date: monday, january 8, 2024

Objectives:

- Groups - fundamental theorem of finite abelian groups, Jordan-Hölder theorem, Sylow theorems
- Rings - polynomial rings, special integral domains
- Fields - extensions, splitting field
- Other topics

I. Groups and Basic Definition

Def$^{\underline{n}}$: A group G is a set with a binary operation $*$ such that

1) $a*(b*c) = (a*b)*c$ for all $a,b,c \in G$ (associativity)
2) $\exists e \in G$ such that $a*e = e*a = a$ for all $a \in G$ (identity)
3) For all $a \in G$, $\exists a^{-1} \in G$ such that $a*a^{-1} = e$ (inverse)

G is abelian if

4) $a*b = b*a$ for all $a,b \in G$

Def$^{\underline{n}}$: Order of G is $|G|$. Say G is finite if $|G| < \infty$.

Basic Properties:

1) $e \in G$ is unique
2) for all $a \in G$, the inverse is unique
3) if $a*b = a*c$, then $b=c$
4) $(a^{-1})^{-1} = a$
5) $(ab)^{-1} = b^{-1}a^{-1}$

Notation. Write ab for $a*b$,

$$a^n = \begin{cases} \underbrace{a*\cdots*a}_{n} & \text{if } n \geq 1 \\ e & \text{if } n=0 \\ \underbrace{(a^{-1})*\cdots*(a^{-1})}_{|n|} & \text{if } n<0 \end{cases}$$

Def$^{\underline{n}}$: The order of $a \in G$, denoted $|a|$, is the smallest $n \geq 0$ such that $a^n = e$. (If no such n, $|a| = \infty$)

eg. $\mathbb{Z}_n=\{0,1,\dots,n-1\}$ with operation + and identity 0

eg. $GL_n(\mathbb{R})=\{$all $n\times n$ invertible matrices with entries in $\mathbb{R}\}$ ← not abelian

eg. D_n = dihedral group of order $2n$
= all rotations of the n-gon

eg. $S_n=\{\sigma \mid \sigma$ is a permutation of $\{1,\dots,n\}\}$

II. Subgroups

Def$^{\underline{n}}$: A subgroup of a group G is a subset $H\subseteq G$ such that H is also a group under the same operation.
$H\subseteq G$ is a subgroup iff

$$\left.\begin{array}{l} 1)\ e\in H \\ 2)\ \text{if } a,b\in H, \text{ then } a*b\in H \\ 3)\ \text{if } a\in H, \text{ then } a^{-1}\in H \end{array}\right\} \iff ab^{-1}\in H$$

Def$^{\underline{n}}$: Let $a\in G$, and $\langle a\rangle=\{a^n \mid n\in\mathbb{Z}\}$,

Thm: $\langle a\rangle$ is a subgroup of G.

Proof
1) $e\in\langle a\rangle$ since $e=a^0\in\langle a\rangle$
2) Suppose $x,y\in\langle a\rangle$, then $x=a^n$ and $y=a^m$. So $xy=a^na^m=a^{n+m}\in\langle a\rangle$.
3) Let $x\in\langle a\rangle$, then $x=a^n$. So $a^{-n}\in\langle a\rangle$ and $xa^{-n}=a^na^{-n}=a^0=e$. So $x^{-1}\in\langle a\rangle$.

□

Def$^{\underline{n}}$: A group G is cyclic if $G=\langle a\rangle$ for some $a\in G$. We call $\langle a\rangle$ the cyclic group generated by a.

eg. $\mathbb{Z}_n=\{0,1,\dots,n-1\}$ is a cyclic group generated by 1
$\langle 1\rangle=\{0\cdot1, 1\cdot1, 2\cdot1,\dots\}=\{0,1,\dots,n-1\}$

Thm: $\mathbb{Z}_n=\langle a\rangle$ iff $\gcd(a,n)=1$

Lagrange's Thm: If H is a subgroup of G (both finite), then $|H| \mid |G|$.

Cor: If $a \in G$, then $|a| \mid |G|$.

