Modern Algebra 1 — Handout
MAT 513/613, Fall 2024 — D. Ivanšić

Test Knowledge

Sections 0, 2–4

Definitions

Greatest common divisor (0)
Binary operation (2)
Group (2)
Commutativity of elements (2)
$\mathbf{Z}_n$ with multiplication and addition module n
$U(n)$ with multiplication modulo n (2)
Dihedral group D_n, number and nature of elements (2)
Order of an element (3)
Subgroup (3)
$GL(n,\mathbf{R})$ and $SL(n,\mathbf{R})$ (3)
Cyclic Subgroup (3)
Subgroup generated by a set S (3)
Center of group $Z(G)$, centralizer of an element $C(a)$
Euler ϕ function (4)

Theorems

Division Algorithm (Theorem 0.1)
GCD is a linear combination (Theorem 0.2)
Fundamental Theorem of Arithmetic (Theorem 0.3)
Inverse of a product (Theorem 2.4)
Two-step subgroup test (Theorem 3.2)
Proposition on subgroups of $\mathbf{Z}$ (3)
Nature of a cyclic group (Theorem 4.1)
$|a| = |\langle a\rangle|$, if $a^k = e$, then $|a|$ divides k (Corollaries 1, 2 to 4.1)
If $ab = ba$, $|ab|$ divides $|a||b|$ (Corollary 3 to 4.1)
$\left\langle a^k\right\rangle = \left\langle a^{\gcd(n,k)}\right\rangle$ and $|a^k| = \frac{n}{\gcd(n,k)}$ (Theorem 4.2)
If $|a| = n$, then $\langle a^i\rangle = \langle a^j\rangle$ iff $\gcd(n,i) = \gcd(n,j)$
and $|a^i| = |a^j|$ iff $\gcd(n,i) = \gcd(n,j)$ (Corollary 2 to 4.2)
Fundamental theorem of cyclic groups (Theorem 4.3)
If d divides $|a|$, number of elements of order d in $\langle a\rangle$ is $\phi(d)$ (Theorem 4.4)
In finite group, no. of elts of order d is a multiple of $\phi(d)$ (Corollary to 4.4)

Proofs

$\mathbf{Z}_n$ with addition modulo n is a group (2)
$U(n)$ with multiplication modulo n is a group (2)
Proposition on subgroups of $\mathbf{Z}$ (3)
Nature of a cyclic group (Theorem 4.1)
If d divides $|a|$, number of elements of order d in $\langle a\rangle$ is $\phi(d)$ (Theorem 4.4)

B-problems

section 2: 20, 23&27, 31, 33, 37, 43&44, 49, 50
section 3: 8, 13&14&20, 15, 28&29, 37, 42d, 47, 50&52, 58, 73, 76, 78
section 4: 13, 14, 22, 30, 31, 34, 35, 57, 59, 65, 67, 71, 72

Modern Algebra 1 — Handout
MAT 513/613, Fall 2024 — D. Ivanšić

Test Knowledge

Sections 5, 10.1, 6

Definitions

Permutation of a set A (5)
Permutation group of a set A (5)
Even and odd permutations (5)
Symmetric group S_n, alternating group A_n (5)
Group homomorphism (10)
Kernel of a homomorphism (10)
Group isomorphism (6)
Automorphism of a group, inner automorphism induced by $a \in G$ (6)
$\operatorname{Aut} G$, $\operatorname{Inn}(G)$

Theorems

Every permutation is a product of disjoint cycles (5.1)
Disjoint cycles commute (5.2)
Order of a permutation (5.3)
Every permutation is a product of 2-cycles (5.4), whose number for a given permutation is always either even or odd (5.5)
$|S_n| = n!$, $|A_n| = n!/2$ (5)
Theorem 10.1
Theorem 10.2, 1–4, 6–7.
Cayley's theorem: every group is isomorphic to a group of permutations (6.1)
Theorem 6.2, 3–7
Theorem 6.3, 1–3, 6
$\operatorname{Aut}(\mathbf{Z}_n) \approx U(n)$, $\operatorname{Aut}(\mathbf{Z}) \approx \{1, -1\}$ (6.5)

Proofs

Theorem 5.7
Theorem 10.1 1, 4, 5 (1.3)
Theorem 10.2 1, 7
Theorem 6.1

B-problems

section 5: 9, 34, 37, 38, 41, 53, 57, 61, 65
section 10.1: 20&52, 22, 23, 27, 28&34, 32
section 6: 19, 20&23, 32, 40, 41, 50&63, 57, 62&64, 65

Test Knowledge

Sections 7–8

Definitions
Left and right coset of H in G (7)
Direct product of groups $G_1 \times \cdots \times G_n$ (8)
$U_k(n)$ (8)

Theorems
Lemma on properties of cosets (7)
Lagrange's theorem: $|H|$ divides $|G|$ (7.1)
Corollaries to Lagrange's theorem 1–4
Theorem 7.2
Order of an element $(g_1, \ldots, g_n)$ is $\text{lcm}(|g_1|, \ldots, |g_n|)$ (8.1)
Theorem 8.2
Corollary 2 of theorem 8.2
When $\gcd(s,t) = 1$, $U(st) = U(s) \times U(t)$ and $U_s(st) \approx U(t)$ (8.3)

Proofs
Lemma on cosets (2.2)
Lagrange's theorem
Theorem 8.2

B-problems
section 7: 20, 25, 27, 29&31, 40&46, 47, 51&52
section 8: 2&31, 5, 10&11, 22, 26, 41&54, 51, 65