Lecture 1 : Basic facts

Def A monoid is an ordered pair $(M, *)$, where M is a set and $*$ is a function

$$M * M \longrightarrow M$$
$$(x, y) \longmapsto *(x,y) =: x * y,$$

such that

M1. $\exists\, e \in M : \forall\, x \in M : \quad e * x = x * e = x$

M2. $\forall\, x, y, z \in M : \quad (x * y) * z = x * (y * z)$

If e' is s.t. (M1), then $e' = e' * e = e$. The such element is unique; we call it the neutral element of the monoid.

Defn A group is a monoid $(G, *)$ s.t.

G. $\forall\ x \in G\ \exists\ x' \in G : \quad x * x' = x' * x = e.$

Here e denotes the neutral element of $(G, *)$.

Given $x \in G$, if x'' r.b. (G), then

$$x' = e * x' = (x'' * x) * x' = x'' * (x * x') = x'' * e = x''.$$

Thus there is exactly one element x' r.t. (G) and we call it the inverse of x. We say that G is abelian if

$$\forall\ x, y \in G : \quad x * y = y * x.$$

Def: Given monoids $(M, *)$ and $(M', *')$, a monoid homomorphism from the former to the latter is a map

$f: M \longrightarrow M'$ s.t.

MH1 $\quad f(1_M) = 1_{M'}$

MH2. $\forall\ x, y \in M : f(x * y) = f(x) *' f(y)$

If G and G' are groups, a *group homomorphism* is just a monoid homomorphism

$$f: G \longrightarrow G'.$$

Remark For group homomorphisms (MH2) $\Longrightarrow$ (MH1).

Indeed, $f(1_G) = f(1_G * 1_G) = f(1_G) * f(1_G) \Longrightarrow 1_{G'} = f(1_G)$

Defn We say that $H \subseteq G$ is a subgroup of G if defines a group

$$H \times H \longrightarrow H$$

$$(h_1, h_2) \longmapsto h_1 h_2$$

structure on H and we write $H \leq G$.

Lemma If $H \leq G$ then

$$G/H := \{ gH : g \in G \}$$

is a partition of G into cosets $gH := \{ gh : g \in G \}$.

Proof

[Ex.]

Definition Given a group G and a subgroup $H \subseteq G$, the index of H in G is the cardinality of the set G/H.

It is denoted $[G:H] := |G/H|$.

Theorem (Lagrange) If G is a finite group and $H \subseteq G$ is any subgroup, then $|G| = |H| \cdot [G:H]$.

Proof

The above lemma implies that $\exists\ g_1, \dots, g_{[G:H]} \in G$ s.t

$$G = \bigcup_{i=1}^{[G:H]} g_i H \quad \& \quad g_i H \cap g_j H \ (i \neq j).$$

We immediately get

$$|G| = \sum_{i=1}^{[G:H]} |g_i H| \qquad (*)$$

But for each $g \in G$ we have a bijective map

$$H \longrightarrow gH$$
$$h \longmapsto gh$$

Therefore $|H| = |gH|$, so $(*)$ yields

$$|G| = \sum_{i=1}^{[G:H]} |H| = |H| \cdot [G:H]. \qquad \square$$

We say that a subgroup $N \leq G$ is *normal* if

$$\forall\, g \in G: \quad gNg^{-1} = N$$

and express this by writing $N \trianglelefteq G$.

Lemma If $N \trianglelefteq G$, then G/N has a natural group structure and

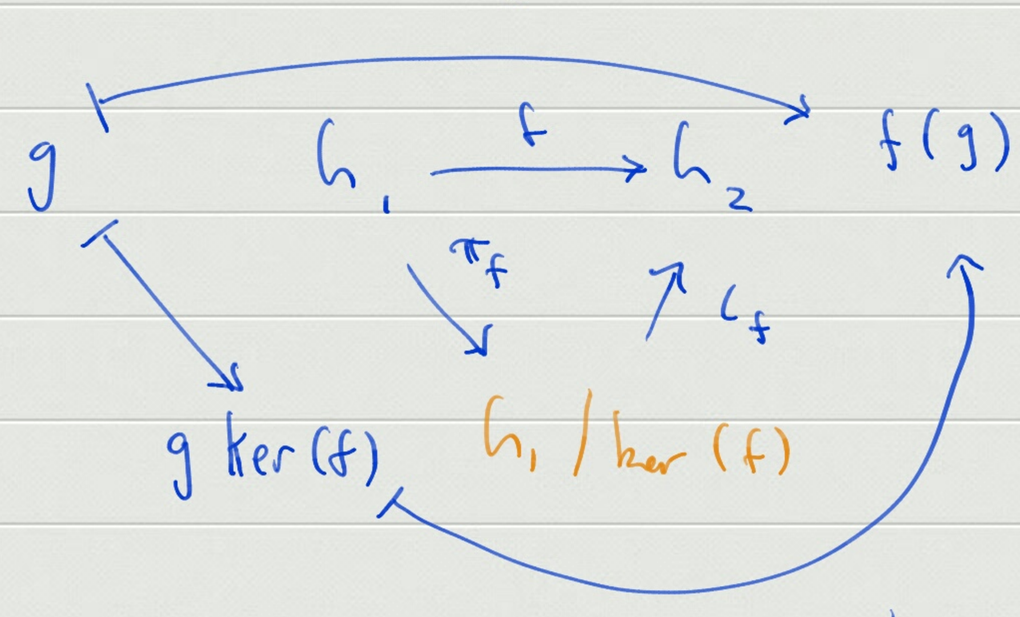
$$\begin{aligned} G &\xrightarrow{\pi} G/N = \{gN \mid g \in G\} \\ g &\longmapsto gN \end{aligned}$$

is a group homomorphism.

Let $G_1 \xrightarrow{f} G_2$ be a group homomorphism. The kernel of f is defined by

$$N := \ker(f) = \{ x \in G_1 : f(x) = 1_{G_2} \} \trianglelefteq G.$$

Moreover, f factors as a surjection followed by an injection:



The factorisation $f = \iota_f \circ \pi_f$ is known as the first isomorphism thm.

Lemma If $|G| < \infty$, then $\forall\, g \in G : g^{|G|} = 1$.

Proof

Let $g \in G$. There is exactly one group homomorphism

$$\mathbb{Z} \xrightarrow{\varphi_g} G$$

that maps $1 \mapsto g$. The first isomorphism thm gives

$$g^{\mathbb{Z}} \cong \mathbb{Z}/m\mathbb{Z} \qquad (\text{some } m \in \{2,3,\dots\})$$

so $g^m = 1_G$. Write $H := g^{\mathbb{Z}}$, so Lagrange's thm implies that $|G| = |H|\,[G:H]$. Therefore

$$g^{|G|} = (g^m)^{[G:H]} = 1 \qquad \square$$