Lecture 8

mean 32/50

Some Recaps of midterm

2. d. Let G be a group of order 4, then G must be cyclic.

FALSE, $U(8)$

3.(a). $\alpha=(123)(2346)\in S_6$ $1\to2\to3\to1$, $2\to4\to6\to2$

$=(12)(346)(5)$

$|\alpha|=2\times3\times1=6$ (lcm of the length)

(b). ...

(c). How many elements of S_6 have order 6?
For part (b). we see $|\alpha|=6$ iff α has cycle type $(3,2,1)$ or (6)

We know there are $5!$ 6-cycles. If we pick a permutation $a_3\cdots a_6$ of $\{1,\cdots,6\}$. Then $(a_1,\cdots,a_6)$ is a 6-cycle
So there are $\frac{6!}{6}=5!$ 6-cycles

For type $(3,2,1)$

( ) ( ) ( )

3 2 1

$\frac{6\cdot5\cdot4}{3}\quad\frac{3\cdot2}{2}$

Answer $=240$

4.
a. let p be a prime #. What's the order of $U(p)$?

$|U(p)|=p-1$

b. Is $U(12)$ cyclic? Prove.
$U(12)=\{1,5,7,11\}=\{-5,-1,1,5\}$

Let's check if $U(12)$ has a generator of order 4.

$1:|1|=1$
$5:5^2=25\equiv1$ $|5|=2$
$-5:(-5)^2=25\equiv1$ $|-5|=2$
$-1:(-1)^2=1$ $|-1|=1$

$\Rightarrow$ No, not cyclic.

c. ...

5.b. For isomorphism, $\phi(a^i)=\phi(a^j) \iff a^i = a^j \iff n \mid (i-j)$

c. Let G_1 be a group of order 2. Then $G_1 = \{e, a\}$, where a denotes the unique element in G that is not identity.
Similarly, write $G_2 = \{e, b\}$.
In G, $a^2 \neq a$, so $a^2 = e$.
Similarly $b^2 = e$ in G_2.

Let $\phi : G_1 \to G_2$
$\phi(e) \to \phi(e)$
$\phi(a) \to \phi(b)$
Clearly it's a bijection. We just need to check that it is multiplicative.
$\phi(e \cdot a) = \phi(e) \cdot \phi(a)$
$\phi(a \cdot e) = \phi(a) \cdot \phi(e)$
$\phi(e \cdot e) = \phi(e) \cdot \phi(e)$
$\phi(a \cdot a) = \phi(a) \cdot \phi(a) = b^2 = e$
||
e

CH7 COSETS & Lagrange's Thm

Notation: Let G be a group and let $H \subseteq G$ be any subset. Let $a \in G$. We define the following sets:
$aH = \{ah \mid h \in H\}$
$Ha = \{ha \mid h \in H\}$
$aHa^{-1} = \{aha^{-1} \mid h \in H\}$ We will primarily use this notation when H is a sub-group.

Def'n: Let G be a group. Let $H \leq G$. $\forall a \in G$, call aH a left coset of H, and we call Ha a right coset of H.

In either case, we call "a" a coset representative of the coset aH (or Ha)

Notation:
$|aH|$ = # elements in aH
$|Ha|$ ... Ha

E.g.
① $G = S_3$, $H = \{e, (13)\}$
$eH = \{e, (13)\}$
$(12)H = \{(12), \underbrace{(12)(13)}_{(132)}\} = aH = (132)H$
$= (132)\{(13), e\}$
$= \{(12), (132)\}$

② $G=D_4$, $K=\{R_0, R_{180}\}$. $R_{90}K=\{R_{90}, R_{270}\}$
$VK=\{V, H\}$

$V\cdot R_{180}\left(\begin{smallmatrix}1&2\\4&3\end{smallmatrix}\right)$

$V\left(\begin{smallmatrix}3&4\\2&1\end{smallmatrix}\right)=\begin{smallmatrix}4&3\\1&2\end{smallmatrix}$

E.g. $G=S_3$, $H=\{e, (13)\}$

$(12)H=\{(12), (132)\}$
$H(12)=\{(12), \underbrace{(13)(12)}_{(123)}\}$

Important fact: In general, $aH\neq Ha$
(We will see that this will hold if H is normal).

E.g. Remark → if G is an additive group. We will write $a+H$ instead of aH and $H+a$ instead of Ha.

