Dummit and Foote Abridged

May 29, 2024

Contents

0 Preliminaries

0.1 Basics

Proposition 1. Let $f\colon A \to B$.

1. The map f is injective if and only if f has a left inverse.
2. The map f is surjective if and onbly if f has a right inverse.
3. The map f is a bijection if and only if there exist $g\colon B \to A$ such that $f \circ g$ is the indentity map on B and $g \circ f$ is the identity map on A.
4. If A and B are finte sets with the same number of elements the $f\colon A \to B$ is bijective if and only if f is injective if and only if f is surjective.

Proposition 2. Let A be a nonempty set.

1. If $\sim$ defines an equivalence relation on A then the set of equivalence classes of $\sim$ form a partision of A.
2. If $\{A_i \mid i \in I\}$ is a parttion of A then there is an equivalence relation on A whose equivalence classes are precisely the sets $A_i, i \in I$

1 Group Theory

1.1 Basic Axioms and Examples

Definition. 1. A *binary operation* $\star$ on a set G is a function $\star\colon G \times G \to G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$.

2. A binary operation $\star$ on a set G is associative if for all $a, b, c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.

3. If $\star$ is a binary operation on a set G we say elements a and b of G *commute* if $a \star b = b \star a$. We say $\star$ (or G) is *commutative* if for all $a, b \in G$, $a \star b = b \star a$.

Proposition 1. If G is a group under the operation $\cdot$, then

1. The identity of G is unique
2. for each $a \in G$, a^{-1} is uninuely determined
3. $(a^{-1})^{-1} = a$ for all $a \in G$
4. $(a \cdot b)^{-1} = (b^{-1}) \cdot (a^{-1})$
5. for any $a_q, a_2, \dots, a_n \in G$ the value of $a_1 a_2 \cdots a_n$ is independent of how the expresion is bracketed

Proposition 2. Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancelation laws hold in G, i.e.,

1. if $au = av$, then $u = v$, and
2. if $ub = vb$, then $u = v$.

Definition. For G a group and $x \in G$ define the *order* of x to be the smallest positive integer n such that $x^n = 1$, denoted $|x|$. If there is no such integer than we define the order of x to be infinity.

1.6 Homomorphism and Isomorphisms

Definition. Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\phi\colon G \to H$ such that $\phi(x \star y) = \phi(x) \diamond \phi(y)$, for all $x, y \in G$ is called a *homomorphism*. Moreover, if ϕ is bijective it is called an *isomorphism* and we say that G and H are *isomorphic* or of the same *isomorphism type*, written $G \cong H$.

Remark. If $\phi\colon G \to H$ is an isomorphism then

1. $|G| = |H|$
2. G is abelian if and only if H is abelian
3. for all $x \in G, |x| = |\phi(x)|$

1.7 Group Actions

Definition. A *group action* of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$, and
2. $1 \cdot a = a$ for all $a \in A$.

Remark. Let the group G act on the set A. From each fixed $g \in G$ we get a map σ_g defined by

$$\sigma_g \colon A \to A$$
$$\sigma_g(a) = g \cdot a.$$

The following are true

1. for each fixed $g \in G$, σ_g is a permutation of A, and
2. the map from G to S_A defined bt $g \mapsto \sigma_g$ is a homomorphism. Moreover this map is called the *permuation representation* associated to the given action.

Remark. As a consequence of the above remark, if $\phi \colon G \to S_A$ is a homomorphism (here S_A is the symmetric group on the set A), then the map from $G \times A$ to A defined by

$$g \cdot a = \phi(g)(a) \text{for all} g \in G, \text{ and all} a \in A$$

is a group action of G on A.

2 Subgoups

2.1 Definition and Examples

Proposition 1. (The Subgroup Criterion) A subset H of a group G is a subgroup if and only if

1. $H \neq \emptyset$, and
2. for all $x, y \in H, xy^{-1} \in H$

2.3 Cyclic Groups and Cyclic Subgroups

Proposition 2. If $H = \langle x \rangle$, then $|H| = |x|$. Moreover,

1. if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements of H, and
2. if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b \in \mathbb{Z}$.

Proposition 3. Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$ then $x^d = 1$ where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$ then $|x|$ divides m.

Theorem 4. Any two cyclic groups of the same order are isomorphic. Moreover,

1. if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of orger n, then the map
$$\begin{aligned} \phi\colon \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$
is well defined and is an isomorphism

2. if $\langle x \rangle$ is an infinite cyclic group, the map
$$\begin{aligned} \phi\colon \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$
is well defined and is an isomorphism

Proposition 5. Let G be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.

1. If $|x| = \infty$, then $|x^a| = \infty$.
2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$.
3. In particular, if $|x| = n < \infty$ and a is a postive integer dividing n, then $|x^a| = \frac{n}{a}$.

Proposition 6. Let $H = \langle x \rangle$.

1. Assume $|x| = \infty$. Then $H = \langle x^a \rangle$ if and only if $a = \pm 1$.
2. Assume $|x| = n < \infty$. Then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$. In particular, the number of generators of H is $\phi(n)$ (where ϕ is Euler's ϕ-function)

Theorem 7. Let $H = \langle x \rangle$ be a cyclic group.

1. Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.
2. If $|H| = \infty$, then for any distinct nonnegative integers a and b, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$, where $|m|$ denotes the absolute value of m, so that the nontrival sungroups of H correspond bijectively with the integers $1, 2, 3, \ldots$.
3. If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a. This subgroup is the cyclic group $\langle x^d \rangle$, where $d = \frac{n}{a}$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that the subgroups of H correspond bijectively with the positive divisors of n.

2.4 Subgroups Generated by Subsets of a Group

Proposition 8. If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.

Proposition 9. $\overline{A} = \langle A \rangle$.

3 Quotient Groups and Homomorphisms

3.1 Definitions and Examples

Proposition 1.