation in H by $*$. A map (=function) $\phi : G \to H$ is called a (group) homomorphism if for every $g, g' \in G$,

$$\phi(g \star g') = \phi(g) * \phi(g').$$

Dropping the operation symbols as usual, a function $\phi : G \to H$[†] is a homomorphism if

$$\phi(gg') = \phi(g)\phi(g') \tag{11}$$

for all $g, g' \in G$. Note that even though it may not be explicitly visible in Eq. (11), one has to keep in mind that the operation on the two sides may not be the same: The product gg' on the left takes place in G, whereas $\phi(g)\phi(g')$ on the right takes place in H.

Examples: (1) Let V and W be vector spaces. Then V are W are groups under addition. Any linear transformation $\phi : V \to W$ is a group homomorphism between the underlying additive groups. Indeed, one of the two defining properties of a linear transformation $\phi : V \to W$ is that for all $v, v' \in V$, $\phi(v + v') = \phi(v) + \phi(v')$.

[†]Recall that if ϕ is a function $G \to H$, we call G (resp. H) the domain (resp. codomain) of ϕ.

(2) Recall that for the determinant of an invertible matrix is nonzero. Thus we have a map $GL_n(\mathbb{R}) \to \mathbb{R}^\times$ given by $A \mapsto \det(A)$. The well-known formula $\det(AB) = \det(A)\det(B)$ tells us that this map is a homomorphism. (Same is of course true if $\mathbb{R}$ is replaced by $\mathbb{Q}$ or $\mathbb{C}$.)

(3) Let $n \geq 2$. Consider the sign map $sgn : S_n \to \mu_2$. We claim that sgn is a group homomorphism. Indeed, let $\sigma, \delta \in S_n$. Suppose σ (resp. δ) is a product of ℓ (resp. k) 2-cycles, so that $sgn(\sigma) = (-1)^\ell$ and $sgn(\delta) = (-1)^k$. Then $\sigma\delta$ is a product of $\ell + k$ 2-cycles, and hence $sgn(\sigma\delta) = (-1)^{\ell+k}$. Now we have

$$sgn(\sigma\delta) = (-1)^{\ell+k} = (-1)^\ell(-1)^k = sgn(\sigma)sgn(\delta).$$

(4) Let $n \in \mathbb{Z}$. Define a map $\phi : \mathbb{Z} \to \mathbb{Z}$ by $a \mapsto na$. (This is called the multiplication by n map, as one would expect.) The equation

$$n(a + b) = na + nb$$

tells us that ϕ is a homomorphism. (Note that $n(a + b) = \phi(a + b)$ and $na + nb = \phi(a) + \phi(b)$.)

(5) The previous example can be generalized as follows. Let G be an abelian group and $n \in \mathbb{Z}$. Define $\phi : G \to G$ by $\phi(g) = g^n$. This is a homomorphism as

$$\phi(gh) = (gh)^n \overset{(\star)}{=} g^n h^n = \phi(g)\phi(h).$$

The assumption that G is abelian is used in $(\star)$. Note that we obtain the previous example if we take $G = \mathbb{Z}$. If the group G is not abelian, this construction usually does not result in homomorphisms. For instance, the map $S_3 \to S_3$ given by $\sigma \mapsto \sigma^2$ is not a homomorphism, as

$$((12)(23))^2 \neq (12)^2(23)^2.$$

(The left hand sind is $(123)^2 = (132)$ whereas the right hand side is identity.)

(6) Let $n \geq 1$. The map $\mathbb{Z} \to \mathbb{Z}/n$ defined by $a \mapsto [a]$ (i.e. the map than sends a number to its residue class mod n) is a group homomorphism, as

$$[a + b] = [a] + [b].$$

This map is sometimes referred to as *reduction mod* n.

(7) Define the map $exp : \mathbb{R} \to \mathbb{R}^\times$ (called the exponential map) by $exp(x) = e^x$. The formula $e^{x+y} = e^x e^y$ tells us that exp is a group homomorphism. (Same is true for $\mathbb{C}$.)

(8) Consider $\mathbb{R}_{>0}$ under multiplication. The map $\mathbb{R}_{>0} \to \mathbb{R}$ given by $x \mapsto \log x$ is a homomophism. This follows from the identity $\log(xy) = \log(x) + \log(y)$.

(9) Let G be any group. The identity map $G \to G$ (which sends $g \mapsto g$) is a group homomorphism.

(10) Let G and H be any groups. The map $G \to H$ which sends every element of G to e_H is a group homomorphism. (This is usually referred to as the trivial homomorphism from G to H.)

(11) Let G be a subgroup of H. Consider the map $\iota : G \to H$ defined by $\iota(g) = g$. This map is a group homomorphism. (One sometimes calls ι ithe inclusion map.)

Exercise 25. Let G be a group. Show that the map $\phi : G \to G$ defined by $\phi(g) = g^{-1}$ is a homomorphism if and only if G is abelian.

9.2. Basic properties of homomorphisms.

PROPOSITION 15. Let $\phi : G \to H$ be a homomorphism. Then we have:

(a) $\phi(e_G) = e_H$ (where e_G and e_H denote the identities of G and H)

(b) For every $g \in G$, $\phi(g^{-1}) = (\phi(g))^{-1}$.

PROOF. (a) We have

$$\phi(e_G)\phi(e_G) = \phi(e_G e_G) = \phi(e_G).$$

Multiplying by the inverse of $\phi(e_G)$ we get $\phi(e_G) = e_H$.

(b) We have

$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_G) = e_H.$$

It follows that $\phi(g^{-1}) = (\phi(g))^{-1}$. □

Exercise 26. Let $\phi : G \to H$ be a homomorphism. Let $g \in G$. Show that for any $n \in \mathbb{Z}$, $\phi(g^n) = (\phi(g))^n$.

Exercise 27. Let $\phi : G \to H$ be a homomorphism. Let $g \in G$ be an element of finite order. Show that $\phi(g)$ also has finite order and that $|\phi(g)|$ divides $|g|$.

PROPOSITION 16. Let $\phi : G \to H$ and $\psi : H \to K$ be homomorphisms. Then the composition $\psi \circ \phi : G \to K$ is a homomorphism.

PROOF. Let $g, g' \in G$. We have

$$\psi \circ \phi(gg') = \psi(\phi(gg')) \overset{(*)}{=} \psi(\phi(g) \cdot \phi(g')) \overset{(**)}{=} \psi(\phi(g)) \cdot \psi(\phi(g')) = \psi \circ \phi(g) \cdot \psi \circ \phi(g').$$

(Note that in $(*)$ (resp. $(**)$) we used the fact that ϕ (resp. ψ) is a homomorphism. □

9.3. Kernels and images. Let $\phi : G \to H$ be a group homomorphism. We define the *kernel* of ϕ to be

$$\ker(\phi) := \{g \in G : \phi(g) = e_H\}.$$

In other words, the kernel of ϕ is the set of all elements of G that get mapped by ϕ to the identity of H. Note that by definition $\ker(\phi)$ is a subset of the domain of ϕ.

The image of ϕ is the subset

$$\mathrm{Im}(\phi) := \{\phi(g) : g \in G\} = \{h \in H : \ h = \phi(g) \text{ for some } g \in G\}$$

of H.[†] More generally, given any subset $S \subset G$, we define

$$\phi(S) := \{\phi(g) : g \in S\}.$$

We call $\phi(S)$ the image of S under ϕ. Note that $\mathrm{Im}(\phi) = \phi(G)$.

PROPOSITION 17. Let $\phi : G \to H$ be a group homomorphism.

(a) $\ker(\phi)$ is a subgroup of G.

(b) $\mathrm{Im}(\phi)$ is a subgroup of H.

(c) For every subgroup $K \leq G$, the image $\phi(K)$ is a subgroup of H. (In short, image of a subgroup under a homomorphism is a subgroup.)

PROOF. (a) We show that $\ker(\phi)$ satisfies the three defining axioms of a subgroup. Since $\phi(e_G) = e_H$, $e_G \in \ker(\phi)$. Now let $g, g' \in \ker(\phi)$. This means $\phi(g) = \phi(g') = e_H$. Then

[†]Recall that in general given a function $f : X \to Y$ (for any sets X and Y) the image (or range) of f is $\mathrm{Im}(f) := \{f(x) : x \in X\}$.

$\phi(gg') = \phi(g)\phi(g') = e_H e_H = e_H$. Hence $gg' \in \ker(\phi)$ and $\ker(\phi)$ is closed under the operation (of G, of course). Also, $\phi(g^{-1}) = (\phi(g))^{-1} = e_H^{-1} = e_H$. Thus $g^{-1} \in \ker(\phi)$ and $\ker(\phi)$ is closed under inverses as well.

(b) First note that $e_H = \phi(e_G) \in \mathrm{Im}(\phi)$. Now let $h, h' \in \mathrm{Im}(\phi)$. Then by definition of $\mathrm{Im}(\phi)$, there are $g, g' \in G$ such that $\phi(g) = h$ and $\phi(g') = h'$. We have $hh' = \phi(g)\phi(g') = \phi(gg')$ and $h^{-1} = (\phi(g))^{-1} = \phi(g^{-1})$. Thus both hh' and h^{-1} are in $\mathrm{Im}(\phi)$.

(c) Let K be a subgroup of G. Let $\iota : K \to G$ be the inclusion map (see Problem 4a(iii) of Assignment 5). Note that $\phi(K)$ is exactly the image of the composition $\phi \circ \iota$. By (b) this is a subgroup of H. □

Examples: (1) Let K be any of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Let $\det : GL_n(K) \to K^\times$ be the determinant map. We have $\ker(\det) = SL_n(K)$ and $\mathrm{Im}(\det) = K^\times$ (why?).

(2) The kernel of the sign map $S_n \to \{1, -1\}$ is the alternating group A_n. Its image is $\{1, -1\}$ (why?).

(3) The kernel of the reduction mod n map $\mathbb{Z} \to \mathbb{Z}/n$ (defined by $a \mapsto [a]$) is $n\mathbb{Z}$. The image is $\mathbb{Z}/n$ (why?).

(4) The kernel of the map $exp : \mathbb{C} \to \mathbb{C}^\times$ defined by $z \mapsto e^{2\pi i z}$ is the subgroup $\mathbb{Z}$. The image is all of $\mathbb{C}^\times$.

(5) Let G be an abelian group and $n \in \mathbb{Z}$. Consider the map $\phi : G \to G$ defined by $\phi(g) = g^n$. Since G is abelian, ϕ is a homomorphism. The kernel of ϕ is

$$\{g \in G : g^n = e\}.$$

Recall that in Problem 1(b) of Assignment 2 you showed by verifying the subgroup axioms that this subset is a subgroup of G. The same conclusion follows from that it is the kernel of a homomorphism. The image of ϕ is the subset

$$\{g^n : g \in G\}$$

of G. In particular, $\{g^n : g \in G\}$ is a subgroup of G.