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

Properties of cosets.
Setup: G is a group, $H\leq G$, $a, b\in G$.
① $a\in aH$
② $aH=H$ iff $a\in H$
③ $(ab)H=a(bH)$ and $H(ab)=(Ha)b$
④ $aH=bH$ iff $a\in bH$
⑤ $aH=bH$ or $aH\cap bH=\emptyset$
⑥ $aH=bH$ iff $a^{-1}b\in H$
⑦ $|aH|=|bH|=|H|$
⑧ $aH=Ha$ iff $H=aHa^{-1}$
⑨ aH is a subgroup of G iff $a\in H$

Proof of some of statements
⑥ $\Rightarrow$ Sps $aH=bH$. Then $\forall h\in H$, $\exists\, h'\in H$ s.t. $ah=bh'$
Then $a^{-1}bh'=h$ $\Rightarrow a^{-1}b=h\cdot(h')^{-1}\in H$

$\Leftarrow$
Sps $a^{-1}b\in H$
Then $\forall h\in H$, $ah=a(a^{-1}b)(a^{-1}b)^{-1}h=b\underbrace{(a^{-1}b)^{-1}h}_{H \text{ by assumption}}\in bH$

So we've shown $aH\subseteq bH$. Similarly we can show $bH\subseteq aH$.

⑦ $|aH| = |H|$

Proof: Define $\varphi: H \to aH$ by $\varphi(h) = ah$
Then it's easy to verify that φ is a bijection. (Exercise).

⑨ Proof: $\Leftarrow$ If $a \in H$, then $aH = H$, which is a subgroup.
$\Rightarrow$ Sps aH is a subgroup, then $e \in aH$.
So $\exists h \in H$, s.t. $e = ah \Rightarrow a = h^{-1} \in H$.

Lagrange's Thm. $|H|$ divides $|G|$

Sps G is a finite group, and sps $H \leq G$.
Then $|H|$ divides $|G|$
Pf: Let $a_1H, \cdots, a_rH$ be the distinct cosets of G.
i.e. $G = a_1H \cup \cdots \cup a_rH$ and $a_iH \cap a_jH = \emptyset$ unless $i = j$
Then $|G| = |a_1H| + \cdots + |a_rH| = |H| + \cdots + |H| = r|H|$ ∎

E.g. $G = S_3$
$H = \{e, (12)\} = (12)H$
$(13)H = \{(13), \underbrace{(13)(12)}_{(123)}\} = (123)H$
$(23)H = \{(23), \underbrace{(23)(12)}_{(132)}\} = (132)H$

$a_1 = e, a_2 = (13), a_3 = (23)$

$a_1 = (12), a_2 = (13), a_3 = (132)$

Remark: We say that $|G| = |H| \cdot r$ where $r = \#$ of left cosets of H in G.

Def'n: The index of H in G, denoted $|G:H| = |G|/|H|$

Exercise: The # of right cosets of H in G is also equal to $|G:H|$.

Corollary: Let G be a finite group, and let $a \in G$, then $|a|$ divides $|G|$.

Proof: $|a| = |\langle a \rangle|$. By Lagrange's thm. $|\langle a \rangle|$ divides $|G|$ ∎

Cor: If G is a finite group and $a \in G$. Then $a^{|G|} = e$

Pf: By previous cor. $|G| = |a|k$ for some $k \in \mathbb{Z}$ and $k > 0$.
So $a^{|G|} = (a^{|G|})^k = e^k = e$ ∎

Cor. (Fermat's Little Thm)
$\forall a \in \mathbb{Z}$, $\forall$ prime p, $a^p \equiv a \bmod p$

Pf: If $a \equiv 0 \bmod p$, LHS $= 0^p = 0$, RHS $= 0$. True.
If $a \not\equiv 0 \bmod p$, then $a \in U(p)$, but $|U(p)| = p - 1$.
So by the previous Cor, $a^{p-1} \equiv 1 \bmod p$

Multiply by a on both sides, we have $a^p \equiv a \bmod p$. ▨

Remark: the converse of Lagrange's thm is not true.
If $k \mid |G|$, there does not exist a subgroup $H \leq G$ s.t. $|H| = k$

Counterexample: $G = A_4$, $|A_4| = 4!/2 = 12$.

Then we see $6 \mid |A_4|$. But there does not exist any subgroup of A_4 of order 6.

