Lecture 10

1

Repetition: G group, N subgroup

$Na = \{na \,;\, n \in N\}$ is a right coset.

If $Na = aN$ for all $a \in G$, then we say that N is normal, and we may define multiplication by $Na \cdot Nb = Nab$.

Def: G/N is the set of all right cosets with operation $Na \cdot Nb = Nab$.

Theorem:
1. G/N is a group
2. G finite $\Rightarrow |G/N| = |G|/|N|$
3. G abelian $\Rightarrow G/N$ abelian

Proof: 1. Ass. and closure OK. Identity $Ne = N$, and $(Na)^{-1} = Na^{-1}$

2. $|G/N| = [G:N] = |G|/|N|$ by Lagrange's th.

3. Exercise. $\square$

G/N is called the quotient (factor) group of G by N.

Ex: (Book, page 167) $N = \{r_0, r_1, r_2, r_3\} \subseteq D_4$ is normal.

We have $Nr_0 = N$, $Nv = \{v, d, h, t\}$, so

2

$D_4 = Nr_0 \cup Nv$ and $D_4/N = \{Nr_0, Nv\}$

$r_0 \cdot r_0 = r_0$, $r_0 \cdot v = v \cdot r_0 = v$, $v \cdot v = r_0$

$\cdot$	Nr_0	Nv
Nr_0	Nr_0	Nv
Nv	Nv	Nr_0

We see that $D_4/N \cong \mathbb{Z}_2$ $\square$

Ex: $N = (\mathbb{Z}, +) \subseteq (\mathbb{Q}, +)$ is normal (subgroup of abelian gr.)

Note that $\mathbb{Z}$ not ideal in $\mathbb{Q}$, so we cannot construct the ring $\mathbb{Q}/\mathbb{Z}$. The group $\mathbb{Q}/\mathbb{Z}$ has infinite order (elements $r + \mathbb{Z}$, $r \in \mathbb{Q}$, $r \in [0,1[$), but every element in $\mathbb{Q}/\mathbb{Z}$ has finite order (exercise 15).

Theorem: G/N abelian $\Leftrightarrow aba^{-1}b^{-1} \in N$ for all $a, b \in G$.

Proof: G/N abelian $\Leftrightarrow Nab = NaNb = NbNa = Nba$

$\Leftrightarrow ab \equiv ba \pmod N \Leftrightarrow ab(ba)^{-1} = aba^{-1}b^{-1} \in N$ $\square$

Note: The subgroup generated by all $aba^{-1}b^{-1}$ is called the commutator subgroup.

Repetition: The center $Z(G) = \{a \in G \,;\, ag = ga \text{ for all } g \in G\}$ is a normal subgroup.

Theorem: $G/Z(G)$ cyclic $\Rightarrow G$ abelian

3

Proof: Let $C = Z(G)$ and assume Cd generates G/C.

$\Rightarrow G/C = \{(Cd)^k = Cd^k \,;\, k \in \mathbb{Z}\}$

$a \in G \Rightarrow a = e \cdot a \in Ca = Cd^i \Rightarrow a = c_1 d^i$ for some $c_1 \in C$

$b \in G \Rightarrow \cdot\ \cdot\ \cdot\ \cdot\ \cdot \Rightarrow b = c_2 d^j$ for some $c_2 \in C$.

We get $ab = c_1 d^i c_2 d^j = c_1 c_2 d^i d^j = c_2 c_1 d^j d^i =$
$= c_2 d^j c_1 d^i = ba$,

since c_1 and c_2 commutes with all elements. $\square$

Note: $G/Z(G)$ cyclic $\Rightarrow G$ abelian $\Rightarrow Z(G) = G$

$\Rightarrow G/Z(G) \cong \{e\}$

Def: Let $f: G \to H$ be a group homomorphism. The set $\ker f = \{a \in G \,;\, f(a) = e_H\}$ is called the kernel of f.

Theorem: $K = \ker f$ is a normal subgroup of G.

Proof: Subgroup:
- $a, b \in K \Rightarrow f(ab) = f(a)f(b) = e_H \cdot e_H = e_H$
  $\Rightarrow ab \in K$
- $a \in K \Rightarrow f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H$
  $\Rightarrow a^{-1} \in K$.

4

Normal: Show $a^{-1}ka \in K$ for all $a \in G$, $k \in K$.

$f(a^{-1}ka) = f(a)^{-1} f(k) f(a) = f(a)^{-1} e_H f(a) =$
$= f(a)^{-1} f(a) = e_H$
$\Rightarrow a^{-1}ka \in K$. $\square$

Theorem: f injective $\Leftrightarrow \ker f = \langle e_G \rangle$

Theorem: N normal in G. Then $\pi: G \to G/N$ def. by $\pi(a) = Na$ is a surjective homom. with kernel N.

Proofs: Copy proofs for rings.

Note: There is a 1-1-correlation between normal subgroups and kernel of homomorphisms.

Theorem (First isomorphism theorem):

Let $f: G \to H$ be a surj. hom. Then

$$G/\ker f \cong H.$$

Proof: Let $K = \ker f$ and define $\varphi: G/K \to H$ by $\varphi(Ka) = f(a)$.

