FPM Algebra

Marie Biolkova

Functions

Proving functions: if $x = y$ then $f(x) = f(y)$.
A function $f : X \to Y$ is called

- *injective* if $f(x_1) = f(x_2)$ implies that $x_1 = x_2$.
- *surjective* if for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$.
- *bijective* if it is both injective and surjective.

Group Axioms

We say that a nonempty set G is group under * if

1. (Closure) * is an operation, so $g * h \in G$ for all $g, h, \in G$.
2. (Associativity) $g * (h * k) = (g * h) * k$ for all $g, h, k \in G$.
3. (Identity) There exists an *identity element* $e \in G$ such that $e * g = g * e = g$ for all $g \in G$.
4. (Inverses) Every element $g \in G$ has an inverse g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Subgroups

A *proper subgroup* is a subgroup that is not the group itself (sometimes denoted $H < G$). If $H \leq G$ then $e_H = e_G$ and the inverse of $h \in H$ equals the inverse of h in G.

Test for a Subgroup

We say $H \subseteq G$ is a subgroup of G if and only if

1. H is not empty.
2. If $h, k, \in H$ then $h * k \in H$.
3. If $h \in H$ then $h^{-1} \in H$.

Lagrange and Co.

Lagrange's Theorem Let G be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.

- Let $g \in G$. Then $o(g)$ divides $|G|$.
- For all $g \in G$ we have $g^{|G|} = e$.
- If $|G| = p$ where p is prime then G is cyclic.
- If $|G| < 6$ then G is abelian.
- A *left coset* is a subset of G of the form gH.
- A *right coset* is a subset of G of the form Hg.
- If $gH = Hg$ for all $g \in G$ then we say the subgroup is normal.
- We denote the set of left cosets of H in G by G/H.
- The *index* of $H \leq G$ is the number of distinct left cosets of H in G and $|G/H| = \frac{|G|}{|H|}$.

Fermat's Little Theorem If p is a prime and $a \in \mathbb{Z}$ then $a^p \equiv a \mod p$.

Homomorphisms and Isomorphisms

Let G, H be groups. A map $\phi : G \to H$ is a group *homomorphism* if

$$\phi(xy) = \phi(x)\phi(y) \text{ for all } x, y \in G.$$

(Product xy on the left is the group operation in G and the product $\phi(x)\phi(y)$ is formed using group operation in H.)
If the map is bijective then it is called an *isomorphism*.

- The *image* of ϕ is im $\phi = \{h \in H | h = \phi(g)$ for some $g \in G\}$.
- The *kernel* of ϕ is ker $\phi = \{g \in G | \phi(g) = e_H\}$.
- im ϕ is a subgroup of H.
- ker ϕ is a subgroup of G.
- Kernels of homomorphisms are normal subgroups.
- If $\phi : G \to H$ is an isomorphism then so is $\phi^{-1} : H \to G$.
- $\phi : G \to H$ is injective iff ker $\phi = \{e\}$.
- If $\phi : G \to H$ is injective then ϕ gives an isomorphism $G \cong$ im ϕ.
- All cyclic groups of order n are isomorphic, in particular every group of order 2 is isomorphic to $\mathbb{Z}_2$.
- Let $H, K \leq G$ with $H \cap K = \{e\}$. Then $\phi : H \times K \to HK$ given by $\phi : (h, k) \mapsto hk$ is bijective. If also $hk = kh$ for all $h \in H, k \in K$ then HK is a subgroup of G isomorphic to $H \times K$ via ϕ.

Group Actions

Let G be a group and X an non empty set. Then a left action of G on X is a map $G \times X \to X$ such that

$$g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \text{ and } e \cdot x = x$$

for all $g_1, g_2 \in G, x \in X$.

- The *kernel* of an action is the set $N = \{g \in G | g \cdot x = x$ for all $x \in X\}$.
- If $N = \{e\}$ (kernel is trivial) then we say the action is *faithful*.

Orbit-Stabilizer

Let G act on X and let $x \in X$. The *stabilizer* of x is

$$\mathrm{Stab}_G(x) = \{g \in G | g \cdot x = x\}$$

and the *orbit* of x under G is

$$\mathrm{Orb}_G(x) = \{g \cdot x | g \in G\}.$$

- The stabilizer is a subgroup of G.
- Orbits partition the set X.
- The kernel is the intersection of stabilizer subgroups, i.e. $\cap_{x \in X} \mathrm{Stab}_G(x)$.