Let us specialize Example (5) to some familar groups.

(5) (i) Let $n \geq 0$. Consider the map $\mathbb{C}^\times \to \mathbb{C}^\times$ which sends $z \mapsto z^n$. For $n \geq 1$, its kernel is μ_n and its image is all of $\mathbb{C}^\times$ (why?). If $n = 0$, the kernel is all of $\mathbb{C}^\times$ and the image is the trivial subgroup $\{1\}$.

(5) (ii) Let $n \neq 0$. Consider the map $\mathbb{R}^\times \to \mathbb{R}^\times$ defined by $x \mapsto x^n$. If n is even (resp. odd), its kernel is $\{1, -1\}$ (resp. $\{1\}$) and its image is $\mathbb{R}_{>0}$ (resp. $\mathbb{R}^\times$).

(5) (iii) Consider the map $\mathbb{Z} \to \mathbb{Z}$ defined by $a \mapsto na$. The image of this map is the subgroup $n\mathbb{Z}$. Its kernel is $\{0\}$ if $n \neq 0$ and is $\mathbb{Z}$ if $n = 0$.

(5) (iv) Let n be a nonzero integer. Consider the map $\mathbb{Q} \to \mathbb{Q}$ defined by $a \mapsto na$. Its kernel is $\{0\}$ and its image is $\mathbb{Q}$.

(5) (v) Let p be an odd prime number. Consider the map $\phi : U(p) \to U(p)$ given by $[x] \mapsto [x]^2$ (x an integer). Let us find the kernel of ϕ. We have $\phi([x]) = [1]$ if and only if $[x]^2 = [1]$ if and only if $[x^2] = [1]$. The last is equivelent to

$$x^2 \equiv 1 \pmod{p}.$$

(Make sure you are okay with the last sentence.) Since p is prime, $p \mid x^2 - 1 = (x-1)(x+1)$ if and only if $x \equiv \pm 1 \pmod{p}$. It follows that $[x] \in \ker(\phi)$ if and only if $[x] = [\pm 1]$. Since p is ≥ 3, $[1] \neq [-1]$, and $\ker(\phi) = \{[1], [-1]\}$ has order 2.

(5) (vi) Let $\phi : \mathbb{Z}/21 \to \mathbb{Z}/21$ be the map defined by $\phi([a]) = 10[a]$. We claim that $\ker(\phi)$ is trivial (i.e. is the trivial subgroup $\{[0]\}$). Indeed, suppose $[a] \in \ker(\phi)$. Then $10[a] = [0]$, so that (by Proposition 4) $|[a]| \mid 10$. (Note that the operation is $\mathbb{Z}/21$ is addition and $10[a]$ is simply a shortcut notation for $[a] + [a] + \cdots + [a]$ with 10 appearances of $[a]$.) On the other hand, since $\mathbb{Z}/21$ is cyclic, $|[a]| \mid |\mathbb{Z}/21| = 21$. It follows $|[a]| \mid \gcd(21, 10) = 1$. Thus $|[a]| = 1$ and $[a] = [0]$. This proves $\ker(\phi) = \{[0]\}$. Note that alternatively, we can see $\ker(\phi) = \{[0]\}$ as follows: Let $[a] \in \ker(\phi)$. Then $10[a] = [0]$, i.e $[10a] = [0]$. This means $21 \mid 10a$. It follows $21 \mid a$ (as $\gcd(21, 10) = 1$), and hence $[a] = [0]$.

Exercise 28. Find the image of $\phi : U(p) \to U(p)$ defined by $g \mapsto g^2$ for $p = 7$ and $p = 11$.

Homomorphisms are afterall functions, and as such we can speak of whether they are injective, surjective, or bijective (or none).†

PROPOSITION 18. A homomorphism is injective if and only if its kernel is trivial.

PROOF. Let $\phi : G \to H$ be a homomorphism. First assume ϕ is injective. Let $g \in \ker(\phi)$. This means $\phi(g) = e_H$. We know $\phi(e_G) = e_H$ as well. Injectivity of ϕ gives $g = e_G$. It follows $\ker(\phi) = \{e_G\}$.

Conversely, suppose $\ker(\phi) = \{e_G\}$. We show that ϕ is injective. Suppose $\phi(g) = \phi(g')$. Then $\phi(g'^{-1}g) = (\phi(g'))^{-1}\phi(g) = e_H$ (justify the first equality), so that $g'^{-1}g \in \ker(\phi)$. It follows that $g'^{-1}g = e_G$ and hence $g = g'$. □

Exercise 29. Go through the homomorphisms of Examples (1)-(5) above and determine whether they are injective, surjective, or bijective (or none).

Exercise 30. Let $\phi : G \to H$ be a homomorphism. Let G be cyclic with g a generator of G. Show that $\mathrm{Im}(\phi)$ is cyclic and generated by $\phi(g)$.

Exercise 31. Let G be a finite group and $\phi : G \to H$ be a surjective homomorphism. Suppose H has an element of order n. Show that G also has an element of order n.

Exercise 32. Let $\phi : G \to H$ be a homomorphism. Show that $\ker(\phi)$ satisfies the following property: If $g \in \ker(\phi)$ and $x \in G$, then $xgx^{-1} \in \ker(\phi)$. (A subgroup N of G is called *normal* if it satisfies the property that for all $g \in N$ and $x \in G$, $xgx^{-1} \in N$. Thus you prove in this exercise that kernels of homomorphisms are normal.)

9.4. Isomorphisms.

DEFINITION. An isomorphism is a bijective homomorphism.

Examples: (1) For $n \geq 2$ the determinant map $\det : GL_n(\mathbb{Q}) \to \mathbb{Q}^\times$ is not an isomorphism, since it is not injective. The map $\mathbb{Z} \to \mathbb{Z}$ given by $a \mapsto 3a$ is injective, but is not surjective and hence is not an isomorphism.

†Recall that a function $f : X \to Y$ is injective if whenever $f(x) = f(x')$ for $x, x' \in X$, we have $x = x'$. A function $f : X \to Y$ is surjective if $\mathrm{Im}(f) = Y$, or equivalently, if for every $y \in Y$ there is $x \in X$ such that $y = f(x)$. A function is bijective if it is both injective and surjective.

(2) Let n be a nonzero integer. The map $\mathbb{Z} \to n\mathbb{Z}$ given by $a \mapsto na$ is an isomorphism (why?). Note that there is another isomorphism $\mathbb{Z} \to n\mathbb{Z}$ as well, namely defined by $a \mapsto -na$. (For instance, multiplication by 2 and by -2 define two isomorphisms $\mathbb{Z} \to 2\mathbb{Z}$.)

(3) Consider $\mathbb{R}_{>0}$ under multiplication. Define $\phi : \mathbb{R} \to \mathbb{R}_{>0}$ by $\phi(x) = e^x$. The familiar identity $e^{x+y} = e^x e^y$ tells us ϕ is a homomorphism. Note that ϕ has an inverse function, namely $\psi : \mathbb{R}_{>0} \to \mathbb{R}$ defined by $\psi(x) = \log x$. Thus ϕ is bijective, and hence an isomorphism. Note that ψ is also a homomorphism (see Example (8) of Paragraph 9.1). It is of course bijective too (its inverse is ϕ). It follows that ψ is also an isomorphism. (See the next proposition.)

(4) Consider the map $\phi : \mathbb{Z}/21 \to \mathbb{Z}/21$ defined by $\phi([a]) = 10[a]$. We saw in Example (4) (vi) of Paragraph 9.3 that $\ker(\phi) = \{[0]\}$. It follows that ϕ is injective. Note that since the domain and codomain of ϕ both have 21 elements, it follows that ϕ is also surjective. Thus ϕ is an isomorphism.

(5) Let G be any group. The identity map $G \to G$ (defined by $g \mapsto g$) is an isomorphism.

PROPOSITION 19. (a) Let $\phi : G \to H$ be an isomorphism. Then the inverse function $\phi^{-1} : H \to G$ (which exists since ϕ is bijective) is also an isomorphism.
(b) Composition of two isomorphisms is an isomorphism.

PROOF. (a) Being the inverse of a bijective function, ϕ^{-1} is of course bijective. We need to show that ϕ^{-1} is a homomorphism. We must show that

$$\phi^{-1}(hh') = \phi^{-1}(h)\phi^{-1}(h')$$

for all $h, h' \in H$. Since ϕ is injective, it suffices to show that the images of both sides under ϕ coincide, i.e. that

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

The left hand side is hh'. Since ϕ is a homomorphism, the right hand side is

$$\phi(\phi^{-1}(h)) \cdot \phi(\phi^{-1}(h')) = hh'$$

as well.

(b) This is immediate from the fact that composition of bijections (resp. homomorphisms) is a bijection (resp. a homomorphism). □

Exercise 33. Let G and H be groups. Show that there is an isomorphism $G \to H$ if and only if there is an isomorphism $H \to G$.

DEFINITION. Given groups G and H, we say G is isomorphic to H and write $G \simeq H$ if there is an isomorphism $G \to H$.

Thus for instance, by Examples (2), (3), and (5), $\mathbb{Z} \simeq n\mathbb{Z}$ for every nonzero integer n, $\mathbb{R} \simeq \mathbb{R}_{>0}$ (the latter under multiplication), and $G \simeq G$ for any group G.

Exercise 34. Show that being isomorphic is an equivalence relation. (Use Proposition 19 and the previous exercise.)

Note that if $G \simeq H$, then in particular there is a bijection $G \to H$, so that G and H have the same cardinality. Thus for instance, two finite groups of different orders cannot be isomorphic. A finite group cannot be isomorphic to an infinite group, and $\mathbb{Q}$ is not isomorphic to $\mathbb{R}$ (why?).

The moral of the following two results is that not only isomorphic groups have the same cardinality, they also have the same "group theoretic" properties. Moreover, an isomorphism $\phi : G \to H$ between two isomorphic groups provides a "bridge" or "dictionary" between them. (Read the statements of the results to get a sense of what we mean here.)

PROPOSITION 20. Let G and H be isomorphic groups. Then:
(a) G is abelian if and only if H is abelian.
(b) G is cyclic if and only if H is cyclic.

We'll leave the proof of this for the assignment.

