Lecture 7

1. Find an isomorphism from the group of integers under addition to the group of even integers under addition.
2. Find Aut(Z).
3. Let $\mathbf{R}^+$ be the group of positive real numbers under multiplication. Show that the mapping $\phi(x) = \sqrt{x}$ is an automorphism of $\mathbf{R}^+$.
4. Show that $U(8)$ is not isomorphic to $U(10)$.
5. Show that $U(8)$ is isomorphic to $U(12)$.
6. Prove that the notion of group isomorphism is transitive. That is, if G, H, and K are groups and $G \approx H$ and $H \approx K$, then $G \approx K$.
7. Prove that S_4 is not isomorphic to D_{12}.
8. Show that the mapping $a \to \log_{10} a$ is an isomorphism from $\mathbf{R}^+$ under multiplication to $\mathbf{R}$ under addition.
9. In the notation of Theorem 6.1, prove that T_e is the identity and that $(T_g)^{-1} = T_{g^{-1}}$.
10. Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is Abelian.
11. For inner automorphisms ϕ_g, ϕ_h, and ϕ_{gh}, prove that $\phi_g \phi_h = \phi_{gh}$.
12. Find two groups G and H such that $G \not\approx H$, but Aut(G) $\approx$ Aut(H).

Midterm: 6pm – 8pm KP108 (Koffler House)
Cover: Chapters 1–6

Priority for the midterm
① Definitions ($U(n)$, $\mathbb{Z}_n$, S_n, ...)
② Understand the statements
③ Apply theorems
④ Proofs of some statements.

Also: the midterm will have true/false questions. But there is a guessing penalty.

There are 4 more classes after midterm, Chapter 7, 8, 9, 10 in those 4 weeks.
On 13th of Nov, HW2 is due.
27th Quiz 2

Question: Let G be a group, and let $a \in G$. Is the centralizer $C(a)$ always an Abelian group?
A: $C(a) = \{x \in G \mid ax = xa\}$

Sps G is a non-abelian group, then $C(e) = G$, which is not abelian.

Q: Compute all elements of order 6 in $\mathbb{Z}_{30}$.
A: $0 \Rightarrow 0^6 = 0$
$5 \Rightarrow 5^6 = 0$
$10 \Rightarrow 10^6 = 10^3 = 0$
$15 \Rightarrow 15^6 = 15^2 = 0$

Because 6 divides 30, we know there are $\varphi(6)$ elements of order 6 in $\mathbb{Z}_{30}$.
and $\varphi(6) = \varphi(3) \cdot \varphi(2)$
$= 2 \cdot 1$
$= 2$
and they are 5, 25

Def: $\varphi(n) = |U(n)| =$ # of integers between 0 & n-1 that are relatively prime

We have a theorem that says $\mathbb{Z}_{30}$ has a unique subgroup of order 6, namely
$\langle 30/6 \rangle = \langle 5 \rangle$
and $\langle 5 \rangle = \langle k \rangle$ iff $\gcd(5, 30) = \gcd(k, 30) = 5$
So we need to find all k s.t. $\gcd(k, 30) = 5$
The only possibilities are 5, 25.

Q: What are the orders of elements of $\mathbb{Z}_{31}$?

A: There is one element of order 1 (namely, 0)
And there are 30 elements of order 31.
b/c 31 divides 31, there are $\varphi(31)=30$ elements of order 31.

Q: What are the order of elements of $\mathbb{Z}_p$? p is prime.
A: 1 element of order 1,
p-1 .... order p.

Example: Find the elements of order 5 in $\mathbb{Z}_{10}$.
A: There are 4 elements. There is a unique subgroup of order 5:
$\langle 10/5\rangle = \langle 2\rangle = \{0,2,4,6,8\}$
When is $\langle 2\rangle = \langle k\rangle \Leftrightarrow \gcd(2,10) = \gcd(k,10)$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \| \quad 2$
As a consequence, $\langle 4\rangle = \langle 6\rangle$

True or False:
Let G be a finite group with $n=|G|$. and let k divide n.
Then $\exists$ a unique subgroup $S \leq G$ with $|S|=k$.
False (b/c it's not a cyclic group)

Find a finite group G s.t. (s.t.) there are distinct subgroups $S_1, S_2 \leq G$. $|S_1|=|S_2|$
Hint: Consider when $|S_1|=|S_2|=2$
Answer: In D_4, $S_1 = \{R_0, V\}$
$S_2 = \{R_0, H\}$

Question: Classify the orders of elements in D_4.
① order 1: 1 element, $\{R_0\}$
② order 2: 5 elements $\{R_{180}, H, V, D, D'\}$
③ order 3: none
④ order 4: $\{R_{90}, R_{270}\}$

Question: Classify all orders of elements in D_n.
① order 1: $\{R_0\}$
② order: case I (n is even), n+1 elements of order 2.
{all the reflections, R_{180}}
case II (n is odd), n elements of order 2
{all the reflections}
order n: S has $\varphi(n)$ elements of order n.
order k: S has $\varphi(k)$ elements of order k if k divides n
0 elements of order k if k not divides n.

Definition: Let $g \in G$ be an element of a group, we say g has order n if, it is the least positive integer s.t. $g^n = e$. If no such n exists, we say g has infinitive order.

Abelian Group: for a group G, we say that G is abelian if for all $a, b \in G$, $ab=ba$.

Center: let G be a group, the center of a group, $Z(G)$ is defined to be the set $\{a \in G \mid \forall x \in G, ax=xa\}$

Let G be a group, let $a \in G$, prove $C(a)$ is a subgroup of G.
recall: $C(a) = \{x \in G \mid xa = ax\}$
① $C(a)$ is not empty, clearly, $e \in C(a)$
② we want to show $C(a)$ is closed under multiplication.
For any $x, y \in C(a)$, $xy \in C(a)$.
Suppose $x, y \in C(a)$.
Then $xya = xay = axy \Rightarrow xy \in C(a)$
③ we want to show that $\forall x \in C(a), x^{-1} \in C(a)$.
Suppose $x \in C(a)$.
Then $xa = ax$, multiple by x^{-1} on left and right
$ax^{-1} = x^{-1}a \Rightarrow x^{-1} \in C(a)$

Q: How many elements in S_6 have order 5 ?
A: How many ways one can find $l_1, l_2, \cdots, l_k$ ($l_j = |C_j|$)
s.t. $l_1 + l_2 + \cdots + l_k = 6$
$\operatorname{lcm}(l_1, \cdots, l_k) = 5$
1 way : $\frac{6!}{5} = 144$

Q: How many elements of order 3 in S_4?
A: $4!/3 = 8$

Definition: we say a has cycle-type $(l_1, \cdots, l_k)$ if when we write a as a product $c_1, \cdots, c_k$ of disjoint cycles (many elements appear only once, we order things, so $|c_1| \leq |c_2| \leq \cdots \leq |c_k|$
if $(l_1, \cdots, l_k) = (|c_1|, |c_2|, \cdots, |c_k|)$