Math 375
Week 2

2.1 Groups

Recall our basic definition:

Definition 1 *Suppose that:*

i) G *is a set and that* $*$ *is a binary operation on* G *(i.e.,* G *is* ***closed*** *under* $*$*);*

ii) $*$ *is associative;*

iii) there exists $e \in G$ *such that* $a * e = e * a = a$ *for all* $a \in G$ *(i.e., the existence of an* ***identity****; the same identity for all* $a \in G$*);*

iv) for each $X \in G$ *there exists* $y \in G$ *so that* $a * b = b * a = e$*, where* e *is the identity element from (iii) (i.e.,* ***inverses*** *exist).*

Then G *with its binary operation* $*$ *is a* ***group*** *and is denoted by* $(G, *)$.

Notice that $\emptyset$ cannot be a group because (iii) fails. Notice that the group operation need not be commutative.

Example 1 Five examples of groups: $(\mathbf{R}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{Z}, +)$, $(\mathbf{R}^*, \times)$, $(\mathbf{Q}^*, \times)$, $(V, +)$ where V is any vector space, e.g. $(M_{m,n}, +)$, $(\mathbf{R}^n, +)$. Also $(Gl(n), \times)$. We will assume that $(\mathbf{Z}_n, \oplus)$ is a group. What about examples of operations on sets that are not groups? $(Z, \times)$, $(M_{n,n}, \times)$, or $(Z, -)$.

Example 2 Let's verify that if

$$\Delta = \left\{ A \in M_{22} |\ A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\ a \in \mathbf{R}^* \right\},$$

then $(\Delta, \cdot)$ is a group.

Definition 2 *For any postive integer* n*, the let* $U(n)$ *denote the set of all postive integers less than* n *that are relatively prime to* n*. It is called the* ***group of units mod*** n.

Example 3 $U(12) = \{1, 5, 7, 11\}$. The Cayley table is

$\odot \bmod 12$	1	5	7	11	
1		1	5	7	11
5	5	1	11	7	
7	7	11	1	5	
11	11	7	5	1	

SOLUTION Let's verify that $U(n)$, the group of units mod n is a group under multiplication. We must check the four group properties. First, note the following. Suppose $1 = \gcd(x, n)$. By the division algorithm $x = qn + r$ where $0 \leq r < n$. By the linear combination theorem,

$$1 = sx + tn = s(qn + r) + tn = sr + (sq + t)n.$$

By the converse of the linear combination theorem since 1 is a linear combination of r and n, then $\gcd(r, n) = 1$ so $r \in U(n)$. (Why didn't we say $x \in U(n)$?

Second: note by a homework problem that you are currently doing,

$$(ab) \bmod n = [(a \bmod n)(b \bmod n)] \bmod n.$$

This says you can mod before or after the operation and you get the same result. By the way, the same is true for addition.

CLOSURE Suppose that $j, k \in U(n)$. Then by the linear combination theorem,

$$1 = qj + rn \qquad 1 = sk + tn.$$

By multiplying:

$$1 = qs \cdot jk + (qjt + rsk + rtn)n,$$

so by the converse to the linear combination theorem (from homework), $1 = \gcd(jk, n)$. So $jk \bmod n$ is in $U(n)$ by our first comment.

ASOCIATIVITY From our second comment

$$\begin{aligned} [(ab \bmod n)(c \bmod n)] \bmod n &= [(ab)c] \bmod n && \text{comment 2} \\ &= [a(bc)] \bmod n && \text{assoc} \\ &= [(a \bmod n)[(bc \bmod n)] \bmod n. \end{aligned}$$

IDENTITY Clearly $e = 1$ is the multiplicative identity in $U(n)$.

INVERSES Notice $k \in U(n)$ implies $\gcd(k, n) = 1$. We must find $r \in U(n)$ so that $rk = 1 \bmod n$. By the linear combination theorem, there are integers b and s so that $1 = ks + bn$. By the division algorithm we may write $s = qn + r$ where $0 \leq r < n$. So

$$1 = ks + bn = k(qn + r) + bn = kr + (kq + b)n = kr \bmod n.$$

By the converse of the linear combination theorem, $\gcd(r, n) = 1$ so $r \in U(n)$. ∎

Basic Properties of Groups

Many basic results are easy to prove if we are careful to use the definition of the concept involved.

THEOREM 3 *If $(G, *)$ is a group then:*

a) *there is only one identity element in G;*

b) *if $x \in G$ then x has only one inverse.*

PROOF From the definition of a group it appears that there *could* be more than one identity element or that an element might have more than one inverse. But we can show that this is not possible.

(i) Suppose that e and e' are both identities in G (what properties do e and e' then have?). Then:

$$e = e * e' = e'$$

so $e = e'$. That is, all identity elements are equal to each other — that is, there is *only one* identtiy element in G.