PROPOSITION 21. Let $\phi : G \to H$ be an isomorphism. Then:
(a) For every $g \in G$, $|g| = |\phi(g)|$.
(b) For every n, ϕ maps bijectively the elements of G of order n to the elements of H of order n. (In particular, ϕ gives a bijection between elements of G of finite order and elements of H of finite order.)
(c) There is a bijection

$$\text{subgroups of } G \longrightarrow \text{subgroups of } H \qquad K \mapsto \phi(K). \tag{12}$$

PROOF. (a) It is enough to show that for every integer n, $g^n = e$ if and only if $\phi(g)^n = e$ (the identities being in the respective groups). Suppose $g^n = e$. Then $\phi(g)^n = \phi(g^n) = \phi(e) = e$. Conversely, suppose $\phi(g)^n = e$. Then $\phi(g^n) = e$. By injectivity of ϕ, $g^n = e$.

(b) By (a), ϕ indeed maps the elements of G of order n to the elements of H of order n, so that we have a function

(13) the set of elements of G of order $n \longrightarrow$ the set of elements of H of order n

given by $g \mapsto \phi(g)$.[†] The assertion is that this function, which we tentatively call F, is bijective. (Note that F is simply ϕ, except that we are taking the domain and codomain smaller.) Injectivity of F is immediate from that of ϕ. As for surjectivity of F, note that given $h \in H$ of order n, applying Part (a) to $g = \phi^{-1}(h)$ we see $|\phi^{-1}(h)| = |h| = n$. Moreover $F(\phi^{-1}(h)) = \phi(\phi^{-1}(h)) = h$.

(c) By Part (c) of Proposition 17, we do indeed have a function as in (12). To show that this function is bijective, we show that it has an inverse. Note that since $\phi^{-1} : H \to G$ is also a homomorphism, we also have a function

(14) subgroups of $H \longrightarrow$ subgroups of G $\qquad K \mapsto \phi^{-1}(K)$.

The function given in (14) is easily seen to be the inverse of the function given in (13). □

Example: (6) We claim that no two of $\mathbb{Q}^\times$, $\mathbb{R}$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, $U(8)$, $U(5)$, D_8, S_3, and $\mathbb{Z}/6$ are isomorphic to each other. Indeed, $\mathbb{Q}^\times$ is (infinite and) countable, whereas the other groups are either uncountable or finite. Thus $\mathbb{Q}^\times$ is not isomorphic to any of the other groups on the list. Similarly, D_8 is the only group on the list which has order 16, thus it is not isomorphic to any of the other groups. In fact, comparing cardinalities we see that that it is enough to show that

(i) $U(8)$, $U(5)$ (both of order 4) are not isomorphic,

(ii) S_3 and $\mathbb{Z}/6$ (both of order 6) are not isomorphic, and

(iii) no two of $\mathbb{R}$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ (which are all uncountable) are isomorphic.

For (i), note that $U(5)$ is cyclic whereas $U(8)$ is not (it has two elements of order 2, namely $[3]$ and $[5]$). For (ii), note that S_3 is not abelian whereas $\mathbb{Z}/6$ is. All the groups in (iii) are abelian and

[†] One says ϕ restricts to a function

the set of elements of G of order $n \longrightarrow$ the set of elements of H of order n.

none is cyclic (as cyclic groups are either finite or countable), so Proposition 20 does not resolve the problem here. Let us think about the order of elements of these groups. The group $\mathbb{R}$ has no element of finite order besides 0 (=identity), $\mathbb{R}^\times$ has two elements of finite order (namely ± 1), and $\mathbb{C}^\times$ infinitely many such elements (all the roots of unity). The desired conclusion follows.

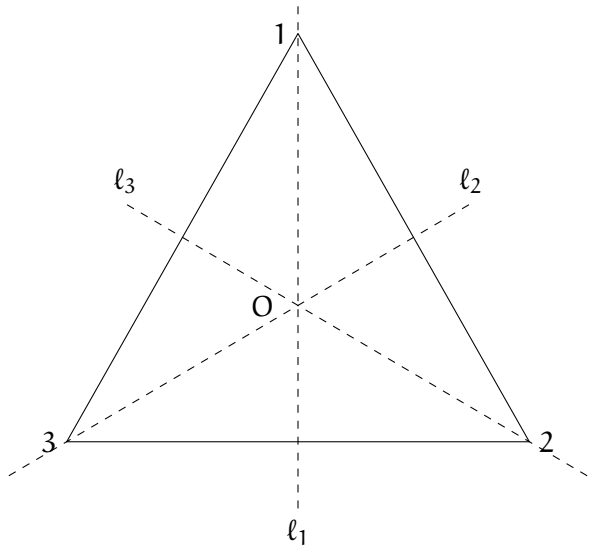
Exercise 35. Let G and H be isomorphic groups. Show that their centers are isomorphic to each other. (See Assignment 2 to recall the definition of the center of a group.)

9.5. Comparing D_3 and S_3. For $n > 3$, the two groups D_n and S_n have different orders (Do you agree?), and hence of course are not isomorphic. The two groups D_3 and S_3 however are both non-abelian and of order 6. We'll see in this paragraph that D_3 and S_3 are indeed isomorphic.

Let $n \geq 3$. Label the vertices of our regular n-gon by the numbers $1, 2, \ldots, n$ (anyhow you like). Every symmetry of a regular n-gon permutes the vertices, and hence via our labeling gives us an element of S_n. Thus we obtain a map $\phi : D_n \to S_n$: For every $f \in D_n$, $\phi(f) \in S_n$ records the data of how f permutes the vertices of the polygon. The map ϕ is a homomorphism. Moreover, since the only symmetry that fixes all the vertices is the identity symmetry, ϕ has trivial kernel and is injective. If $n = 3$, since $|D_3| = |S_3| = 6$, any injective function $D_3 \to S_3$ is also surjective. In particular, ϕ is bijective, and hence an isomorphism. We record the result as a proposition.

PROPOSITION 22. $D_3 \simeq S_3$

Note that to define ϕ above we had to choose a labeling of the vertices. Different labelings will result in different isomorphisms $D_3 \to S_3$ (and injective homomorphisms $D_n \to S_n$ in general). Below we give one isomorphism $\phi : D_3 \to S_3$ corresponding to a particular labeling of the vertices. Here r_i is reflection about ℓ_i , and ρ_1 (resp. ρ_2) is counterclockwise rotation by $2\pi/3$ (resp. $4\pi/3$).



$$\phi : e \mapsto e, \quad r_1 \mapsto (23), \quad r_2 \mapsto (12), \quad r_3 \mapsto (13), \quad \rho_1 \mapsto (132), \quad \rho_2 \mapsto (123)$$

9.6. Classification of cyclic groups. In general, groups (or even abelian groups) of the same order may not be isomorphic; for instance, the groups μ_{24}, $U(45)$, S_4, and D_{12} all have order 24, but are mutually non-isomorphic. There is however a class of groups that, up to isomorphism, are determined by their order:

PROPOSITION 23 (Classification of cyclic groups up to isomorphism). Suppose G and H are cyclic groups of equal order (finite or infinite). Then $G \simeq H$. In particular, every infinite cyclic group is isomorphic to $\mathbb{Z}$, and every cyclic group of order n is isomorphic to $\mathbb{Z}/n$.

PROOF. Infinite case: Suppose G and H have infinite orders. Let g (resp. h) be a generator of G (resp. H). Then $G = \{g^a : a \in \mathbb{Z}\}$, with the g^a all distinct since g has infinite order. Define a function $\phi : G \to H$ by $\phi(g^a) = h^a$. One easily checks that ϕ is a homomorphism:

$$\phi(g^a g^b) = \phi(g^{a+b}) = h^{a+b} = h^a h^b = \phi(g^a)\phi(g^b). \tag{15}$$

We have $\mathrm{Im}(\phi) = \langle \phi(g) \rangle = H$, hence ϕ is surjective. Moreover, since the h^n are all distinct, ϕ is injective. Thus ϕ is an isomorphism.

Finite case: Suppose $|G| = |H| = n$. Choose generators g of G and h of H. We claim that

$$\phi : G \to H \qquad \phi(g^a) = h^a$$

gives an isomorphism between G and H. Here are the things we need to check:

(i) ϕ is well-defined. (Note that given $g' \in G$, there is more than one (in fact infinitely many) a such that $g' = g^a$, and formula for $\phi(g')$ appears to depend on the choice of one such a.)

(ii) ϕ is a homomorphism.

(iii) ϕ is bijective.

To show ϕ is well-defined, we need to check that if $g^a = g^b$, then $h^a = h^b$ as well. Suppose $g^a = g^b$. Then $g^{a-b} = e$, i.e. $n = |g| \mid a - b$. Since $|h| = n$ as well, we have $h^{a-b} = e$, thus $h^a = h^b$, as desired. Now that we know ϕ is well-defined, checking that it is a homomorphism is an identical computation to Eq. (15). As for bijectivity, since $|G| = |H| < \infty$, it is enough to verify one of injectivity or surjectivity; the other will follow. Since G is generated by g, $\mathrm{Im}(\phi) = \langle \phi(g) \rangle = \langle h \rangle = H$, hence ϕ is surjective. □

Example: Consider the groups $\mathbb{Z}/n$ and μ_n. They are both cyclic of order n. To define an explicit isomorphism $\mathbb{Z}/n \to \mu_n$, following the proof of the proposition, we choose a generator for each of $\mathbb{Z}/n$ and μ_n. Say we choose $[1]$ as our generator of $\mathbb{Z}/n$ and $e^{2\pi i/n}$ as our generator of μ_n. Now

$$\phi : \mathbb{Z}/n \to \mu_n \qquad [a] \mapsto e^{2\pi i a/n}$$

is an isomorphism.

Exercise 36. Define three isomorphisms $\mathbb{Z}/8 \to \mu_8$.

Exercise 37. Let G and H be cyclic of order n. Show that there are $\varphi(n)$ isomorphisms $G \to H$. (Here φ is the Euler function.)

10. Cosets and Lagrange's theorem

10.1. Cosets. Throughout the following discussion, G is any group and H is a subgroup of G. Denote the operation in G by $\cdot$. For each element $g \in G$, define

$$g \cdot H := \{g \cdot h : h \in H\}.$$

The sets $g \cdot H$ are called the *left cosets* of H (in G). As usual, when it won't lead to confusion we drop the operation symbol and write gH for $g \cdot H$. Note that $eH = H$, so that H itself is a left coset of H.

PROPOSITION 24. (a) Distinct left cosets of H are disjoint[†] and form a partition of G.
(b) For any $g, g' \in G$, $g' \in gH$ if and only if $g^{-1}g' \in H$ if and only if $g'H = gH$.