Orbit-Stabilizer Theorem Let G be a finite group acting on X, let $x \in X$. Then

$$|\mathrm{Orb}_G(x)| \times |\mathrm{Stab}_G(x)| = |G|.$$

Cauchy's Theorem If a prime p divides $|G|$ then G contains an element of order p.

- An action is *transitive* if for all $x, y \in X$ there exists $g \in G$ such that $y = g \cdot x$. Equivalently, X is a single orbit under G.
- $\mathrm{send}_x(y) = \{g \in G | g \cdot x = y\}$
- $\mathrm{Fix}(g) = \{x \in X | g \cdot x = x\}$ is the *fixed point set*.
- The number of orbits in $X = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$.

Conjugacy Classes

Let $g, h \in G$, then $h \cdot g = hgh^{-1}$ defines an action of group G on itself (*conjugation action*).

- The orbits are called *conjugacy classes*.
- We say g_1, g_2 are *conjugate* if there exists $h \in G$ such that $g_2 = hg_1h^{-1}$, i.e. if they lie in the same conjugacy class.
- If G is abelian then each element is its own conjugacy class.
- $C(g) = \{h \in G | gh = hg\}$ is the *centralizer* of g in G and it is a subgroup of G.
- $C(G) = \{g \in G | gh = hg$ for all $h \in G\}$ is the *centre* of a group G.
- If $g \in C(G)$ we say g is *central*.
- The centre is the intersection of all centralizers and it is a subgroup of G.
- G is abelian iff $C(G) = G$.
- (number of conjugates of g in G) $\times |C(g)| = |G|$.
- $\{e\}$ is always a conjugacy class of G.
- $\{g\}$ is a conjugacy class iff $g \in C(G)$. Hence $C(G)$ is the union of all one-element conjugacy classes.
- If $|G| = p^k$ where p is prime and $k \in \mathbb{N}$, then $|C(G)| \geq p$.

Let G be a group with conjugacy classes $C_1, ..., C_n$ (C_1 is always $\{e\}$) with sizes $c_1, ..., c_n$ (so $c_1 = 1$). If $g \in C_k$ then $c_k = \frac{|G|}{|C(g)|}$. In particular, c_k divides the order of the group. Then the *class equation of G* is

$$|G| = c_1 + c_2 + ... + c_n.$$

Conjugacy in S_n

The number of elements os S_n of cycle type $1^{m_1}, 2^{m_2}, ..., n^{m_n}$ is

$$\frac{n!}{m_1! ... m_n! 1^{m_1} 2^{m_2} ... n^{m_n}}.$$

Dihedral Group D_n

We call the group of symmetries of and n-gon the dihedral group D_n.

- $|D_n| = 2n$.
- D_n is not abelian.

Symmetric Group S_n

The set of all symmetries (permutations) of a set X of n objects is the symmetric group S_n.

- $|S_n| = n!$.
- S_n is abelian iff $n = 2$.

General Linear Group $GL(n, \mathbb{R})$

The set of invertible $n \times n$ matrices with entries in $\mathbb{R}$ is a group under matrix multiplication.

- $GL(n, \mathbb{R})$ is not abelian.
- Subgroups:
  $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) | \det A = 1\}$,
  $O(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) | A^T = A^{-1}\}$,
  $SO(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) | \det A = 1 \text{ and } A^T = A^{-1}\}$
- $|GL(n, \mathbb{Z}_p)| = (p^n - 1)(p^n - p)(p^n - p^2)...(p^n - p^{n-1})$

Useful facts

- If a group G is cyclic then G is abelian.
- G is cyclic iff G has an element of order $|G|$.
- If $g^2 = e \quad \forall g \in G$ then G is abelian.
- Every group of order p^2 (p prime) is abelian.
- If H, K are cyclic the $H \times K$ is cyclic iff $gcd(|H|, |K|) = 1$.
- $(gh)^{-1} = h^{-1}g^{-1}$
- If G, H are finite subgroups that intersect trivially then $|G \times H| = |G||H|$.
- $o(g) = o(g^{-1})$
- If G is abelian and $H \leq G$ then left cosets are the same as right cosets.
- Let $o(g) = k$ then if k is even $o(g^2) = \frac{k}{2}$ and if k is odd then $o(g^2) = k$.