## Lecture 9

Assume $G$ group, $K$ subgroup and $a, b \in G$.

Def (congruence): $a$ is (right) congruent to $b$ modulo $K$, written $a \equiv_{(R)} b \pmod{K}$ if $ab^{-1} \in K$.

Note: With additive notation this is written $a - b \in K$

Note: $ab^{-1} \in K \iff ba^{-1} \in K$, since $(ba^{-1})^{-1} = ab^{-1}$, but $ab^{-1} \in K \not\Leftrightarrow a^{-1}b \in K$ in general.

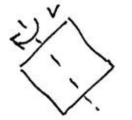
It can be proven that $\equiv_{(R)}$ is an equivalence relation, and thus we can define congruence classes

$$[a] = \{b \in G \,;\, b \equiv a \pmod{K}\} = \{b \in G \,;\, ba^{-1} \in K\} =$$
$$= \{b \in G \,;\, ba^{-1} = k,\, k \in K\} = \{b \in G \,;\, b = ka,\, k \in K\} =$$
$$\stackrel{\text{def.}}{=} Ka.$$

The congr. class $Ka$ is called a right coset of $K$.

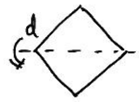
It can also be proven that two right cosets either are disjoint or identical.

Ex: Consider the dihedral group $D_4$ (see book, page 167). The set $K = \{r_0, v\}$ is a subgroup since $v \cdot v = r_0 = e$.






We also have




$$Kd = \{r_0 \cdot d, v \cdot d\} = \{d, r_3\}$$
$$dK = \{d \cdot r_0, d \cdot v\} = \{d, r_1\},$$

so in this case $Kd \neq dK$. □

Note: Here $dK$ is a left coset, which we obtain from left congruence: $a \equiv_{(L)} b \pmod{K} \iff a^{-1}b \in K$.

Ex: Let $I$ be an ideal (or subring) of a ring $R$. Then $(I, +)$ is a (abelian) subgroup of $(R, +)$. In this case we have $a + I = I + a$ for all $a \in R$. □

- Our next goal is to create a quotient group $G/K$ from right cosets. For that to work we need to define multiplication: $Ka \cdot Kb = Kab$.
  What property do we need for this to be well-defined?

Well-defined if $\left.\begin{array}{l} a \equiv_{(R)} b \pmod{K} \\ c \equiv_{(R)} d \pmod{K} \end{array}\right\} \Rightarrow ac \equiv_{(R)} bd \pmod{K}$,

i.e. $\left.\begin{array}{l} ab^{-1} \in K \\ cd^{-1} \in K \end{array}\right\} \Rightarrow ac(bd)^{-1} \in K$.

We "check": $ac(bd)^{-1} = acd^{-1}b^{-1}$, where $cd^{-1} = k_1 \in K$.



If $ak_1 = k_2 a$ for some other $k_2 \in K$, then

$$ac(bd)^{-1} = ak_1 b^{-1} = k_2 ab^{-1} = k_2 k_3 \in K, \text{ where } k_3 = ab^{-1} \in K.$$

Conclusion: We need that $aK = Ka$.

Def (normal): A subgroup $N$ of $G$ is called normal if $Na = aN$ for all $a \in G$.

Note: This means that for all $n_1 \in N$, there exists $n_2 \in N$ such that $n_1 a = an_2$. (Not necessarily that $na = an$ for all $n \in N$.)

Ex: Every subgroup of an abelian group is normal. □

It is not necessary though for a group to be abelian to have normal subgroups:

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

Ex: $N = \{r_0, r_1, r_2, r_3\}$ is a normal subgroup of $D_4$ (check!). In this case we have $Nv = vN$, but $nv \neq vn$ for all $e \neq n \in N$.

- Which is the easiest way to check whether a subgroup is normal or not?



**Theorem:** $N$ subgroup of $G$. The following are equivalent:

1. $N$ is normal
2. $a^{-1}Na \subseteq N$ for all $a \in G$ $\quad (a^{-1}Na = \{a^{-1}na \,;\, n \in N\})$
3. $a^{-1}Na = N$ for all $a \in G$

Proof: 1 ⇒ 2: $n \in N \Rightarrow a^{-1}na = a^{-1}an_1 = en_1 = n_1 \in N$

2 ⇒ 3: We need to show $N \subseteq a^{-1}Na$.
Assume $n \in N$. Then $n = a^{-1}(ana^{-1})a$, and
$n_1 = ana^{-1} = (a^{-1})^{-1}na^{-1} \in N$ by 2, so
$n = a^{-1}n_1 a \in a^{-1}Na$.

3 ⇒ 1: Assume $n_1 a \in Na$. Since $a^{-1}n_1 a = n_2 \in N$ by 3
$\Rightarrow n_1 a = a(a^{-1}n_1 a) = an_2 \in aN$, so $Na \subseteq aN$.
Same argument shows that $aN \subseteq Na$. □

---

- Again, $G$ group, $K$ subgroup and $Ka$ right coset.