PROOF. Define a relation $\sim$ on G by

$$g \sim g' \text{ if and only if } g^{-1}g' \in H. \tag{16}$$

This is an equivalence relation. Indeed, for every g, $g^{-1}g = e \in H$ so that $g \sim g$. If $g \sim g'$, by definition we have $g^{-1}g' \in H$, so that since H is a subgroup $g'^{-1}g = (g^{-1}g')^{-1} \in H$ as well; it follows that $g' \sim g$ and $\sim$ is symmetric. Finally, if $g \sim g'$ and $g' \sim g''$, we have $g^{-1}g',\ g'^{-1}g'' \in H$, and hence $g^{-1}g'' = (g^{-1}g')(g'^{-1}g'') \in H$. It follows $g \sim g''$ and $\sim$ is transitive. For each $g \in G$, the equivalence class of g (with respect to the relation Eq. (16)) is exactly the left coset gH:

$$\begin{aligned}
[g] &= \{g' \in G : g^{-1}g' \in H\} \\
&= \{g' \in G : g^{-1}g' = h \text{ for some } h \in H\} \\
&= \{g' \in G : g' = gh \text{ for some } h \in H\} \\
&= gH.
\end{aligned}$$

Both parts follow. (See Lemma 1 and Theorem 1.) □

Examples: (1) The left cosets of $H = \langle (12) \rangle$ in S_3 are

$$eH = \{e, (12)\} = (12)H,$$

[†]In other words, for any $g, g' \in G$, either $gH = g'H$ or $gH \cap g'H = \emptyset$.

$$(13)H = \{(13), (13)(12)\} = \{(13), (123)\} = (123)H,$$

and

$$(23)H = \{(23), (23)(12)\} = \{(23), (132)\} = (132)H.$$

(2) The left cosets of $H = \langle(123)\rangle$ in S_3 are

$$eH = H = \{e, (123), (132)\} = (123)H = (132)H$$

and

$$(12)H = \{(12), (12)(123), (12)(132)\} = \{(12), (23), (13)\} = (23)H = (13)H.$$

(3) Take $G = \mathbb{Z}$. Let us find the left cosets of the subgroup $\langle 3\rangle = 3\mathbb{Z}$ of all multiples of 3. The left coset containing the integer a is

$$a + 3\mathbb{Z} = \{a + 3k : k \in \mathbb{Z}\},$$

i.e. the residue class of a mod 3. In other words, the left cosets of $3\mathbb{Z}$ are exactly the residue classes mod 3. Similarly, for every integer $n \geq 1$, the left cosets of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ are exactly the residue classes mod n:

$$a + n\mathbb{Z} = \{a + nk : k \in \mathbb{Z}\} = \text{the residue class of } a \text{ mod } n.$$

In the examples above, note that each left coset of H has as many elements as H. This is in general true:

PROPOSITION 25. Every left coset of H has the same cardinality as H.

PROOF. The function $H \to gH$ which sends $h \mapsto gh$ is a bijection (why?). □

So far we have talked about left cosets. Of course, one similarly has a notion of *right cosets*: For each $g \in G$, we define $H \cdot g$ as

$$H \cdot g := \{h \cdot g : h \in H\}.$$

The set $H \cdot g$ is called a right coset of H. Again for simplicity we drop the operation symbol and simply write Hg if it won't lead to confusion. Note that $He = H$, so that H itself is a right coset of H. We leave the analogs of Propositions 24 and 25 as exercises.

Exercise 38. (a) Show that distinct right cosets of H are disjoint and form a partition of G. (b) Show that for every $g, g' \in G$, $g' \in Hg$ if and only if $g'g^{-1} \in H$ if and only if $Hg = Hg'$. (Suggestion for both parts: Define a relation on G by $g \sim g'$ if and only if $g'g^{-1} \in H$.)

Exercise 39. Show that every right coset of H has the same cardinality as H.

Examples: (4) The right cosets of $H = \langle (12) \rangle$ in S_3 are

$$He = H = \{e, (12)\} = H(12),$$

$$H(13) = \{(13), (12)(13)\} = \{(13), (132)\} = H(132),$$

and

$$H(23) = \{(23), (12)(23)\} = \{(23), (123)\} = H(123).$$

Comparing with Example (1), we observe that the left and right cosets of $\langle (12) \rangle$ are not the same.

(5) The left cosets of $H = \langle (123) \rangle$ in S_3 are

$$He = H = \{e, (123), (132)\} = H(123) = H(132)$$

and

$$H(12) = \{(12), (123)(12), (132)(12)\} = \{(12), (13), (23)\} = H(13) = H(23).$$

Comparing with Example (5), we see that the left and right cosets of $H = \langle (123) \rangle$ are actually the same.

(6) If G is abelian, then it is clear from the definitions that $gH = Hg$, i.e. left and right cosets of H coinside.

Exercise 40. Let $H \leq G$. Show that $gH = Hg$ for all $g \in G$ if and only if H is a normal subgroup of G. (See Problem 6 of Assignment 5 (Exercise 32 here) to recall the definition of normality.)

10.2. Index of a subgroup. Let $H \leq G$. The number of left cosets of H in G (finite or infinite) is called the *index* of H in G, and is denoted by $[G : H]$. Thus for instance, the subgroups $\langle (12) \rangle$

and $\langle(123)\rangle$ of S_3 have respectively indices 3 and 2. For $n \geq 1$, the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ has index n (why?).

The following exercise tells us we can equivalently define the index as the number of right cosets.

Exercise 41. Show that $gH \mapsto Hg^{-1}$ gives a bijection between the collection of left cosets of H and the collection of right cosets of H.[†]

Exercise 42. Let H be a subgroup of G of index 2 (i.e. $[G : H] = 2$). Show that H is a normal subgroup of G.

10.3. A useful formula and Lagrange's theorem. Now suppose G is a finite group and as before, H is a subgroup of G. Then, of course, H and $[G : H]$ will be finite as well.

PROPOSITION 26. Let H be a subgroup of a finite group G. Then

$$|G| = [G : H] \cdot |H|. \tag{17}$$

PROOF. The distinct left cosets of H partition G. Moreover, each left coset has $|H|$ elements. The formula follows. □

The following result is known as Lagrange's theorem. It is immediate from the formula (17).

THEOREM 3 (Lagrange's theorem). Let H be a subgroup of a finite group G. Then $|H| \,\big|\, |G|$.

Example: As an example of how Lagrange's theorem can be sometimes used in applications, we show that the only subgroup of A_4 that contains all the 3-cycles is A_4 itself. The number of 3-cycles in A_4 is $\binom{4}{3} \cdot 2! = 8$ (why?). Let H be a subgroup of A_4 that contains all the 3-cycles. Then H has at least 8 (actually 9, since $e \in H$ too) elements. We also know $|H| \,\big|\, |A_4| = 12$ by Lagrange's theorem. Putting these together we get $|H| = 12$ and $H = A_4$.

Exercise 43. Show that the only subgroup of D_n that contains all the reflections is D_n.

Exercise 44. Show that the only subgroup of A_5 that contains all the 3-cycles is A_5.

Exercise 45. Let G be a finite group, and $K \leq H \leq G$. Show that $[G : K] = [G : H] \cdot [H : K]$.

[†]What goes wrong if instead we do the naive thing and try to define a bijection by $gH \mapsto Hg$?

10.4. Some corollaries of Lagrange's theorem. In this paragraph, we give some interesting consequences of Lagrange's theorem.

COROLLARY 2. Let G be a finite group. For every $g \in G$, $|g| \mid |G|$ (or equivalently $g^{|G|} = e$).

PROOF. Let $g \in G$. Applying the previous result to the subgroup $H = \langle g \rangle$ of G we obtain $|g| = |H| \mid |G|$. □

Specializing to $G = U(n)$ we recover a classical result of Euler and Fermat, namely that

COROLLARY 3. If $\gcd(a, n) = 1$, $a^{\phi(n)} \equiv 1 \pmod{n}$. In particular, if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.[†]

PROOF. Take $G = U(n)$ and $g = [a]$ in the previous corollary. We get $[a]^{\phi(n)} = [1]$, which is exactly to say $a^{\phi(n)} \equiv 1 \pmod{n}$. We get the second assertion if we take $n = p$ prime. □

COROLLARY 4. Every group of prime order is cyclic.

PROOF. Let G be a group of order p, where p is a prime number. Pick any element $g \in G$ that is not the identity. Consider $\langle g \rangle$. By Lagrange's theorem, $|\langle g \rangle|$ divides p. Since p is prime, it follows $|\langle g \rangle|$ is either 1 or p. The former is not the case as $\langle g \rangle$ contains g and e (and $g \neq e$). Thus $|\langle g \rangle| = p$ and $\langle g \rangle = G$. □

Exercise 46. Let $a \geq 2$ and $n \geq 1$. Show that $n \mid \varphi(a^n - 1)$. (Hint: Consider $[a]$ in $U(a^n - 1)$.)

Exercise 47. Let G and H be finite groups and $\gcd(|G|, |H|) = 1$. Show that the only homomorphism $G \to H$ is the trivial homomorphism. (In other words, show that if $\phi : G \to H$ is a homomorphism, then $\phi(g) = e$ for every $g \in G$.)

11. Quotient groups

11.1. The quotient of a group by a normal subgroup. Let G be a group and H be a subgroup of G. We denote the set of all left cosets of H in G by G/H:

$$G/H := \{gH : g \in G\}.$$

[†]The statement about general n is usually referred to as Euler's theorem. The special case for primes is usually referred to Fermat's theorem.

Note that G/H has $[G : H]$ elements.

Roughly speaking, we would like to know if the group structure on G can be used to define a group structure on G/H. Note that if we want to use the binary operation in G to define a binary operation $\cdot$ on G/H, the natural candidate would be to try to define the operation on G/H as follows: Given left cosets C, C' of H, *choose* $g, g' \in G$ such that $C = gH$ [†] and $C' = g'H$, and then set

$$C \cdot C' = (gg')H.$$

In other words, for every $g, g' \in G$, we would like to set

$$gH \cdot g'H = (gg')H \tag{18}$$

Since our "definition" of the operation on G/H involves choosing representatives for cosets, one has to address well-definedness:

Example: Take $G = S_3$ and $H = \langle (12) \rangle$. One easily checks that the left cosets are H, $\{(13), (123)\}$, and $\{(23), (132)\}$, so that

$$G/H = \left\{ H, \{(13), (123)\}, \{(23), (132)\} \right\}.$$

Let us try to calculate

$$\{(13), (123)\} \cdot \{(23), (132)\} \tag{19}$$

following the formula (18). On the one hand, we can write the two cosets in the product as $(13)H$ and $(23)H$, so that the formula gives

$$\{(13), (123)\} \cdot \{(23), (132)\} = (13)H \cdot (23)H = ((13)(23))H = (132)H.$$

On the other, we can express the two cosets in the product (19) as $(123)H$ and $(132)H$, so that we should have

$$\{(13), (123)\} \cdot \{(23), (132)\} = (123)H \cdot (132)H = ((123)(132))H = eH = H.$$

[†]Note that $gH = C$ if and only if $g \in C$. In accordance with the terminology for equivalence classes, any element $g \in G$ such that $gH = C$ (i.e. any element of C) is called a *representative* of C.

