problem session for Section 8.1

Problem Session Section 8.1

23 p246 G has more than one element, and has no proper subgroups
(57 p213) Prove $G \simeq \mathbb{Z}_p$ for a prime p.

Let $a \in G$, $a \neq e$. Consider $\langle a \rangle \subseteq G$.
Since G has no proper subgroups, $\langle a \rangle = G$.
Let $|a| = |\langle a \rangle| = n$. If n is not a prime, say $n = km$, $(k, m) = 1$,
then $\langle a^k \rangle \subset \langle a \rangle$ is a proper subgroup: $|\langle a^k \rangle| = m$.
Thus $n = p$ is a prime, and $G = \langle a \rangle = \mathbb{Z}_p$.

24 p246 $|G| = 25$
Prove that G is either cyclic, or else every non-identity element has order 5

Pf. Assume that G is not cyclic.
Let $a \neq e$, $a \in G$. Wanted: $|a| = 5$
Consider $\langle a \rangle \subseteq G$, subgroup generated by a.
$\langle a \rangle \neq G$ because G is assumed to be not cyclic.

Lagrange thm implies that $|\langle a\rangle| \mid |G|$

$|a| \mid 25$

The only option is $|a| = 5$

25 p246 $a \in G$, $|a| = 30$ Wanted: the index of $\langle a^4\rangle$ in $\langle a\rangle$

$|\langle a\rangle| = 30$

$\langle a^4\rangle \subseteq \langle a\rangle$

$|\langle a^4\rangle| \mid 30$

Let us find the order of $|\langle a^4\rangle| = |a^4|$

$(a^4)^{15} = a^{60} = (a^{30})^2 = e^2 = e$

By Th 7.9, it follows that $|a^4| \mid 15$

Option for $|a^4|$ (divisors of 15): 1 - no, because $|a| = 30$

3 - $(a^4)^3 = e$ $a^{12} = e$ - no; $30 \nmid 12$

5 - $(a^4)^5 = e$ $a^{20} = e$ - no; $30 \nmid 20$

15 - $(a^4)^{15} = a^{60} = e$

Found: $|a^4| = 15$

$[\langle a\rangle : \langle a^4\rangle] = \frac{30}{15} = 2$

---

29 p 246   G - finite ;   H, K - subgroups of G,

$K \subseteq H \subseteq G$

Prove that $[G:K] = [G:H][H:K]$

Pf

All info from Lagrange's thm (Th 8.5)

$[G:K]\,|K| = |G|$ $[G:K] = |G|/|K|$

$[G:H]\,|H| = |G|$

$[H:K]\,|K| = |H|$

$[G:H][H:K]\,|K| = |G|$

$[G:H][H:K] = |G|/|K|$

36 p 247   G - finite group, H, K - subgroups of G

$[G:H] = p$ $[G:K] = q$;   p and q are distinct primes

Prove that pq divides $[G: H\cap K]$

Pf $G \supseteq H \supseteq H\cap K$ $G \supseteq K \supseteq H\cap K$

$$[G:H\cap K] = \underbrace{[G:H]}_{p}[H:H\cap K] \qquad [G:H\cap K] = \underbrace{[G:K]}_{q}[K:H\cap K]$$

$$p \mid [G:H\cap K] \qquad q \mid [G:H\cap K]$$

By the Fundamental Thm of Arith (p and q are distinct primes)

$$pq \mid [G:H\cap K]$$

---

30 p246 (cf. 29 p246)

G is not necessarily finite.

$$K \subseteq H \subseteq G$$

Assume that the indeces $[G:H]$ and $[H:K]$ are finite.

Prove that $[G:K]$ is finite, and

$$[G:K] = \underbrace{[G:H]}_{n}\underbrace{[H:K]}_{m}.$$

Pf

$\vee$ $G = \bigcup\limits_i Ha_i = Ha_1 \cup Ha_2 \dots \cup Ha_n$ — union of non-overlapping subsets (cosets)

$H = \bigcup\limits_j Kb_j = Kb_1 \cup Kb_2 \dots \cup Kb_m$ ——— // ———

$\checkmark$ $Ha_i = \{ha_i \mid h \in H\} = \{ha_i \mid h \in Kb_j \text{ for some } j\}$

$$= \bigcup_{j=1}^{m} \{kb_j a_i \mid k \in K\} \qquad \Big\} \; Ha_i = \bigcup_{j=1}^{m} \; \bar{m}_i$$

$$= \bigcup_{j=1}^{m} Kb_j a_i$$

these are non-overlapping subsets of Ha_i

$$k_1 b_j a_i = k_2 b_{j'} a_i$$

$$k_1 b_j = k_2 b_{j'}$$

b_j and b_j belong to the same K-coset, that is $j = j'$

We thus have a union of non-overlapping subsets:

$$G = \bigcup_{i,j} Kb_j a_i$$

- the right coset decomposition of the group G with respect to a subgroup K:

$$G = \bigcup_{c \in G} Kc$$

The amount of cosets

$[G:H] = n\,m = [G:H][H:K]$

$i = 1, \dots n$

$j = 1, \dots m$

34 p247 G - abelian group of odd order

$|G| = n$, $G = \{a_1, \dots, a_n\}$ - list of (distinct) elements.

Prove that $a_1 \dots a_n = e$

Pf

1-st way - partion the list $\{a_1, \dots, a_n\}$ into pairs $\{a, a^{-1}\}$

$$a_1 \dots a_n = b_1 \dots b_k \qquad b_i = b_i^{-1}$$

If $b = b^{-1}$, then $b^2 = e$, thus $|b| = 2$, and $|\langle b \rangle| = 2$
or $b = e$

$|\langle b \rangle| = 2$ cannot happen because $\langle b \rangle$ is a subgroup of G,
but $|G|$ is odd, and $|\langle b \rangle| = 2$
would contradict Lagrange's thm.

Thus $a_1 \dots a_n = e$

2-nd way

Consider $\{a_1^{-1}, a_2^{-1}, \dots a_n^{-1}\}$ - this is also a full list
of distinct elements of G.

Thus $a_1 \dots a_n = a_1^{-1} \dots a_n^{-1}$ (this is a permutation of the same list of elements; G is abelian)

$= (a_1 \dots a_n)^{-1}$

As before, if $a_1 \dots a_n \neq e$,

then $|\langle a_1 \dots a_n \rangle| = 2$ ← that cannot happen.

<u>37 p247</u> $|G| = n$, G is abelian g.c.d. $(k, n) = 1$

$$f : G \longrightarrow G \qquad a \longmapsto a^k$$

is an <u>isomorphism</u>

① homomorphism $f(uv) = (uv)^k \underset{G \text{ is abelian}}{=} u^k v^k = f(u) f(v)$

② bijection

Since G is finite, <u>injective</u> would suffice

For injectivity (Th 8.17), we show that kernel consists of nothing but $e \in G$.

$a \in \ker(f)$ means $f(a) = e$ $\quad a^k = e$

$|a| = |\langle a \rangle| \mid k$ by Th 7.9 (from $a^k = e$)

$|a| = |\langle a \rangle| \mid n$ because $\langle a \rangle$ is a subgroup in G.

Since g.c.d. $(k, n) = 1$,

the two divisibilities imply $|a| = 1$, that is $a = e$.