Definitions and Theorems

2-5: Basic properties of groups

Definitions

Def: $*$ is a *binary operation* on a set G if $\forall x, y \in G,\ x * y \in G$

Def: Let G be a set, and let $* : G \times G \to G$ be a *binary operation* on G. Suppose

1. $*$ is *associative*, i.e., $\forall x, y \in G,\ (x * y) * z = x * (y * z)$
2. $*$ has an *identity element*, i.e., $\exists e \in G$ s.t. $\forall x \in G,\ x * e = e * x = x$
3. $*$ has *inverses*, i.e., $\forall x \in G,\ \exists y \in G$ s.t. $x * y = y * x = e$

We then say that $(G, *)$ is a *group*. If $(G, *)$ is a group and $*$ is *commutative*, we say G is an *abelian group*.

Theorems

Lemma: (division algorithm) Let $a, n \in \mathbb{Z}$ with $n \geq 1$. Then $\exists! q, r \in \mathbb{Z}$ s.t.

1. $a = qn + r$
2. $0 \leq r \leq n - 1$

Prop: Let G be a group.

1. The identity element e is unique
2. $\forall x \in G$, the inverse x^{-1} is unique

Prop: Let G be a group. Then

1. $\forall x \in G,\ (x^{-1})^{-1} = x$
2. $\forall x, y \in G,\ (xy)^{-1} = y^{-1}x^{-1}$

Prop: Let G be a group.

1. If $x, y \in G$ s.t. $xy = e$, then $x = y^{-1}$ and $y = x^{-1}$
2. If $x, g \in G$ s.t. $xg = x$ (or $gx = x$), then $g = e$

Prop: (cancellation laws) Let G be a group, and $x, y, z \in G$. Then

1. If $xy = xz$, then $y = z$
2. If $yx = zx$, then $y = z$

Corollary: Let G be a group with $g \in G$. Define $f_1, f_2 : G \to G$ by $f_1(x) = gx,\ f_2(x) = xg$. Then f_1 and f_2 are 1 to 1 and onto.

Corollary: (stated differently) Let G be a group, $g \in G$. Then $\forall y \in G$,

1. $\exists! x_1 \in G$ s.t. $gx_1 = y$
2. $\exists! x_2 \in G$ s.t. $x_2 g = y$