<u>Proof</u>

Given $a \in G$, consider the subgroup $\langle a \rangle$. Then $|a| = |\langle a \rangle|$. By Lagrange's, $|\langle a \rangle| \mid |G|$.

$\square$

Cor: If $|G| = p$ is a prime, then G is cyclic.

<u>Proof</u>

Let $a \in G$ such that $a \neq e$. So $|a| \mid |G| = p$. But $|a| \neq 1$, so $|a| = p$. So $|\langle a \rangle| = p$. But $|G| = p$. So $\langle a \rangle = G$.

$\square$

Theme: If we know factorization of $|G|$, what can we say about the structure?

<u>Sketch of Lagrange's Proof</u>

Fix a subgroup H of G. The left coset of H with representative g is the set $gH = \{gh \mid h \in H\}$.

Facts
1) $g_1H = g_2H$ iff $g_1^{-1}g_2 \in H$
2) $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$
3) $|gH| = |H|$

Suppose $g_1H, g_2H, \dots, g_nH$ are the distinct left cosets. Then $G = g_1H \cup \cdots \cup g_nH$ is a disjoint partition by 2). So $|G| = |g_1H| + \cdots + |g_nH|$. But by 3), $|g_iH| = |H|$. So $|G| = |H| + \cdots + |H| = n|H|$. So $|H| \mid |G|$.

$\square$

date: wednesday, january 10, 2024

Equivalence Relations

Equivalence relations appear throughout algebra:
↳ quotient groups
↳ group actions

Def$^{\underline{n}}$: An equivalence relation R on a set X is a subset $R \subseteq X \times X$ such that
① Reflexive: $(x,x) \in R$ for all $x \in X$
② Symmetric: if $(x,y) \in R$, then $(y,x) \in R$
③ Transitive: if $(x,y),(y,z) \in R$, then $(x,z) \in R$

Notation: We sometimes write $x \sim y$ for (x,y)

An equivalence relation "partitions" the set X.
Fix $x \in X$. Then the equivalence class of x is the set: $[x] = \{y \in X \mid (x,y) \in R\}$

Lemma: If $\sim$ is an equivalence relation, then for any $x,y \in X$, either $[x] \cap [y] = \emptyset$ or $[x] = [y]$.

Proof
Suppose that $[x] \cap [y] \neq \emptyset$. So there is an $a \in [x] \cap [y]$. Since $a \in [x]$, have $x \sim a$ and $a \in [y]$ implies $y \sim a$. So $a \sim y$. So by transitivity, $x \sim y$.
Let $b \in [x]$. Then $x \sim b$. So $b \sim x$ and $x \sim y$, so $b \sim y$. So $y \sim b$, ie. $b \in [y]$.
Thus, $[x] \subseteq [y]$.
Let $b \in [y]$. Then $y \sim b$. Since $x \sim y$ and $y \sim b$, $x \sim b$. So $b \in [x]$. So $[y] \subseteq [x]$.
□

Theorem: Let X be a set and R an equivalence relation on X. Let $[x_1], \dots, [x_n]$ be the distinct equivalence classes. Then,

$$X = [x_1] \cup [x_2] \cup \cdots \cup [x_n] \quad \leftarrow \text{a partition.}$$

Proof
Since each $[x_i] \subseteq X$, it's clear that $[x_1] \cup [x_2] \cup \cdots \cup [x_n] \subseteq X$.

Let $y \in X$. Then $[y]$ is an equivalence class, and $[y]=[x_i]$ for some i.
So $y \in [y] = [x_i] \subseteq [x_1] \cup \cdots \cup [x_n]$.
So $X = [x_1] \cup \cdots \cup [x_n]$ and $[x_i] \cap [x_j] = \emptyset$ by Lemma.