(ii) Suppose y and z were both inverses of x (what properties would y and z have?). Then:

$$y = y * e = y * (x * z) = (y * x) * z = e * z = z.$$

Part (ii) means that we can use x^{-1} to indicate *the* inverse of x in any group. That is, there can be no ambiguity about which element we are referring to with the notation x^{-1} because x has a single inverse. ∎

From linear algebra you know that if $A,\ B \in GL(n)$, then $(AB)^{-1} = B^{-1}A^{-1}$. The same result is true in *any* group.

LEMMA 4 *If $(G, *)$ is a group and $x,\ y \in G$, then:*

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

PROOF We need to show that $y^{-1} * x^{-1}$ acts like the inverse of $x * y$.

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

Similarly, $(x * y) * (y^{-1} * x^{-1}) = e$. Since $(x * y)^{-1}$ is unique, it must be $y^{-1} * x^{-1}$. ∎

We can solve 'algeraic equations' in the usual ways by cancellation of factors.

LEMMA 5 *Let $(G, *)$ be a group with $x,\ y,\ z \in G$. Then:*

a) *if $x * y = x * z$ then $y = z$ (left cancellation) (note order: not $y * x = x * z$);*

b) *if $y * x = z * x$ then $y = z$ (right cancellation).*

PROOF For (ii):

$$y = y * e = y * (x * x^{-1}) = (y * x) * x^{-1}$$
$$= (z * x) * x^{-1} = z * (x * x^{-1}) = z * e = z.$$

The proof of (i) is quite similar. ∎

LEMMA 6 *If $(G, *)$ is a group and $x \in G$, then $(x^{-1})^{-1} = x$.*

PROOF Use cancellation on the equation: $xx^{-1} = e = (x^{-1})^{-1}x^{-1}$. ∎

EXAMPLE 4 For $(\mathbf{R}^*, \cdot)$, the Lemma says that $\frac{1}{\frac{1}{x}} = x$.

DEFINITION 7 *If $(G, *)$ is a group and $*$ is commutative, then the group is called* ***abelian****. (After Abel, the great Scandanvian mathematician of the late 19^{th} century.)*

EXAMPLE 5 What are some other examples of abelian groups with which your are familiar? Do you know any non-abelian groups? $((GL(n), \cdot))$, D_4

Example 6 The **Unit Quaternions,** Q_8, are the eight 2×2 matrices

$$\{I, -I, J, -J, K, -K, L, -L\}$$

with entries in the complex numbers, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$
$$K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad L = JK = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Determine whether these matrices form a group under multiplication by filling in a Cayley Table. (Remember, matrix multiplication is associative and does not need to be checked.) Is it commutative?

SOLUTION It is a group, but not commutative (since the table is not symmetric).

$\cdot$	I	$-I$	J	$-J$	K	$-K$	L	$-L$
I	I	$-I$	J	$-J$	K	$-K$	L	$-L$
$-I$	$-I$	I	$-J$	J	$-K$	K	$-L$	L
J	J	$-J$	$-I$	I	L	$-L$	$-K$	K
$-J$	$-J$	J	I	$-I$	$-L$	L	K	$-K$
K	K	$-K$	$-L$	L	$-I$	I	J	$-J$
$-K$	$-K$	K	L	$-L$	I	$-I$	$-J$	$-J$
L	L	$-L$	K	$-K$	$-J$	J	$-I$	I
$-L$	$-L$	L	$-K$	K	J	$-J$	I	$-I$

Exponents and Order

We now fix the following conventions for **powers** of elements in G.

Definition 8 *Let $x \in G$, a group. Then*

a) $x^0 = e$;

b) *for $n \in \mathbf{Z}^+$, $x^n = xx \cdots x$ (n factors);*

c) *for $n \in \mathbf{Z}^+$, $x^{-n} = (x^{-1})^n$.*

As you would expect, the familiar laws for exponents are satisfied:

Theorem 9 *Let G be a group with $x \in G$. Let $m, n \in \mathbf{Z}$. Then*

a) $x^m x^n = x^{m+n}$;

b) $(x^n)^{-1} = x^{-n}$;

c) $(x^m)^n = x^{mn} = (x^n)^m$.

