Chap 16: The fundamental homomorphism theorem.

Chap 15: $H \triangleleft G \Rightarrow$ the quotient group G/H is a homomorphic image of G under the canonical homomorphism $f: G \to G/H$

$$g \mapsto gH$$

Conversely, we want to show that any homomorphic image of G is a quotient group.

Thm 1.: Let $f: G \to H$ be a homomorphism with kernel K. Then.

$$f(a) = f(b) \text{ iff } Ka = Kb$$

Pf: $f(a) = f(b) \Leftrightarrow f(ab^{-1}) = f(a) \cdot f(b)^{-1} = e_H \Leftrightarrow ab^{-1} \in K \Leftrightarrow \underset{(aK}{Ka} = \underset{bK)}{Kb}$

This says that if f is a homomorphism from G to H with kernel K, then

(i) all the elements in any fixed coset of K have the same image.

(ii) conversely, elements which have the same image are in the same coset of K.

Thm 2: Let $f: G \to H$ be a homomorphism of G $\boxed{\text{onto}}$ H. If $K = \ker(f)$, then

$$H \cong G/K$$

Pf: Consider the map: $\phi: G/K \to H$

$$Ka \mapsto f(a).$$

Thm 1 implies that this is well defined: $Ka = Kb \Rightarrow f(a) = f(b)$

- ϕ is injective: $f(a) = f(b) \overset{\text{Thm 1}}{\Longrightarrow} Ka = Kb$.
- ϕ is surjective: f is onto $\Rightarrow \forall h \in H, \exists a \in G$ s.t. $f(a) = h \Rightarrow \phi(Ka) = h$.
- ϕ is homomorphism: $\phi(Ka \cdot Kb) = \phi(Kab) = f(ab)$

$$\phi(Ka) \cdot \phi(Kb) = f(a) f(b) = f(ab)$$

$\Rightarrow \phi$ is an isomorphism.

Thm 2 is called the fundamental homomorphism theorem: symbolically we write:

If $f: G \xrightarrow[K]{} \!\!\!\!\to H$ then $H \cong G/K$.

Ex: A. 1. $f: \mathbb{Z}_{20} \to \mathbb{Z}_5$ $\quad \ker(f) = \langle \bar{5} \rangle = \{0, \bar{5}, \overline{10}, \overline{15}\} \cong \mathbb{Z}_4$

$\bar{n}^{20} \mapsto \bar{n}^5$ $\quad \Rightarrow \mathbb{Z}_5 \cong \mathbb{Z}_{20}/\langle \bar{5} \rangle$.

Ex: $f: \mathbb{Z} \to \mathbb{Z}_q$ $\quad \ker(f) = \langle q \rangle \cong \mathbb{Z}$

$n \mapsto \bar{n}$ $\quad \Rightarrow \mathbb{Z}_q = \mathbb{Z}/\langle q \rangle = \mathbb{Z}/q\mathbb{Z}$.

C. G abelian group. $H = \{x^2 : x \in G\}$. $K = \{x \in G : x^2 = e\}$

1. $f(x) = x^2$ is a homomorphism of G onto H: $f(xy) = (xy)^2 \overset{G \text{ is abelian}}{=} x^2 y^2 = f(x) f(y)$
2. $\ker(f) = \{x \in G : x^2 = e\} = K$
3. $H = \operatorname{Im}(f) = G/\ker(f) = G/K$.

F. G a group. $H \lhd G$, $K < G$.

1. $H \cap K$ is a normal subgroup of K: $H \cap K < K$

$\forall x \in K, \forall a \in H \cap K$. $\quad x \cdot a \cdot x^{-1} \in H$ because $H \lhd G$ $\Rightarrow x a x^{-1} \in H \cap K$

$x a x^{-1} \in K$ because $x, a \in K$. $\quad \Rightarrow H \cap K \lhd K$

2. $HK = \{xy : x \in H \text{ and } y \in K\}$, then HK is a subgroup of G.

Pf: $(x_1 y_1)(x_2 y_2) = x_1 (y_1 x_2 \cdot y_1^{-1}) y_1 y_2 \in HK$

$(xy)^{-1} = y^{-1} x^{-1} = (y^{-1} x^{-1} y) \cdot y^{-1} \in H \cdot K$

3. H is a normal subgroup of HK

Pf: $H < HK$, $H \lhd G$ $\Rightarrow H \lhd HK$

4. $HK/H = \{ H\cdot h\cdot k = Hk \, ; \, k \in K \}$.