Thus depending on the choice of representatives for the cosets $C = \{(13), (123)\}$ and $C' = \{(23), (132)\}$, our formula gives different values for $C \cdot C'$, and hence it is not well-defined. (In more blunt terms, it does not make sense.)

Now we can precisely formulate the problem we would like to address:

1. When does Eq. (18) give a well-defined binary operation on G/H?
2. Assuming well-definedness, does G/H form a group under the operation Eq. (18)?

The next two propositions address these questions. Recall that the subgroup H of G is called a normal subgroup (of G) if for every $g \in G$ and $h \in H$, we have $ghg^{-1} \in H$. We write $H \trianglelefteq G$ to signify that H is a normal subgroup of G.

PROPOSITION 27. The formula

$$gH \cdot g'H = (gg')H \qquad \text{for every } g, g' \in G \tag{20}$$

defines a (well-defined) binary operation on G/H if and only if $H \trianglelefteq G$.

PROOF. Suppose $\cdot$ given by Eq. (20) is well-defined. Let $g \in G$ and $h \in H$. On the one hand we have

$$gH \cdot g^{-1}H = (gg^{-1})H = eH = H.$$

On the other hand, since $g^{-1}(gh) \in H$, we have $gH = (gh)H$, and hence

$$gH \cdot g^{-1}H = (gh)H \cdot g^{-1}H = (ghg^{-1})H.$$

Thus $(ghg^{-1})H = H$, and hence $ghg^{-1} \in H$. Thus $H \trianglelefteq G$.

Conversely, suppose H is normal in G. We show that the operation given in Eq. (20) is well-defined. Indeed, let $gH = g_1H$ and $g'H = g_1'H$. We need to show that $(gg')H = (g_1g_1')H$. Set $h = g^{-1}g_1$ and $h' = g'^{-1}g_1'$. Note that $h, h' \in H$ (why?). Then we have

$$(gg')^{-1}(g_1g_1') = g'^{-1}g^{-1}g_1g_1' = g'^{-1}hg_1' = g'^{-1}h(g'h') = (g'^{-1}hg')h' \in H,$$

as by normality of H, $g'^{-1}hg' \in H$. It follows that $(gg')H = (g_1g_1')H$. □

PROPOSITION 28. Let $H \trianglelefteq G$. The operation defined in Eq. (20) makes G/H (the set of left=right cosets of H, see Exercise 40) a group. The identity of this group is the coset H and the inverse of

gH is $g^{-1}H$. Moreover, the map

$$\pi : G \to G/H \qquad \pi(g) = gH$$

is a surjective homomorphism with kernel H.

PROOF. Let us verify that the operation on G/H is associative. We have

$$(gH \cdot g'H) \cdot g''H = (gg')H \cdot g''H = ((gg')g'')H = (g(g'g''))H = gH \cdot (g'g'')H = gH \cdot (g'H \cdot g''H).$$

(Note that the third equality is by associativity in G, and the other equalities are by definition of the operation in G/H.) For every $gH \in G/H$,

$$gH \cdot eH = (ge)H = gH = (eg)H = eH \cdot gH,$$

so that $eH = H$ indeed satisfies the defining property of the identity in G/H. Given $gH \in G/H$, we have

$$gH \cdot g^{-1}H = (gg^{-1})H = eH = (g^{-1}g)H = g^{-1}H \cdot gH,$$

so that gH has an inverse. Thus G/H is a group under (20). Note that in the process we also verified the assertions about the idenity and the inverse of gH.

That π is a homomorphism is essentially gauranteed by the definition of the binary operation in G/H. Indeed,

$$\pi(g)\pi(g') = gH \cdot g'H = (gg')H = \pi(gg').$$

Given any coset of H, we can express it as gH for some g, and then $\pi(g) = gH$; this proves surjectivity of π. Finally, let us calculate the kernel of π. On recalling that the identity of G/H is H, we have

$$g \in \ker(\pi) \quad \Leftrightarrow \quad \pi(g) = e_{G/H} \quad \Leftrightarrow \quad gH = H \quad \Leftrightarrow \quad g \in H.$$

Thus $\ker(\pi) = H$ as desired. □

Terminology: Let H be a normal subgroup G. Then as we just saw, G/H is group under the operation given in Eq. (20). We call this group the *quotient* of G by H. The map π of Proposition 28 is called the quotient map (or sometimes the natural map).

Before we look at some examples, note that if G is abelian, then for every subgroup $H \leq G$, G/H is group (as the normality condition is gauranteed). Note that in view of Problem 3 of Assignment 6, the quotient G/H is then in fact also abelian.

Examples: (1) Consider the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$. The quotient group $\mathbb{Z}/n\mathbb{Z}$ is exactly what we earlier denoted by $\mathbb{Z}/n$, i.e. the group of residue classes mod n under addition. The quotient map

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \qquad a \mapsto a + n\mathbb{Z}$$

is the reduction mod n map.

(2) Let G be any group. The $G \trianglelefteq G$ and $\{e\} \trianglelefteq G$. The quotient G/G is trivial (i.e. a group with one element only) and $G/\{e\} \simeq G$ (why?).

(3) Consider the quotient $\mathbb{R}^\times/\mathbb{Q}^\times$. This is an infinite (in fact uncountable) group (why?). Let us find the order of the element $\sqrt{3}\mathbb{Q}^\times$ of it. Since $\sqrt{3} \notin \mathbb{Q}^\times$, $\sqrt{3}\mathbb{Q}^\times \neq \mathbb{Q}^\times$ (=the identity of $\mathbb{R}^\times/\mathbb{Q}^\times$). We have

$$(\sqrt{3}\mathbb{Q}^\times)^2 = \sqrt{3}\mathbb{Q}^\times \cdot \sqrt{3}\mathbb{Q}^\times = (\sqrt{3}\sqrt{3})\mathbb{Q}^\times = 3\mathbb{Q}^\times = \mathbb{Q}^\times.$$

Thus $|\sqrt{3}\mathbb{Q}^\times| = 2$.

(4) Consider the group $\mathbb{R}/\mathbb{Z}$. We claim that the element $\frac{1}{2} + \mathbb{Z}$ of $\mathbb{R}/\mathbb{Z}$ has order 2. Indeed, $\frac{1}{2} + \mathbb{Z} \neq \mathbb{Z}$ (=the identity of $\mathbb{R}/\mathbb{Z}$), but

$$(\frac{1}{2} + \mathbb{Z}) + (\frac{1}{2} + \mathbb{Z}) = (\frac{1}{2} + \frac{1}{2}) + \mathbb{Z} = \mathbb{Z}.$$

(5) We claim that every element of the group $\mathbb{Q}/\mathbb{Z}$ has finite order. Indeed, any element of $\mathbb{Q}/\mathbb{Z}$ can be expressed as $\frac{m}{n} + \mathbb{Z}$, where $m, n \in \mathbb{Z}$ and $n > 0$. Then in view of Exercise 48(a) below we have

$$n(\frac{m}{n} + \mathbb{Z}) = n\frac{m}{n} + \mathbb{Z} = m + \mathbb{Z} = \mathbb{Z}.$$

Exercise 48. (a) Let $H \trianglelefteq G$ and $g \in G$. Show that $(gH)^n = g^nH$ (in G/H).

(b) Show that $gH \in G/H$ has finite order if and only if $g^n \in H$ for some $n \geq 1$.

Exercise 49. Suppose $H \trianglelefteq G$ and $H \leq K \leq G$. Show that $H \trianglelefteq K$ and that $K/H \leq G/H$.

Exercise 50. Show that an element $x + \mathbb{Z}$ of $\mathbb{R}/\mathbb{Z}$ has finite order if and only if $x \in \mathbb{Q}$. (In other words, show that

$$\mathbb{Q}/\mathbb{Z} = \text{the subgroup of } \mathbb{R}/\mathbb{Z} \text{ consisting of all the elements of finite order.})$$

11.2. Applications of quotients. In this paragraph we give some applications of quotients. As the first application, we shall prove that

PROPOSITION 29. A_4 does not have a subgroup of index 2.

Before we prove this, note that this result in particular tells us that in general, given a group G of order n and a divisor d of n, G may not have a subgroup of order d (as the proposition says A_4 does not have a subgroup of order $\frac{12}{2} = 6$).

PROOF OF PROPOSITION 29. Let $H \leq A_4$ be a subgroup of index 2 (i.e. of order 6). We shall show that H must contain all the 3-cycles. Note that this will give us a contradiction, since the number of 3-cycles in A_4 is 8.

By Exercise 42, $H \trianglelefteq A_4$. The quotient A_4/H is a group of order 2. Let $\pi : A_4 \to A_4/H$ be the quotient map. Let $\sigma \in A_4$ be a 3-cycle. Then $|\sigma| = 3$, so that $|\pi(\sigma)| \mid 3$ (why?). But on the other hand, $|\pi(\sigma)| \mid 2$ (why?). It follows that $|\pi(\sigma)| = 1$, i.e. $\pi(\sigma)$ is the identity of A_4/H. Thus $\sigma \in \ker(\pi) = H$ as claimed. □

Exercise 51. Show that S_n has no normal subgroup of index 3. (Hint: Suppose $H \trianglelefteq S_n$ has index 3. Use the quotient map $\pi : S_n \to S_n/H$ to show that H contains every 2-cycle.)

Our second application of the construction of quotients is a proof of a special case of the so-called Cauchy's theorem. The result, in its full generality, asserts that if G is a finite group, then for every prime divisor p of $|G|$, G has an element of order p.[†] We will prove this result in the case that G is abelian.

THEOREM 4 (Cauchy's theorem for abelian groups). Let p be a prime number. If p divides the order of a finite abelian group G, then G has an element of order p.