PROOF All the results are familiar. ∎

CONVENTIONS

Multiplicatve like $\mathbf{R}^*$ or $U(n)$		**Additive** like $\mathbf{Z}$ or $\mathbf{Z}_n$	
$a \cdot b$ or ab	multiplication	$a + b$	sum
e or 1	identity	0	zero, additive identity
a^{-1}	inverse of a	$-a$	negative, add inverse
a^n	power of a	na	multiple of a
ab^{-1} (not $(ab)^{-1}$)	quotient	$a - b$	difference

For example in additive notation:

$$(x^n)^{-1} = x^{-n} \qquad \text{becomes} \qquad -(nx) = (-n)x.$$

EXAMPLE

a) Show that in an abelian group we have $(ab)^n = a^n b^n$. (How would this be written in additive notation?)

b) Show that in general: $(ab)^n \neq a^n b^n$. In D_4, we have $(r_{270}v)^2 = d^2 = e$, but ${r_{270}}^2 v^2 = r_{180}$. In the unit Quaternions Q_8, we have $(JK)^2 = L^2 = -I$, but $J^2K^2 = (-I)(-I) = I$. □

DEFINITION 10 *The number of elements in a group (whether finite or infinite) is called the* ***order*** *of the group. It is denoted* $|G|$.

EXAMPLE 8 Give 5 examples of groups of infinite order and groups of finite order.

DEFINITION 11 *Let* $x \in G$, *a group. The* ***order*** *of* x *is the smallest positive integer* n *such that* $x^n = e$. *(In additive notation,* $nx = 0$.*) If no such* n *exists, then* x *is said to have* ***infinite order****. The order will be denoted by* $|x|$ *or by* $o(x)$.

EXAMPLE

a) For any group G, we have $|e| = 1$.

b) Find the order of each element of Q_8, e.g., $o(J) = 4$.

c) In $(D_3, \circ)$ the flip reflection a has order 2 because: $a^1 = a \neq r_0$ and $a^2 = r_0$. Similarly for any otther reflection in any D_n. Notice $|r_{120}| = 3$ since $r_{120} \neq r_0$ and $r_{120}^2 = r_{240}$, but $r_{120}^3 = r_0$. Similarly $|r_{240}| = 3$.

d) In $(\mathbf{Z}, +)$, $o(2) = \infty$ since for all $n \in \mathbf{Z}^+$, $n2 \neq 0$.

e) In $GL(2)$ we have,

$$\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = 2.$$

f) $2I \in GL(3)$ since $\det 2I_3 = 2^3 \cdot \det I = 8 \cdot 1 = 8 \neq 0$. However $|2I| = \infty$ since $(2I_3)^n = 2^n I \neq I \ \forall n \in \mathbf{Z}^+$.

Lemma 12 *Let G be a group. Assume $x^2 = e\ \forall x \in G$ (what does this say about order?). Show that G is an abelian group.*

SOLUTION We must show that $\forall a, b \in G\ ab = ba$. We use our standard 'trick.'

$$\begin{aligned} ab = (ab)e = (ab)(ba)^2 &= ab((ba)ba) \\ &= a(bb)a(ba) \\ &= aea(ba) = (aa)(ba) = e(ba) = ba. \end{aligned}$$ □

2.2 Introduction to Subgroups

The Definition and Basic Tests

We know that $(\mathbf{R}, +)$ is a group and that $(\mathbf{Q}, +)$ is also a group and that $\mathbf{Q} \subseteq \mathbf{R}$. Similarly $(\mathbf{Z}, +)$ is a group and $\mathbf{Z} \subseteq \mathbf{Q}$ and $\mathbf{Z} \subseteq \mathbf{R}$. Yet not all subsets of $\mathbf{R}$ are groups. For example, the odd integers are not a group nor is $\mathbf{R}^+$; neither set is closed under the operation of addtion.

In general how do you determine which subsets are groups? This problem is akin to the question of determining which subsets of a vector space are subspaces under the original vector space operation.

Definition 13 *A subset H of a group $(G, *)$ is a **subgroup** of G if the elements of H form a group under the operation $*$. (This means you have to check all four group conditions on H with operation $*$.) We use the notation $H \leq G$ to indicate a subgroup and $H < G$ to indicate a proper subgroup.*

Notice that $H = \{e\}$ is always a subgroup of G. It is called the **trivial subgroup** of G.

Notice that $\mathbf{Z}_n$ is *not* a subgroup of $\mathbf{Z}$ since the operations of addition are different.

Example

a) $\{r_0, r_{120}, r_{240)}\}$ is a subgroup of D_3. (Use the Cayley table.)

b) $\{r_0, v\}$ is a subgroup of D_3 (where v is a flip over an axis).

c) $M = \{A \in GL(n) |\ \det A = 2\}$.

d) Is $\{a, b, c\}$ a subgroup of $(D_3, *)$?

e) Is $\{0, 2, 4, 6\}$ a subgroup of $(\mathbf{Z}_8, \oplus)$?

We mentioned that $\mathbf{Z}$ is a subgroup of $(\mathbf{R}, +)$. Now when you worked with subspaces, you did not go through checking all eight vector space axioms for the subspace in question, in fact you only checked the two closure properties for addition and scalar multiplication. We have a similar situation with groups. Instead of checking all four group properties all one needs to check is clossure and the existence of inverses.

