Math 113, Fall 2019
Lecture 5, Thursday, 9/12/2019

Topics Today:

- $\mathbb{Z}_n$ is a group
- Groups via tables
- Subgroups
- Subgroups of U_6
- x^n and cyclic (sub)groups

Handout on x^n.
Homework due Sept 19: §4 : 2,6,24,30,36,37 ; §5: 4,11,13,16,22,23,50 ; §6 : 2, 6, 10, 18, 22, 34, 46.
Readings: Up to top of p. 70

1 Clicker Questions

Which of the following are true?
(False) Multiplicative notation is used **only** for nonabelian groups. (True) Additive notation is used **only** for abelian groups.

How many of the following are true?
(False) $\langle \mathbb{Q}^*, \times \rangle$ is a subgroup of $\langle \mathbb{Q}, + \rangle$ (not the induced operation)
(False) $\mathbb{N}$ is a subgroup of $\mathbb{Z}$ ($\mathbb{N}$ is not a group)
(False) $\mathbb{Z}_2 := \{0, 1\}$ is a subgroup of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
(True) U is a subgroup of $\langle \mathbb{C}^*, \times \rangle$.
Where $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ and $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$.

2 Review

Recall that last time, we took $n \in \mathbb{Z}^+$ and let $\tilde{\mathbb{Z}}_n$ to be the set of equivalence classes of $\equiv_n$ (congruence mod n) in $\mathbb{Z}$.

$$\tilde{\mathbb{Z}}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

and these are each distinct.
Binary operation $+'$ on $\tilde{\mathbb{Z}}_n : \overline{a} +' \overline{b} = \overline{a+b}$ shows that $\tilde{\mathbb{Z}}_n$ is a group.
Define $\Psi : \mathbb{Z}_n \to \tilde{\mathbb{Z}}_n$ by $\Psi(a) = \overline{a}$ for all $a \in \mathbb{Z}_n := \{0, 1, \dots, n-1\}$. This is a bijection. It is an isomorphism because for all $a, b \in \mathbb{Z}_n$, we have:

$$a +_n b = \begin{cases} a+b, & a+b < n \\ a+b-n, & a+b \geq n \end{cases}$$

and either way, $a +_n b \equiv a + b \pmod{n}$. Therefore,

$$\overline{a +_n b} = \overline{a+b}, \forall_{a,b \in \mathbb{Z}_n}.$$

Therefore

$$\Psi(a +_n b) = \overline{a +_n b} = \overline{a+b} = \overline{a} +' \overline{b} = \Psi(a) +' \Psi(b).$$

So Ψ is an isomorphism (of binary structures). Since $\tilde{\mathbb{Z}}_n$ is a group, then we conclude that so is $\mathbb{Z}_n$. That is, definitions D_1, D_2, D_3 are structural properties.
So we have a diagram:

$$\begin{tikzcd}
 & a \arrow[rrdd, mapsto] & & \\
a \arrow[dd, mapsto] & \mathbb{Z}_n \arrow[dr, "\phi"] \arrow[dd, "\psi"'] & & \\
 & & U_n & \zeta^a \\
\bar{a} & \tilde{\mathbb{Z}}_n \arrow[ur, "\rho"'] & & \\
 & \bar{a} \arrow[rruu, mapsto] & &
\end{tikzcd}$$

where $U_n = \{z \in \mathbb{C} : Z^n = 1\}$, $\zeta = e^{2\pi i/n} \in U_n$, and $U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$.
ϕ is an isomorphism from Fraleigh page 18. This diagram commutes. That is, $\phi = \rho \circ \psi$.
To see this:

$$\begin{aligned}
\overline{a} = \overline{b} \implies & a \equiv b \pmod{n} \\
& a = b + qn \text{ with } q \in \mathbb{Z} \\
\implies & \zeta^a = \zeta^{b+qn} = \zeta^b (\zeta^n)^a = \zeta^b \cdot 1^a = \zeta^b.
\end{aligned}$$

Definition: isomorphism of groups -

An **isomorphism of groups** is an isomorphism of the underlying binary structures. That is, it is a bijection that satisfies the homomorphism property.
Note that an isomorphism from G to G' takes the identity element of G to the identity element of G' (Theorem 3.14). Additionally, $\forall_x \in G$, it takes the inverse of x in G to the inverse of $\varphi(x)$ in G' (where φ is the isomorphism). This is because

$$\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e) = e' = \varphi(x)\varphi(x)^{-1}.$$

Now cancel $\varphi(x)$ to get $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Definition: Order of a group -

The **order** of a group G is the number of elements in the set G (or our convention is the order is infinity if G is infinite). We denote this $|G|$.

3 Groups via tables

If a group is small (and finite), then it is possible to give its binary operation using a table.

Example: A group of order 3. Let G be such a group, actually $\langle G, * \rangle$. Let the elements of G be e, a, b where e is the identity element. Then we know (so far) that the table looks something like:

$$\begin{bmatrix} * & e & a & b \\ e & e & a & b \\ a & a & - & - \\ b & b & - & - \end{bmatrix}.$$

Now the entries on the second row must all be different by cancellation:

$$a * a = a * b \implies a = b,$$

which is a contradiction to that we know these elements are different. Also, we must include every element of G because G is finite.