5. $f: K \longrightarrow HK/H$ is a homomorphism. $f(k_1 k_2) = Hk_1k_2 = Hk_1 \cdot Hk_2 = f(k_1)f(k_2)$

$k \mapsto Hk$ $\quad$ f is onto: by 4. $Hk = f(k)$

6. $\ker(f) = \{ k \in K ; f(k) = Hk = H \} = \{ k \in K ; k \in H \} = H \cap K$

By the FHT, $K/_{H\cap K} = HK/_H$

k. Cauchy's thm: If G is a group and p is any prime divisor of $|G|$, then G has at least one element of order p.

Case 1: G is abelian (Chap 13. Exer H4).

use induction on $|G|$: • If $|G|=1$. this is true

• let $|G|=k$ and suppose our claim is true for every abelian group whose order is less than k. Let p be a prime factor of k.

Take any element $a \neq e$. If $ord(a) = p$ or a multiple of p then we are done:

1. $ord(a) = tp \Rightarrow ord(a^t) = p$.

2-3 suppose $ord(a)$ is not equal to a multiple of p. Then $G/\langle a\rangle$ is a gp. having fewer than k elements. and $p \mid |G/\langle a\rangle|$. By induction $G/\langle a\rangle$ has an elem of order p

4. $\exists \ \langle a\rangle x \in G/\langle a\rangle$ s.t. $ord(Hx) = p$.

$\langle a\rangle = H$

$ord(Hx) \mid ord(x)$: $x^r = e \Rightarrow (Hx)^r = Hx^r = H$

$\Rightarrow p \mid ord(x) \Rightarrow ord(x) = p\cdot s$

$\Downarrow$

$ord(x^s) = p$.

Case 2: G is not abelian. Again use induction. $|G|=1$ case is true.

let $|G|=k$ and suppose our claim is true for any group of order less than k.

let C be the center of G. and C_a the centralizer of a for each $a \in G$.

let $k = c + k_s + \cdots + k_t$ be the class equation of G: ($k_s, \cdots, k_t$ are the sizes of all distinct conjugacy classes of elements $x \notin C$).

1. If p is a factor of $|C_a|$ for any $a \in G$, where $a \notin C$, we are done.

Because: $a \notin C \Rightarrow C_a \neq G \Rightarrow |C_a| < G$. by induction we are done

2. Prove that for any $a \notin C$ in G. if p is not a factor of $|C_a|$, then p is a factor of $(G:C_a)$:

Pf: $|G| = |C_a| \cdot |(G:C_a)|$, $\left.\begin{matrix} p \mid G \\ p \nmid |C_a| \end{matrix}\right\} \Rightarrow p \mid (G:C_a)$

3. Solving the equation $k = c + k_s + \cdots + k_t$ for $c \Rightarrow c = k - k_s - \cdots - k_t$

$p \mid k$. by 1. we assume $p \nmid |C_a|$. $\forall a \notin C$. then

by 2, we have $p \mid (G:C_a)$ $\forall a \notin C \Rightarrow p \mid k_s, \cdots, p \mid k_t$

$\Rightarrow p \mid (c = |C|)$

Since G is nonabelian, $C \lneqq G$. so by induction, $\exists x \in C$ s.t. $x^p = e$. we are done.

L. Prelude to Sylow.

Let p be a prime number. A p-group is any group whose order is a power of p. It will be shown that

Thm: If $|G| = p^k$, then G has a normal subgroup of order p^m for every m between 1 and k. The proof is by induction on G. we therefore assume our result is true for all p-groups smaller than G.

1. Prove: there is an element a in the center of G s.t. $\operatorname{ord}(a) = p$

Pf: By Chap 15. Exer G: C = center of $G \neq \{e\}$.

$C \triangleleft G \Rightarrow |C| \mid |G| = p^k \Rightarrow C$ is a p-group, abelian. By Cauchy's thm. (for Abelian groups, Chap 15. Exer H), there is an element $\underset{\in C}{a}$ with $\operatorname{ord}(a) = p$.

2.2 $\langle a \rangle$ is a normal subgroup: $\forall g \in G$, $a^k \in \langle a \rangle \subset C$

$g a^k g^{-1} = a^k \Rightarrow \langle a \rangle \triangleleft G$.

2.3. $|G/\langle a \rangle| = \frac{|G|}{|\langle a \rangle|} = \frac{|G|}{p} = p^{k-1} < p^k$. By induction, $\exists$ normal subgp. of order p^{m-1}.

2.3. $G \to G/\langle a \rangle$ $\quad \bar{H} \triangleleft G/\langle a \rangle \Rightarrow p^{-1}(\bar{H}) = H \triangleleft G$

with $|p^{-1}(\bar{H})| = |H| \cdot |\langle a \rangle| = p^{m-1} \cdot p = p^m$.