PROOF. We prove this by induction on the order of G. Note that if $|G| = p$, then the assertion is certainly true; by Lagrange's theorem, any element other than the idenitity has order p. Now suppose G is a finite abelian group of order $|G|$ divisible by p, and that the assertion is true for all abelian groups of order $< |G|$, i.e. that every finite abelian group K with $p \mid |K| < |G|$ has an element

[†]Thus the result can be thought of as a partial converse to Corollary 2.

of order p. Take an element $g \neq e$ in G. If $p \mid |g|$, then

$$g^{\frac{|g|}{p}}$$

has order p (why?), and so we are done. Now suppose $p \nmid |g|$. Let $H = \langle g \rangle$. Consider the quotient G/H. Since $p \mid |G|$ and $p \nmid |H|$, p divides $|G/H|$ $(= \frac{|G|}{|H|})$. We also have $|G/H| < |G|$ (why?). Thus by our induction hypothesis, G/H has an element of order p. Since there is a surjective homomorphism $G \to G/H$ (e.g. the quotient map), it follows in view of Exercise 31 that G has an element of order p as well. (When did we use the assumption that G is abelian?) □

COROLLARY 5. Let G be an abelian group of order pq, where p and q are distinct primes. Then G is cyclic.

PROOF. By Cauchy's theorem, G has an element of order p and an element of order q. Let $|g| = p$ and $|h| = q$. We claim that the element gh has order pq and hence $G = \langle gh \rangle$ is cyclic. Indeed, by Lagrange's theorem $|gh|$ is one of 1, p, q, and pq. Since an element and its inverse have the same order $g \neq h^{-1}$, i.e. $gh \neq e$. Also, since G is abelian, $(gh)^p = g^p h^p = h^p \neq e$ (why?). Similarly $(gh)^q \neq e$. □

Let q be a prime number > 2. By the previous result, an abelian group of order $2q$ is cyclic. As another application of quotients, we shall prove that every non-abeliam group of order $2q$ is isomorphic to the dihedral group D_q.

PROPOSITION 30. Let G be a non-abelian group of order $2q$, where $q > 2$ is a prime number. Then $G \simeq D_q$.

PROOF. We do this in a few steps. First, we claim that G has an element of order q.[†] Indeed, by Lagrange's theorem and in view of primality of q, every element of G is of order $1, 2, q$ or $2q$. Since G is not abelian, it is of course not cyclic and hence no element has order $2q$. Thus the non-identity elements of G have order 2 or q. By the Exercise 52, at least one element must be of order q.

Let $h \in G$ be an element of order q. Let $H = \langle h \rangle$. We have

$$H = \{e, h, h^2, \ldots, h^{q-1}\},$$

[†]Of course, this is immediate from the general form of Cauchy's theorem, but in the interest of keeping the discussion more self-contained we give another argument.

$|H| = q$, and every non-identity element of H has order q (why?). We claim that every element of $G - H$ has order 2. Indeed, $[G : H] = 2$ (why?) and hence by Exercise 42 H is a normal subgroup of G. Let $\pi : G \to G/H$ be the quotient map. For every element $x \in G - H$, $|\pi(x)| = 2$ (why?) and hence $2 \mid |x|$ (by Exercise 27). On recalling the possible values for $|x|$ it follows $|x| = 2$.

Thus every element of $G - H$ has order 2. Let g be an element of $G - H$. We have

$$G - H \overset{\text{why}}{=} gH = \{ge, gh, \ldots, gh^{q-1}\}.$$

Thus the $2q$ elements of G can be expressed as

$$e, \underbrace{h, h^2, \ldots, h^{q-1}}_{\text{each of order } q}, \overbrace{g, gh, \ldots, gh^{q-1}}^{\text{each of order 2}}.$$

We claim that the entire Cayley table of G (with the elements of G written as above) can be calculated, as follows: Of course, $h^i h^j = h^{i+j}$ and $(gh^i)h^j = gh^{i+j}$. For the other two possible types of products (i.e. those of the form $(gh^i)(gh^j)$ and $h^i(gh^j)$), first note that since $|gh| = 2$, we have $ghgh = e$, so that $ghg = h^{-1}$ $(= h^{q-1})$. Using this we have

$$(gh^i)(gh^j) = (gh^i g)h^j \overset{\text{why}}{=} (ghg)^i h^j = h^{j-i}$$

and

$$h^i(gh^j) = (h^i g)h^j \overset{\text{why}}{=} (gh^{-i})h^j = gh^{j-i}.$$

From this we can conclude that every two non-abelian groups of order $2q$ are isomorphic! Indeed, if G' is another non-abelian group of order $2q$, by the above argument, there will be elements $h', g' \in G'$ with $|h'| = q$ and $|g'| = 2$ such that

$$G' = \{e', h', h'^2, \ldots, h'^{q-1},\ g', g'h', \ldots, g'h'^{q-1}\},$$

and the Cayley table of G' is described by equations identical to those in G, with g' and h' replacing g and h. The map $\phi : G \to G'$ sending every element to its $'$-decorated counterpart is then an isomorphism.

The dihedral group D_q is an non-abelian group of order $2q$. The result follows. □

Exercise 52. Suppose G is a group such that $g^2 = e$ for every $g \in G$. Show that G is abelian.

Exercise 53. List all groups of order 14 up to isomorphism.

Exercise 54. Suppose G is a group and $H \leq G$ is a subgroup of index 2. Let $g, g' \in G - H$. Show that $gg' \in H$.[†]

12. The first isomomorphism theorem

12.1. An example. Consider the homomorphism

$$\phi : \mathbb{C}^\times \to \mathbb{R}^\times \qquad \phi(w) = |w|.$$

Its kernel is the unit circle $S := \{z \in \mathbb{C} : |z| = 1\}$ and its image is $\mathbb{R}_{>0}$. Let us take a moment to describe the cosets of S. Given $w \in \mathbb{C}^\times$, the coset wS is obtained by scaling S by $|w|$ and then rotating the outcome by $\arg(w)$ (the argument of w). It follows that wS is just the circle centred at 0 and passing through w, or in other words, the circle centred at zero with radius $|w|$. Thus in short, the cosets of S are the circles centred at 0. Observe that:

(i) ϕ maps the entirety of each coset of $\ker(\phi)$ to the same element. (Clear from the definition of ϕ and the describtion of the cosets.)

(ii) ϕ maps different cosets of $\ker(\phi)$ to different elements. (Each circle is mapped to its radius.)

(iii) For every $r \in \mathrm{Im}(\phi)$, there is a coset of $\ker(\phi)$ (namely the circle centred at 0 and with radius r) the elements of which are mapped by ϕ to r.

All of this can be summarized by saying that we have a bijection

$$\mathbb{C}^\times/\ker(\phi) \;=\; (\text{the set of cosets of } \ker(\phi) \text{ in } \mathbb{C}^\times) \;\longrightarrow\; \mathrm{Im}(\phi)$$

given by

$$w\ker(\phi) \mapsto \phi(w) \qquad\qquad (\text{i.e. a circle} \mapsto \text{its radius}).$$

(Observation (i) is the well-definedness, (ii) is the injectivity, and (iii) is the surjectivity.)

One can check that the bijection above is also a homomorphism, and hence an isomomorphism.

[†]Solution: Being a subgroup of index 2 H is normal in G (see Exercise 42). The quotient G/H is a group of order 2. Consider the quotient map $\pi : G \to G/H$. Note that since $g, g' \notin H$ and $[G : H] = 2$, $\pi(g) = \pi(g')$ $(= G - H)$. Thus $\pi(gg') = \pi(g)\pi(g') = \pi(g)^2 = e_{G/H} = H$. It follows that $gg' \in \ker(\pi) = H$.

12.2. Statement of the theorem and its proof. What we saw in the previous paragraph is an instance of a very general phanomenon, summerized by the following theorem.

THEOREM 5 (The first isomorphism theorem). Let $\phi : G \to K$ be a homomorphism. There is an isomorphism

$$\overline{\phi} : G/\ker(\phi) \to \mathrm{Im}(\phi)$$

defined by

$$\overline{\phi}(g\ker(\phi)) = \phi(g).$$

Before we talk about the proof, note that the bijectivity statement amounts exactly to the statements (i)-(iii) of the previous paragraph.

PROOF. First note that $\ker(\phi) \trianglelefteq G$ (by Problems 6(a) of Assignment 5), and hence $G/\ker(\phi)$ is a group. There are four things we have to check:

(i) $\overline{\phi}$ is well-defined.

(ii) $\overline{\phi}$ is injective.

(iii) $\overline{\phi}$ is surjective.

(iv) $\overline{\phi}$ is a homomorphism.

For well-definedness, we need to verify that

$$\text{if } g\ker(\phi) = g'\ker(\phi), \text{ then } \phi(g) = \phi(g').$$

(In other words, that ϕ maps the entirety of a coset of $\ker(\phi)$ to the same element.) If $g\ker(\phi) = g'\ker(\phi)$, then $g^{-1}g' \in \ker(\phi)$ and hence $\phi(g)^{-1}\phi(g') = \phi(g^{-1}g') = e$, thus $\phi(g) = \phi(g')$ as desired.

Injectivity amounts to that

$$\text{if } \phi(g) = \phi(g'), \text{ then } g\ker(\phi) = g'\ker(\phi).$$

Suppose $\phi(g) = \phi(g')$. Then $\phi(g^{-1}g') = e$ (why?), i.e. $g^{-1}g' \in \ker(\phi)$. It follows $g\ker(\phi) = g'\ker(\phi)$.

For surjectivity, let $k \in \mathrm{Im}(\phi)$. There is g is G such that $k = \phi(g)$. We then have $\overline{\phi}(g\ker(\phi)) = \phi(g) = k$.

Finally, we check that $\overline{\phi}$ is a homomorphism:

$$\overline{\phi}\left(\, g\ker(\phi)\cdot g'\ker(\phi)\,\right)=\overline{\phi}\left(\,(gg')\ker(\phi)\,\right)=\phi(gg')=\phi(g)\phi(g')=\overline{\phi}\left(\, g\ker(\phi)\,\right)\cdot\overline{\phi}\left(\, g'\ker(\phi)\,\right).$$

□

With notation as in the theorem, the isomorphism $\overline{\phi}$ is said to be *induced* by ϕ.

COROLLARY 6. Let G be a finite group and $\phi : G \to K$ be a homomorphism. Then

$$|G| = |\ker(\phi)| \cdot |\mathrm{Im}(\phi)|.$$

PROOF. We have

$$|G| = |\ker(\phi)| \cdot [G : \ker(\phi)] = |\ker(\phi)| \cdot |G/\ker(\phi)| = |\ker(\phi)| \cdot |\mathrm{Im}(\phi)|,$$

where in the last equality we used the first isomorphism theorem. □

Exercise 55. Suppose G and K are finite groups such that $\gcd(|G|, |K|) = 1$. Show that there is no nontrivial homomorphism $G \to K$. (Hint: Let $\phi : G \to K$ be a homomorphism. Try to show that $|\mathrm{Im}(\phi)| = 1$.)