Thm: $H, K \leq G$, G is a finite group.
Define $HK = \{hk \mid h \in H, k \in K\}$ (In general, this is just some subset of G.)

Then $|HK| = \frac{|H|\,|K|}{|H \cap K|}$

Pf: Define a map $\phi: H \times K \longrightarrow HK$ $\quad \phi((h,k)) = hk$

Recall
$$H \times K = \{(h,k) \mid h \in H, k \in K\}$$

Then clearly ϕ is surjective

Define for $x \in HK$, $\phi^{-1}(x) = \{(h,k) \mid \phi(h,k) = x \text{ i.e. } hk = x\}$

Claim: $|\phi^{-1}(x)| = |\phi^{-1}(e)|$
Proof: write $x = \underline{h}\underline{k}$ for some fixed $\underline{h} \in H$, $\underline{k} \in K$.
Then define
$$\chi : \phi^{-1}(x) \to \phi^{-1}(e)$$
$$\chi((h,k)) = (h^{-1}\underline{h}, \underline{k}k^{-1})$$
To check χ is well-defined, suppose $(h,k) \in \phi^{-1}(x)$, i.e. $hk = x$

We know $\underline{h}\underline{k} = x$.
So $hk = \underline{h}\underline{k} \Rightarrow h^{-1}\underline{h}\,\underline{k}\,k^{-1} = e$
So $(h^{-1}\underline{h}, \underline{k}k^{-1}) \in \phi^{-1}(e)$.

ex: Prove χ is a bijection.

$$|HK| = \sum_{x \in HK} 1 = \sum_{(h,k) \in H \times K} \frac{1}{|\varphi^{-1}(hk)|} = \sum_{(h,k) \in H \times K} \frac{1}{|\varphi^{-1}(e)|}$$
$$= \frac{|H \times K|}{|\varphi^{-1}(e)|} = \frac{|H|\,|K|}{|\varphi^{-1}(e)|}$$

Claim: $|\phi^{-1}(e)| = |H \cap K|$

Pf: $\tau : \phi^{-1}(e) \to H \cap K$

$\tau(h,k) = h$

Since $(h,k) \in \phi^{-1}(e)$ iff $hk = e$, i.e. $h = k^{-1}$.

$h = k^{-1} \in K$. So $h \in H \cap K$

ex: τ is a bijection.

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

$$|HK| = \sum_{x \in HK} 1$$

General fact: If $f : X \to Y$ is a surjection, then $|Y| = \sum_{y \in Y} 1 = \sum_{x \in X} \frac{1}{|f^{-1}(f(x))|}$

$$= \sum_{y \in Y} \left(\sum_{x \in f^{-1}(y)} \frac{1}{|f^{-1}(y)|} \right)$$

Classification of Groups of order $2p$

Thm: Let p be a prime > 2. If G is a group of order $2p$, then either G is isomorphic to $\mathbb{Z}_{2p}$, or G is iso to D_p.

Pf: If G has an element of order $2p$, then G is iso to $\mathbb{Z}_{2p}$.

So assume it does not have an element of order $2p$. Then by a cor. of Lagrange's thm, all non-identity elements must have order 2 or p.

We want to prove $\exists$ at least one element of order p.

Sps o.w., i.e. $|x| = 2, \forall x \in G$, $x \neq e$.

Then if $a, b \in G$. Then $a^{-1} = a$, $b^{-1} = b$.

So $(ab)^{-1} = ab$

So $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$

Thus G is abelian. So if a, b are distinct non-identity elements, then $\{e, a, b, ab\}$ is a subgroup. Contradiction.

Let $a \in G$ be some element of order p. Let $b \in G$, where $b \notin \langle a \rangle$.

Then $|\langle a \rangle \cap \langle b \rangle| = 1$ since $|\langle a \rangle \cap \langle b \rangle| < p$ but it must divide p.

So by the previous thm, $|\langle a \rangle \langle b \rangle| = |\langle a \rangle||\langle b \rangle|$

Therefore, $G = \langle a \rangle \langle b \rangle$. Thus $|\langle b \rangle| = 2$.

So all elements of G look like

$a^k b^l$, where $l = 0$ and $k = 0, 1, 2, \cdots, p-1$

And $ab = ba^{-1}$

So define $\varphi : G \to D_p$

$\varphi(a) = R_{360°/p}$

$\varphi(a^k) = R_{(360°/p \cdot k)}$

$\varphi(b) =$ some inflection