Remark: We cannot have $a * a = a$, because cancellation would imply $a = e$. Additionally, we cannot have $a * a = e$, because then the last element in row $a * \cdot$ would have to be b, where we already have a b in that last column $(e * b = b)$. This makes it so the only possibility is: $\boxed{a * a = b}$.

Now we can fill in the rest of the table easily:

$$\begin{bmatrix} * & e & a & b \\ e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{bmatrix}.$$

We notice that this group is also abelian.

Remark: We know this is a group because we know that groups of order 3 exist ($\mathbb{Z}_3$)

4 Clicker Question

For the table on the right, fill it out as far as you can. Then what is $c * c$?

$$\begin{bmatrix} * & e & a & b & c \\ e & e & a & b & c \\ a & a & e & - & - \\ b & b & - & e & - \\ c & c & - & - & - \end{bmatrix}$$

Voyta gives the solution brute-forcing all entries to ultimately get the final entry, namely our desired $c * c$.
Alternatively, we reason that we must have $c * c = e$ because e is present in all columns and rows except the last of each.

Remark: This example we worked with is not $\mathbb{Z}_4$, because $\mathbb{Z}_4$ is:

$$\begin{bmatrix} +_4 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{bmatrix}$$

where the additive inverses are in different places.

Definition: Subgroups -

A **subgroup** of a group $G := \langle G, * \rangle$ is a subset H of G, such that:
(1) H is closed under $*$, and
(2) H is a group, using the induced operation.
We say that $H \subsetneq G$ is a proper subgroup if $H \neq G$ (proper subset of G). As for notation, we write:

$$H \leq G, G \geq H$$

to mean H is a subgroup of G, and

$$H < G, G > H$$

to mean H is a proper subgroup of G (that is, $H \leq G$ and $H \neq G$.)

Examples:
(1) Every group G contains itself as a subgroup (called the "improper subgroup"). That is, for all groups G, we have $G \leq G$.
(2) Every group contains the trivial subgroup $\{e\}$, where e is the identity element.
(3) $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ (where we assume addition operation when we write these as groups).
(4) Similarly, $\{\pm 1\} < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$ (under multiplication), where $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$, etc, as usual.
(5) $U_n < U < \mathbb{C}^*$, for all $n \in \mathbb{Z}^+$.
(6) The set of even integers $< \mathbb{Z}$ (is a subgroup of $\mathbb{Z}$).

Remark: The empty set $\{\}$ is NOT a subgroup of any group G, because a group must have an identity element. In particular, a group must have an element.

Then we have the following theorem:

Theorem 4.1. Let $\langle G, * \rangle$ be a group. A subset H of of G is a subgroup of G if (and only if):
(1) H is closed under $*$ (otherwise there's no induced operation)
(2) H contains the identity element of G (the identity may happen with rings but not here), and
(3) H is closed under the operation of taking inverses ($x^{-1} \in H, \forall_{x \in H}$)

Proof. See Fraleigh for proof. $\square$

Remark: Let G be a group and $H < G$ (H is a subgroup of G). Then
(1) The identity elements of G and H are the same, and
(2) For all $x \in H$, its inverse in H equals its inverse in G.

Proof. (1) Let e_G, e_H be the identity elements of G and H, respectively. Then:

$$e_H * e_H = e_H = e_H * e_G,$$

where the final equality is from e_G as identity, and performing left-cancellation of e_H* gives $e_H = e_G$.
(2) Let $x \in H$, and let x^{-1} be its inverse in G. Let x' be its inverse in H. Then

$$x * x' = e_H = e_G = x * x^{-1},$$

where cancelling gives $x' = x^{-1}$. □

Another Useful Fact:
Let H be a sub**set** of a group G. Then $H < G$ (H is a sub**group** of G) if (and only if) :

$$H \neq \{\} \text{ and } xy^{-1} \in H, \forall_{x,y \in H}$$

Proof. For the forward $\implies$ direction,

$$H \leq G \implies H \neq \{\}$$

and

$$x, y \in H \implies x, y' \in H \implies xy^{-1} \in H$$

Now for the backwards $\impliedby$ direction, consider that $H \neq \emptyset$ implies (by setting $y := x$):

$$\exists_{x \in H} : xx^{-1} \in H \implies e \in H,$$

and

$$ex^{-1} \in H \implies x^{-1} \in H \implies H \text{ is closed under inverse.}$$

Also, $xy = x(y^{-1})^{-1} \in H$, so H is closed under $*$. Now apply the earlier theorem.

□

Example: Let $\varphi : G \to G'$ be an isomorphism, and let $H \leq G$ and recall

$$\varphi[H] = \{\varphi(x) : x \in H\}$$

Then $\varphi[H] \leq G'$.

Proof. (1) $\varphi[H] \neq \{\}$ because $H \neq \{\}$. That is, because H is nonempty, the set $\varphi[H]$ itself cannot be empty.
(2) Let $a', b' \in \varphi[H]$. Then $\exists_{a,b \in H} : \varphi(a) = a'$ and $\varphi(b) = b'$. Also, $ab^{-1} \in H$, so $\varphi(ab^{-1}) \in \varphi[H]$. Vojta leaves us with a cliffhanger, in that it remains to prove:

$$\varphi(ab^{-1}) = a'(b')^{-1}$$

□

Lecture ends here.