Well-def: $Ka = Kb \Rightarrow ab^{-1} \in K \Rightarrow f(a)f(b)^{-1} =$

$= f(a)f(b^{-1}) = f(ab^{-1}) = e_H \Rightarrow f(a) = f(b)$

Homom.: $\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb)$

Surj.: Clear!

Inj: $f(a) = f(b) \Rightarrow f(a)f(b)^{-1} = e_H \Rightarrow f(a)f(b^{-1}) = e_H$
$\Rightarrow f(ab^{-1}) = e_H \Rightarrow ab^{-1} \in K \Rightarrow$ [redacted] $Ka = Kb$

Conclusion: φ isomorphism $\square$

Note: If f not surjective, then we have

$$G/\ker f \cong \operatorname{Im} f.$$

Ex: $N = \{a+bi;\ a^2+b^2 = 1\}$ is normal subgroup of $(\mathbb{C}^*, \cdot)$ (non-zero). Let $f : (\mathbb{C}^*, \cdot) \to (\mathbb{R}^{**}, \cdot)$ (positive) be defined by $f(a+bi) = a^2+b^2$. Then f is a surjective homomorphism (exercise 4).
Identity in $(\mathbb{R}^{**}, \cdot)$ is 1, so $\ker f = N$ and

$$(\mathbb{R}^{**}, \cdot) \cong (\mathbb{C}^*, \cdot)/N \quad \text{by F.I.Th.}$$

Subgroups of G/N:

Let N be a normal subgroup of G, and let K be a subgroup with $N \leq K \leq G$.

Theorem: ①: K/N is a subgroup of G/N
②: K/N normal in $G/N \Leftrightarrow K$ normal in G
③: T subgroup of $G/N \Rightarrow$ there exists subgroup $H \leq G$ such that $N \leq H$ and $T = H/N$.

Proof: ①: N normal in $G \Rightarrow N$ normal in $K \Rightarrow$
$\Rightarrow K/N$ group, and $K/N = \{Na;\ a \in K\} \subseteq \{Nb;\ b \in G\} = G/N$

②: K normal $\Rightarrow a^{-1}Ka \subseteq K$ for all $a \in G$.
Let $a \in G, k \in K$. Then $Na^{-1}NkNa = Na^{-1}ka = Nk_1$ for some $k_1 \in K$
$\Rightarrow Na^{-1}\, K/N\, Na \subseteq K/N \Rightarrow K/N$ normal.

[redacted] K/N normal $\Rightarrow Na^{-1}ka = Na^{-1}NkNa \in K/N$ for all $a \in G, k \in K \Rightarrow Na^{-1}ka = Nk_1$ for some $k_1 \in K \Rightarrow a^{-1}kak_1^{-1} \in N \subseteq K$
$\Rightarrow a^{-1}ka \in K \Rightarrow K$ normal

③: Let $H = \{a \in G;\ Na \in T\}$. Show that H is a subgroup of G:

$a, b \in H \Rightarrow Nab = NaNb \in T$ (since T subgroup) $\Rightarrow ab \in H$
$a \in H \Rightarrow Na^{-1} = (Na)^{-1} \in T$ (— " —) $\Rightarrow a^{-1} \in H$.

Now $a \in N \Rightarrow Na = Ne_G = e_{G/N} \in T \Rightarrow a \in H$,
so $N \subseteq H$

Furthermore $H/N = \{Na;\ a \in H\} = \{Na;\ Na \in T\} = T$ $\square$

Def: A group G $(\neq \langle e \rangle)$ is called simple if the only normal subgroups are $\langle e \rangle$ and G.

Theorem: G abelian and simple $\Leftrightarrow G \cong \mathbb{Z}_p$, p prime

Proof: $\Leftarrow$) Let $H \leq \mathbb{Z}_p$ be subgroup. By Lagrange's th. we have $|H| \,/\, |\mathbb{Z}_p| = p \Rightarrow |H| = 1$ or $|H| = p$
$\Rightarrow H = \langle e \rangle$ or $H = \mathbb{Z}_p$.

$\Rightarrow$) G abelian $\Rightarrow$ every subgroup is normal, so only subgroups of G are $\langle e \rangle$ and $G \Rightarrow$
$\Rightarrow$ for $e \neq a \in G$, $\langle a \rangle = G \Rightarrow G$ cyclic
$\Rightarrow G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}_n$.
It cannot be $\mathbb{Z}$, since it has many subgroups, and if $n = s \cdot t$, then $\langle a^s \rangle$ is a proper subgroup of $\mathbb{Z}_n \Rightarrow G \cong \mathbb{Z}_p$, p prime. $\square$

Note: There are not so many non-abelian simple groups: 5 of order ≤ 1000, 56 of order $\leq 10^6$.

Classification of finite groups using simple groups:
"Outline": Assume G finite and take normal subgroup $G_1 \neq G$ of largest order $\Rightarrow G/G_1$ simple (every normal subgroup of G/G_1 is of the form H/G_1, $G_1 \leq H \leq G$). If $G_1 \neq \langle e \rangle$, then take normal subgroup $G_2 \leq G_1$ of largest order, and so on. We will get

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = \langle e \rangle$$

with all composition factors G_i/G_{i+1} simple.

Jordan-Hölder theorem: Any two composition series are isomorphic (comp. factors independent of choice of G_i)

All finite simple groups are classified (1981)
(Proof > 10000 pages)