**Theorem:**

1. $G = \bigcup_{a \in G} Ka$
2. $|Ka| = |Kb|$ for all $a, b \in G$.

Proof: 1: Clear, since $a = ea \in Ka$ for all $a \in G$.

5

2: Enough to show that $|Ka| = |K|$.

Define $f: K \to Ka$, via $f(x) = xa$. This function is surjective and injective (check!) $\Rightarrow$ $f$ bijective. □

**Def (index):** The index $[G:K]$ of $K$ in $G$ is the number of disjoint right cosets.

**Ex:** $\left[(\mathbb{Q},+) : (\mathbb{Z},+)\right] = \infty$, $\left[(\mathbb{Z},+), \langle 3 \rangle\right] = 3$.

**Theorem (Lagrange's th.):** If $G$ finite, then $|K|$ divides $|G|$ and $|G| = |K| \cdot [G:K]$.

**Proof:** If $[G:K] = n$, then $G = Ka_1 \cup Ka_2 \cup \cdots \cup Ka_n$ disjoint union of cosets and $|Ka_i| = |Ke| = |K|$ for all $i$. This means $|G| = [G:K] \cdot |K|$. □

**Corollary:** If $G$ is finite and $a \in G$, then

1. $|a| \,\big|\, |G|$
2. $|G| = k \Rightarrow a^k = e$.

**Proof:** 1: $|a| = n$. Now let $K = \langle a \rangle$. Since $|K| = n$, it follows that $n \,|\, |G|$.

2: $|a| = n \Rightarrow k = |G| = l \cdot n$ by 1 $\Rightarrow a^k = (a^n)^l = e^l = e$. □

(6)

- We will now make a classification of some finite groups:

**Theorem:** Assume $p$ prime. Every group of order $p$ is cyclic and isomorphic to $(\mathbb{Z}_p, +)$.

**Proof:** Let $e \neq a \in G$. We then have $|a| > 1$ and $|a| \,\big|\, |G| = p \Rightarrow |a| = |\langle a \rangle| = p$

$\Rightarrow G = \langle a \rangle \cong (\mathbb{Z}_p, +)$ (see lecture 8). □

**Note:** $G = \langle a \rangle$ for all $a \neq e$ in this case.

**Theorem:**

$$|G| = 4 \Rightarrow G \cong \mathbb{Z}_4 \text{ or } G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

**Proof:** If $G$ has element of order 4, then $G \cong \mathbb{Z}_4$.

Assume it has not. Then every $e \neq a \in G$ has order 2 (the order must divide 4).

We write mult. table:

| $\cdot$ | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | | |
| b | b | | e | |
| c | c | | | e |

no two elements in same row/column

$\Rightarrow$

| $\cdot$ | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

7

"Identical" table as for $\mathbb{Z}_2 \times \mathbb{Z}_2$ (see page 192), so $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

**Theorem:**

$$|G| = 6 \Rightarrow G \cong \mathbb{Z}_6 \text{ or } G \cong S_3.$$

**Proof:** 1) Assume $|a| = 2$ for all $e \neq a \in G$.

This means $a \cdot a = e \Rightarrow a^{-1} = a$ for all [redacted] $a \in G$.

$\Rightarrow ab = a^{-1}b^{-1} = (ba)^{-1} = ba \Rightarrow G$ abelian

$\Rightarrow K = \{e, a, b, ab\}$ subgroup (check!)

~~This means~~ But $4 = |K| \nmid |G| = 6$, a contradiction.

2) Assume there exists $a \in G$ with $|a| = 3$, and (and that no element has order 6) let $K = \langle a \rangle = \{e, a, a^2\}$. If $b \notin K$, then

$Kb = \{b, ab, a^2b\} \neq K \Rightarrow G = Ke \cup Kb =$

$= \{e, a, a^2, b, ab, a^2b\}$.

By "exclusion" we can now prove that $b^2 = e$ and $ba = a^2b$, and get a full mult. table (see book)

Comparing the table with the one for $S_3$, it follows that $G \cong S_3$.

3) If there is $a \in G$ with $|a| = 6$, then $G$ cyclic and $G \cong \mathbb{Z}_6$. □

8

Classification of finite groups up to order 7:

| $\lvert G\rvert$ | abelian | non-abelian |
|---|---|---|
| 1 | $\{e\}$ | |
| 2 | $\mathbb{Z}_2$ | |
| 3 | $\mathbb{Z}_3$ | |
| 4 | $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ | |
| 5 | $\mathbb{Z}_5$ | |
| 6 | $\mathbb{Z}_6$ | $S_3$ |
| 7 | $\mathbb{Z}_7$ | |