12.3. Examples. We will give several examples for the first isomorphism theorem and how it can be used.

(1) Consider the map $\phi : \mathbb{C}^\times \to \mathbb{R}^\times$ defined by $\phi(w) = |w|$. The kernel of ϕ is the unit circle $S = \{z \in \mathbb{C} : |z| = 1\}$ and the image of ϕ is the subgroup $\mathbb{R}_{>0}$ of $\mathbb{R}^\times$. By the first isomorphism theorem, we have an isomorphism

$$\overline{\phi} : \mathbb{C}^\times/S \longrightarrow \mathbb{R}_{>}0$$

defined by

$$\overline{\phi}(wS) = |w|.$$

In particular,

$$\mathbb{C}^\times/S \simeq \mathbb{R}_{>0}.$$

(Note that $\overline{\phi}$ simply maps a circle centred ar 0 (=a coset of S) to the radius of the circle.)

(2) Consider the determinant map $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$. Its kernel is (by definition) $SL_n(\mathbb{R})$. Given any $r \in \mathbb{R}^\times$, if we take A to be the $n \times n$ diagonal matrix with (1,1) entry r and all the other diagonal entries 1, then $\det(A) = r$. Thus $\mathrm{Im}(\det) = \mathbb{R}^\times$. By the first isomorphism theorem, we have an isomorphism

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$$

given by

$$A \cdot SL_n(\mathbb{R}) \mapsto \det(A).$$

(3) We will use the first isomorphism theorem to show that

$$\mathbb{R}/\mathbb{Z} \simeq S.$$

(Here S is again the unit circle.) Consider the map $\phi : \mathbb{R} \to \mathbb{C}^\times$ defined by $\phi(x) = e^{2\pi i x}$. Note that ϕ is a homomorphism. We have $\mathrm{Im}(\phi) = S$ and $\ker(\phi) = \mathbb{Z}$. By the first isomorphism theorem we have an isomorphism

$$\overline{\phi} : \mathbb{R}/\mathbb{Z} \longrightarrow S$$

defined by

$$\overline{\phi}(x + \mathbb{Z}) = e^{2\pi i x}.$$

In particular, $\mathbb{R}/\mathbb{Z} \simeq S$.

(4) Consider the homomorphism $\phi : \mathbb{R}^\times \to \mathbb{R}^\times$ given by $\phi(x) = |x|$. Note that $\ker(\phi) = \{1, -1\}$ and $\mathrm{Im}(\phi) = \mathbb{R}_{>0}$. Thus by the first isomorphism ϕ induces an isomorphism

$$\overline{\phi} : \mathbb{R}^\times/\{1, -1\} \longrightarrow \mathbb{R}_{>0}$$

given by

$$\overline{\phi}(\{x, -x\}) = x^2 \ (= (-x)^2).$$

(Note that the cosets of $\{1, -1\}$ are of the form $\{x, -x\}$.) In particular, we see that

$$\mathbb{R}^\times/\{1, -1\} \simeq \mathbb{R}_{>0}.$$

Now let n be a nonzero even integer and define $\psi_n : \mathbb{R}^\times \to \mathbb{R}^\times$ by $\psi_n(x) = x^n$. Then $\ker(\psi_n)$ is also $\{1, -1\}$ (since n is even and nonzero) and $\mathrm{Im}(\psi_n) = \mathbb{R}_{>0}$, so that ψ_n also induces an isomorphism

$$\mathbb{R}^\times/\{1, -1\} \longrightarrow \mathbb{R}_{>0}.$$

This isomorphism sends

$$\{x, -x\} \mapsto x^n.$$

(5) Let $n \geq 1$. We shall show that

$$\mathbb{C}^\times/\mu_n \simeq \mathbb{C}^\times.$$

Indeed, consider the map

$$\phi : \mathbb{C}^\times \to \mathbb{C}^\times \qquad \phi(z) = z^n.$$

Note that ϕ is surjective and $\ker(\phi) = \mu_n$. Thus by the first isomorphism theorem, we have an isomorphism

$$\overline{\phi} : \mathbb{C}^\times/\mu_n \to \mathbb{C}^\times \qquad \overline{\phi}(z\mu_n) = z^n.$$

Since $\overline{\phi}$ is an isomorphism, it has an inverse (which is also an isomorphism). Let us describe this inserve. Every $z \in \mathbb{C}^\times$ has n complex n-th roots. Let w, w' both be n-th roots of z, i.e. $w^n = w'^n = z$. Then

$$(\frac{w}{w'})^n = \frac{w^n}{w'^n} = \frac{z}{z} = 1.$$

Thus $\dfrac{w}{w'} \in \mu_n$, and hence $w\mu_n = w'\mu_n$. It follows that for every $z \in \mathbb{C}^\times$, $\sqrt[n]{z}\mu_n$ is a well-defined element of $\mathbb{C}^\times/\mu_n$. Indeed, even though there are n possible values for $\sqrt[n]{z}$, they all belong the same coset of μ_n. The inverse of $\overline{\phi}$ is the map

$$\mathbb{C}^\times \to \mathbb{C}^\times/\mu_n \qquad z \mapsto \sqrt[n]{z}\mu_n.$$

(Roughly speaking, the ambiguity of having different possible values for $\sqrt[n]{z}$ is cancelled out after passing to the quotient $\mathbb{C}^\times/\mu_n$, since in the quotient $\mathbb{C}^\times/\mu_n$ complex numbers that differ (multiplicatively) by an element of μ_n are *identified* with one another (they belong to the coset).)

Exercise 56. Let $n \geq 2$. Show that there is no homomophism $\phi : \mathbb{C}^\times \to \mathbb{C}^\times$ such that for every $z \in \mathbb{C}^\times$, $\phi(z)^n = z$. (Every $z \in \mathbb{C}^\times$ has n distinct n-th roots. One might think that perhaps it is possible to pick *an* n-th root $\sqrt[n]{z}$ of z for each z in such a way that $z \mapsto \sqrt[n]{z}$ is a homomorphism.

The question asserts that this is not possible. Hint: Try to argue by contradiction. Try to show that if there is such ϕ, then $\mathrm{Im}(\phi)$ is a proper subgroup of $\mathbb{C}^\times$ which has finite index.[†])

Exercise 57. Give an example of a group G, together with a normal subgroup $H \neq \{e\}$ such that G/H is isomorphic to G.

(6) Let p be a prime number > 2. Let $\phi : U(p) \to U(p)$ be the map defined by $\phi([x]) = [x]^2$. As we see saw in Example (5)(v) of Paragraph 9.3, $\ker(\phi) = \{[1], [-1]\}$. Since $p > 2$, $[1] \neq [-1]$ and hence $|\ker(\phi)| = 2$. By Corollary 6,

$$|\mathrm{Im}(\phi)| = \frac{|U(p)|}{|\ker(\phi)|} = \frac{p-1}{2}.$$

Let us denote $\mathrm{Im}(\phi)$ by $U(p)^2$. Thus

$$U(p)^2 = \{[x]^2 : [x] \in U(p)\}.$$

Note that an element $[a] \in U(p)$ belongs to $U(p)^2$ if and only if there is an integer x such that

$$x^2 \equiv a \pmod{p}.$$

Traditionally, the elements of $U(p)^2$ are called the *quadratic residues* mod p. For instance, let us consider $p = 11$. The elements of $U(11)$ are

$$[\pm 1],\ [\pm 2],\ [\pm 3],\ [\pm 4],\ [\pm 5].$$

Squaring these we see that the quadratic residues mod 11 are

$$[1],\ [4],\ [9],\ [16] = [5],\ [25] = [3].$$

There are $5 = \frac{11-1}{2}$ of them, as expected.

The subgroup $U(p)^2$ of $U(p)$ has index

$$\frac{|U(p)|}{|U(p)^2|} = \frac{p-1}{(p-1)/2} = 2.$$

[†]This question will not be on the exam.

By Exercise 54, the product of every two non-quadratic residues is a quadratic residue. For instance, back to the example of $p = 11$, the non-quadratic residues mod 11 are

$$[2],\ [6],\ [7],\ [8],\ [10].$$

The product of any two of these is a quadratic residue., e.g. $[2] \cdot [7] = [3]$ and $[7] \cdot [10] = [4]$.

13. Direct products

13.1. Definition. Let G and H be groups. Consider the cartesian product

$$G \times H = \{(g, h) : g \in G \text{ and } h \in H\}$$

of the sets G and H. One can define a binary operation on $G \times H$ by

$$(g, h) \cdot (g', h') = (gg', hh').$$

Note that the product gg' in the first entry is taking place in G and the product hh' in the second entry is taking place in H. It is easy to check that $G \times H$ under this operation forms a group. We leave the verification of associativity to the reader. The identity of $G \times H$ is (e_G, e_H), as

$$(g, h) \cdot (e_G, e_H) = (ge_G, he_H) = (g, h)$$

(and similarly $(e_G, e_H) \cdot (g, h) = (g, h)$). The inverse of (g, h) is (g^{-1}, h^{-1}):

$$(g, h) \cdot (g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H)$$

and similarly $(g^{-1}, h^{-1}) \cdot (g, h) = (e_G, e_H)$.

The group $G \times H$ (with operation as above) is called the *direct product* of G and H. It is clear that $|G \times H| = |G| \cdot |H|$.

For example, consider the direct product $\mathbb{Z}/6\mathbb{Z} \times S_5$. Each of its elements is a pair of the form $([a], \sigma)$, where $[a] \in \mathbb{Z}/6\mathbb{Z}$ and $\sigma \in S_5$. We have

$$([4], (123)) \cdot ([3], (1245)) = ([4] + [3], (123)(1245)) = ([1], (13)(245)).$$

The identity of this group is the pair $([0], e)$ (e the identity of S_5). The inverse of $([4], (123))$ is $([2], (321))$.

The direct product of more than two groups is defined similarly: Let $G_1, G_2, \ldots, G_n$ be groups. The set

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) : g_i \in G_i\}$$

forms a group under the operation defined by

$$(g_1, g_2, \ldots, g_n) \cdot (g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n').$$

This group is called the direct product of $G_1, G_2, \ldots, G_n$. Its identity is

$$(e_{G_1}, e_{G_2}, \ldots, e_{G_n})$$

and

$$(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}).$$

13.2. Orders in a direct product.

PROPOSITION 31. Let G and H be groups, $g \in G$ and $h \in H$. Then $(g, h) \in G \times H$ has finite order if and only if g and h have finite order. Moreover, if g and h have finite order, then

$$|(g, h)| = \operatorname{lcm}(|g|, |h|).$$

(Here lcm stands for the least common multiple.)