$\square$

eg. $X = \{\text{all McMaster students}\}$
$R = \{(x,y) \mid x \text{ and } y \text{ have same height}\}$ ← equivalence relation
$[\text{Bob}] = \{\text{all students same height as Bob}\}$

eg. Let G be a group and H a subgroup. Let $R = \{(g_1, g_2) \mid g_1^{-1} g_2 \in H\}$.
This is an equivalence relation:
1) reflexive: $(g,g) \in R$ since $g^{-1}g = e \in H$
2) symmetric: $(g_1, g_2) \in R$, then
$$g_1^{-1}g_2 \in H \Rightarrow (g_1^{-1}g_2)^{-1} = g_2^{-1}g_1 \in H \Rightarrow (g_2, g_1) \in R$$
3) transitive: $(g_1,g_2),(g_2,g_3) \in R \Rightarrow g_1^{-1}g_2, g_2^{-1}g_3 \in H$. So,
$$g_1^{-1}g_2g_2^{-1}g_3 = g_1^{-1}g_3 \in H \Rightarrow (g_1, g_3) \in R.$$
Note: $[g] = gH = \{gh \mid h \in H\}$

Proof
Let $b \in [g]$. So $(g,b) \in R \Rightarrow g^{-1}b = h \in H$. So $b = gh \in gH$. So $k = gh$ for some $h \in H$. Thus, $g^{-1}k = h \in H$. So $(g,k) \in R \Rightarrow k \in [g]$.

Last class: For Lagrange's theorem, used the partition
$G = g_1H \cup g_2H \cup \cdots \cup g_nH$. This is the same as
$G = [g_1] \cup [g_2] \cup \cdots \cup [g_n]$.

$\square$

Factor Groups/Quotient Groups

Given a group G and subgroup H, can form $G/H = \{gH \mid g \in G\}$.

eg. $G = \mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$
$H = \langle 3 \rangle = \{0, 3, 6, 9\}$
Cosets: $0+H = \{0,3,6,9\}$, $1+H = \{1,4,7,10\}$, $2+H = \{2,5,8,11\}$
$G/H = \{0+H, 1+H, 2+H\}$

$\mathbb{Z}_{12}$

0	3	6	9
1	4	7	10
2	5	8	11

Q: Does G/H have a group structure?

Need an operation!

$(aH)*(bH)=(ab)H$? Almost right... This operation depends upon the coset representative, ie. if $a_1H=a_2H$ and $b_1H=b_2H$, then why is $a_1b_1H=a_2b_2H$? False in general

eg. $S_3=\{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$, $H=\{(1),(1\ 2)\}$

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

$(2\ 3)H=(1\ 3\ 2)H$ $\quad$ $(1\ 2\ 3)(1\ 3\ 2)H=(1)H$ $\neq$

Fix: only allow special subgroups

Def$^{\underline{n}}$: A subgroup $N\leq G$ is normal if $gN=Ng$ for all $g\in G$ <=> $gNg^{-1}\subseteq N$ for all $g\in G$.

$gNg^{-1} = \{gng^{-1}\mid n\in N\}$

Lemma: If N is a normal subgroup, then $(aN)*(bN)=(ab)N$ is well-defined.

<u>Proof</u>

Suppose $a_1N=a_2N$ and $b_1N=b_2N$. Want to show that $a_1b_1N=a_2b_2N$ <=> $(a_1b_1)^{-1}a_2b_2\in N$ <=> $b_1^{-1}a_1^{-1}a_2b_2\in N$.

Since $a_2\in a_2N=a_1N$, there is $n_1\in N$ such that $a_2=a_1n_1$.

Since $b_2\in b_2N=b_1N=Nb_1$, there is $n_2\in N$ such that $b_2=n_2b_1$.

So, $b_1^{-1}a_1^{-1}a_2b_2=b_1^{-1}a_1^{-1}a_1n_1n_2b_1$

$=b_1^{-1}n_1n_2b_1$

$\in b_1^{-1}Nb_1\subseteq N$.

$\square$

Theorem: If N is any normal subgroup of G, then $G/N=\{gN\mid g\in G\}$ is a group under the operation $(aN)*(bN)=(ab)N$.

Remark: The identity is $eN=N$.

Fact: For any abelian group G, all subgroups are normal.

eg. $\mathbb{Z}_{12}/\langle 3\rangle$ is a group $= \{0+H, 1+H, 2+H\}$.