THEOREM 14 ***(Two Step Test)*** *Let H be a nonempty subset of a group G. If*

i) $\forall\ a, b \in H$, $ab \in H$ (H is closed under the same operation as in G);

ii) $\forall\ a \in H$, $a^{-1} \in H$ (inverses exist in H);

then H is asubgroup of G.

PROOF We must show that if (i) and (ii) hold then the four group conditions are satisfied. These are

CLOSURE H is closed. This holds by (i).

ASSOCIATIVITY Holds because it holds in G, that is $\forall\ a, b, c \in H$, $a(bc) = (ab)c$ because this is true in G and if $a, b, c \in H$ then $a, b, c \in G$.

IDENTITY Let e be the identity in G. Then since $H \neq \emptyset$, there is an element $h \in H$. But by condition (ii), $h \in H \Rightarrow h^{-1} \in H$. But then by condition (i), $hh^{-1} = e \in H$. So H has an identity.

INVERSES Exist for every element in H by condition (ii).

EXAMPLE 11 Verify that $SL(\mathbf{R}, n) = \{A \in GL(\mathbf{R}, n) = GL(n) \mid \det A = 1\}$ is a subgroup.

EXAMPLE 12 Is $H = \left\{ A \in GL(\mathbf{R}, n) \mid A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \right\}$ a subgroup of $GL(\mathbf{R}, n)$?

THEOREM 15 ***(One Step Test)*** *Let G be a group and H a nonempty subset of G. Then H is a subgroup if ab^{-1} is in H whenever a and b are in H.*

PROOF Let $x \in H$. By hypothesis, $xx^{-1} = e \in H$. Thus, for any element y in H, $ey^{-1} = y^{-1} \in H$, so H is closed under inverses. Next, for any x and y in H, since $y^{-1} \in H$, then $x(y^{-1})^{-1} = xy \in H$. So H is closed. By the two step test, $H \leq G$. ∎

EXAMPLE 13 If H and K are both subgroups of G show that $H \cap K$ is a subgroup of G.

I like two step, but you may like one step method.

EXAMPLE 14 Show that $H = GL^{+}(\mathbf{R}, n) = \{A \in M_{nn} \mid \det A > 0\}$ is a subgroup of $GL(\mathbf{R}, n)$.

SOLUTION We need to know that H is nonempty. (It is usually simple to see if H contains the identity.) Notice $I \in H$ since $\det I = 1 > 0$. Now let $A, B \in H$. Show $AB^{-1} \in H$. Well, check $\det AB^{-1} = \det A(\det B)^{-1} > 0$ since $\det A, \det B > 0$. □

Notice that when checking subgroups by either the one or two step method, it is crucial to:

1. Identify the property that distinguishes the elements of the set. *What property puts an element in H?*
   For the one step method:
2. Prove that e has the property (to verify that H is not empty).
3. *Assume* that a and b have the property, and *show* that ab^{-1} has the property.
   In the two step method:

2'. *Assume* that a has the property, and *show* that a^{-1} has the property.
3'. *Assume* that a and b have the property, and *show* that ab has the property.

Thus, either process is conceptually quite simple. But it hinges on being able to determine the defining property of H.

When the group G is finite, there is an even easier test.

THEOREM 16 ***(Finite Subgroup Test)*** *Let H be a nonempty subset of a group G. If H is closed (under the operation in G), then $H \leq G$.*

PROOF Use the two step method. We are given closure. So all we have to do is show that if $a \in H$, then $a^{-1} \in H$. But since H is closed, then $a, a^1, a^2 \ldots \in H$. But H is finite, so not all of these elements are distinct. Thus $a^n = a^m$ for some $i \neq j$ where we may asume that $n > m$. But then $e = a^{n-m} = aa^{n-m-1} = e$, where $n - m - 1 \geq 0$. So $a^{-1} = a^{n-m-1} \in H$ since all nonnegative powers of a are in H. ∎

EXAMPLE 15 $\{1, -1, i, -i\} \leq \mathbf{C}^*$.

EXAMPLE 16 Let k be a divisor of n. Let $U_k(n) = \{x \in U(n) \mid x = 1 \bmod k\}$. Show that $U_k(n)$ is a subgroup of $U(n)$.

EXAMPLE 17 Let's see what this means before we do the proof. Consider $U_4(24)$ (note that 4 is a divisor of 24). $U_4(24) = \{1, 5, 13, 17\}$. Why isn't $9 \in U_4(24)$?

$\odot \bmod 24$	1	5	17	23
1	1	5	17	23
5	5	1	17	13
13	13	17	1	5
17	17	13	5	1

Does this group (pattern) look familiar?

SOLUTION Use the finite subgroup test. Let $a, b \in U_k(n)$. Is $ab \in U_k(n)$? Well

$$ab \bmod k = [(a \bmod k)(b \bmod k)] \bmod k = 1 \cdot 1 \bmod k = 1 \bmod k.$$ □