PROOF. Note that $(g, h)^n = (g^n, h^n)$. Thus for any integer n,[†]

$$(g, h)^n = (e, e) \text{ if and only if } g^n = e \text{ and } h^n = e.$$

If (g, h) has finite order, there is $n \geq 1$ such that $(g, h)^n = (e, e)$ (=identity of $G \times H$), i.e. $g^n = e$ and $h^n = e$, so that $|g|$ and $|h|$ are finite. Conversely, suppose g and h have finite order. Then

$$(g, h)^{\operatorname{lcm}(|g|,|h|)} = (g^{\operatorname{lcm}(|g|,|h|)}, h^{\operatorname{lcm}(|g|,|h|)}) = (e, e),$$

[†]To simplify the notation we shall often just write e for both e_G and e_H. It will be clear from the context which identity e refers to.

and hence (g,h) has finite order. Let $\ell = |(g,h)|$. It follows from the above calculation that $\ell \mid \operatorname{lcm}(|g|,|h|)$. We also have $g^\ell = e$ and $h^\ell = e$ (why?), so that $|g| \mid \ell$ and $|h| \mid \ell$. It follows $\operatorname{lcm}(|g|,|h|) \leq \ell$. Putting together with the earlier conclusion that $\ell \mid \operatorname{lcm}(|g|,|h|)$ we get $\ell = \operatorname{lcm}(|g|,|h|)$. □

Exercise 58. Find the order of the given elements.

(a) $([2],(12)) \in U(5) \times S_3$

(b) $([2],(12345)) \in \mathbb{Z}/6\mathbb{Z} \times S_5$

(c) $([1],[1]) \in \mathbb{Z}/4\mathbb{Z} \times U(4)$

COROLLARY 7. Let G and H be finite cyclic groups. Then $G \times H$ is cyclic if and only if $\gcd(|G|,|H|) = 1$.

PROOF. Let $|G| = m$ and $|H| = n$. Note that $|G \times H| = mn$. Suppose $\gcd(m,n) = 1$. Let $G = \langle g \rangle$ and $H = \langle h \rangle$. Then

$$|(g,h)| \overset{\text{why}}{=} \operatorname{lcm}(|g|,|h|) \overset{\text{why}}{=} \operatorname{lcm}(m,n) = mn,$$

since m and n are coprime. Thus $G \times H$ is cyclic generated by (g,h).

For the converse, we shall show that if $\gcd(|G|,|H|) > 1$, then $G \times H$ is not cyclic. Indeed, for every $(g',h') \in G \times H$,

$$(g',h')^{\operatorname{lcm}(m,n)} = (g'^{\operatorname{lcm}(m,n)}, h'^{\operatorname{lcm}(m,n)}) \overset{\text{why}}{=} (e,e).$$

Thus every element of $G \times H$ has order $\leq \operatorname{lcm}(m,n)$, which is $< mn$ if $\gcd(|G|,|H|) > 1$. □

Thus for instance, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ are not cyclic. On the other hand, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2 \times \mu_3$ are cyclic (and hence isomophic to $\mathbb{Z}/6\mathbb{Z}$). Note that a generator for $\mathbb{Z}/2 \times \mu_3$ is $([1], e^{2\pi i/3})$ (see the proof of the corollary). Similarly, $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is cyclic (and hence isomorphic to $\mathbb{Z}/120\mathbb{Z}$). A generator for $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is $([1],[1])$. Another generator is $([2],[3])$.

Exercise 59. Let $G_1, G_2, \ldots, G_n$ be groups, and $g_i \in G_i$. Show that $(g_1, g_2, \ldots, g_n) \in G_1 \times \cdots \times G_n$ has finite order if and only if each g_i has finite order, and moreover if the g_i all have finite order, then

$$|(g_1, g_2, \ldots, g_n)| = \operatorname{lcm}(|g_1|, \ldots, |g_n|).$$

Exercise 60. Let $G_1, \ldots, G_n$ be finite cyclic groups. Let $|G_i| = m_i$. Show that $G_1 \times \cdots \times G_n$ is cyclic if and only if the m_i are pairwise coprime.

13.3. Some remarks. In this paragraph we make some remarks and observations about direct products. Throughout, G and H are groups.

(1) The notion of direct product gives us a way of constructing "larger" groups from "smaller" ones.

(2) If $K \leq G$ and $L \leq H$, then $K \times L \leq G \times H$. If $K \trianglelefteq G$ and $L \trianglelefteq H$, then $K \times L \trianglelefteq G \times H$. (Verify these as exercises.)

(3) One has $G \times H \simeq H \times G$. Indeed, the map

$$G \times H \to H \times G \qquad (g, h) \mapsto (h, g)$$

is an isomorphism.

(4) The maps

$$G \to G \times H \qquad g \mapsto (g, e)$$

and

$$H \to G \times H \qquad h \mapsto (e, h)$$

are injective homomorphisms. They are called the natural embeddings of G and H into the direct product. These embeddings give isomorphisms $G \to G \times \{e\}$ and $H \to \{e\} \times H$.

(5) One has surjective homomorphisms

$$pr_1 : G \times H \to G \qquad (g, h) \mapsto g$$

and

$$pr_2 : G \times H \to H \qquad (g, h) \mapsto h.$$

These are called the *projections* onto the first and second factor (or onto G and H). Note that $\ker(pr_1) = \{e\} \times H$, so that by the first isomorphism theorem

$$(G \times H)/(\{e\} \times H) \simeq G.$$

Similarly, applying the first isomorphism theorem to the projection onto H we get

$$(G \times H)/(G \times \{e\}) \simeq H.$$

(6) $G \times H$ is abelian if and only if both G and H are abelian. Indeed, if G and H are abelian, then for every $(g, h), (g', h') \in G \times H$,

$$(g, h) \cdot (g', h') = (gg', hh') = (g'g, h'h) = (g', h') \cdot (g, h).$$

Conversely, if $G \times H$ is abelian, then since $pr_1 : G \times H \to G$ is a surjective homomorphism, G is abelian (see Problem 3 of Assignment 6). Similarly in view of pr_2 we see H is abelian. Alternatively, to see that G and H must be abelian if $G \times H$ is abelian, one can use the fact that G (resp. H) is isomophic to the subgroup $G \times \{e\}$ (resp. $\{e\} \times H$) of $G \times H$.

(7) Suppose $G \times H$ is cyclic. Then both G and H will be cyclic. Indeed, this follows by applying Problem 3 of Assignment 6 to the projection maps pr_1 and pr_2. (Alternatively, one can use the fact that G and H are isomorphic to the subgroups $G \times \{e\}$ and $\{e\} \times H$ of $G \times H$, which are cyclic since every subgroup of a cyclic group is cyclic.)

Exercise 61. Suppose H is a group such that $\mathbb{Z} \times H$ is cyclic. Show that H is trivial (i.e. $|H| = 1$).

Exercise 62. Let G, G', H be groups and $G \simeq G'$. Show that $G \times H \simeq G' \times H$.

Exercise 63. Suppose G and H are finite cyclic groups, $|G| = m$, $|H| = n$, and $\gcd(m, n) = 1$. Show that (g, h) is a generator of $G \times H$ if and only if g is a generator of G and h is a generator of H. (The "if" statement is already done in the proof of the Corollary 7. For the "only if" part, i.e. that $G \times H = \langle (g, h) \rangle$ implies $G = \langle g \rangle$ and $H = \langle h \rangle$, use the projection maps onto G and H. Also see Exercise 30.)

Exercise 64. Let m, n be positive integers that are relatively prime. Show that $\varphi(mn) = \varphi(m)\varphi(n)$. (Here φ is the Euler function. Hint: Use the previous exercise and count the number of generators of $G \times H$, where G (resp. H) is a cyclic group of order m (resp. n).)

13.4. Classification of finite abelian groups. The following result is sometimes referred to as the fundamental theorem of finite abelian groups.[†]

[†]There are more precise versions of this result, which we won't have time to discuss.

THEOREM 6 (The fundamental theorem of finite abelian groups). Every finite abelian group is isomorphic to a direct product of cyclic groups. In other words, if G is a finite abelian group, there are integers k and $n_1, \ldots, n_k$ such that

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

We will skip the proof. The result can be used to classify all abelian groups of a given order up to isomophism.

Examples. (1) By the fundamental theorem of finite abelian groups, every abelian group of order 4 is isomorphic to one of the two groups $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. These two groups are not isomorphic (why), so that *up to isomophism*, there are exactly two abelian groups of order 4:

$$\mathbb{Z}/4\mathbb{Z} \text{ and } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

One can show that in fact every group of order 4 is abelian (see Exercise 52), so that up to isomophism there are exactly two groups of order 4.

(2) We already know that every abelian group of order 6 is cyclic and hence isomorphic to $\mathbb{Z}/6\mathbb{Z}$ (see Corollary 5). The fundamental theorem above gives the same conclusion: Indeed, every abelian group of order 6 is isomophic to one of $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. But these are isomorphic to one another (since $\gcd(2,3) = 1$).

Exercise 65. Let $n = p_1 \cdots p_k$, where the p_i are distinct primes. Show that every abelian group of order n is cyclic. (Hint: You can either use Theorem 6 or give an argument along the lines of that of Corollary 5.)

(3) Every abelian group of order 8 is isomophic to one of $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4 \times \mathbb{Z}/2$, and $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$. These are mutually non-isomorphic. (To see that $\mathbb{Z}/4 \times \mathbb{Z}/2$ and $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ are not isomorphic note that $\mathbb{Z}/4 \times \mathbb{Z}/2$ has an element of order 4 whereas $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ does not.) Thus up to isomorphism, there are three abelian groups of order 8, namely $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4 \times \mathbb{Z}/2$, and $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.

Exercise 66. The group $U(15)$ is an abelian group of order 8, and as such is isomorphic to one of the groups listed in the example above. Which one?

(4) Let us find all abelian groups of order 12 up to isomoprhism. By Theorem 6, every abelian group of order 12 is isomorphic to one of

$$\mathbb{Z}/12,\ \mathbb{Z}/6 \times \mathbb{Z}/2, \mathbb{Z}/4 \times \mathbb{Z}/3,\ \mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Note that $\mathbb{Z}/12 \simeq \mathbb{Z}/4 \times \mathbb{Z}/3$ and $\mathbb{Z}/6 \times \mathbb{Z}/2 \simeq \mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ (why?). Thus up to isomorphism, there are two abelian groups of order 12, namely $\mathbb{Z}/12$ and $\mathbb{Z}/6 \times \mathbb{Z}/2$.

Exercise 67. List all abelian groups of order 15 up to isomorphism.

Exercise 68. List all abelian groups of order 18 up to isomorphism.

Exercise 69. List all abelian groups of order 24 up to isomorphism.

Exercise 70. List all abelian groups of order 27 up to isomorphism.

Exercise 71. List all abelian groups of order 36 up to isomorphism.

Exercise 72. List all abelian groups of order 40 up to isomorphism.