Modern Algebra 1 — Handout
MAT 514/614, Spring 2025 — D. Ivanšić

Test Knowledge

Sections 9–13

Definitions

Normal subgroup (9)
Quotient group and its operation, quotient map (9)
Partition of a natural number n (11)
Ring, commutative ring, unity, unit element (12)
Subring (12)
Zero-divisor, integral domain (13)
Field (13)
Characteristic of a ring (13)

Theorems

H is normal if and only if $aHa^{-1} \subseteq H$ for all $a \in G$ (Theorem 9.1)
If H is normal, then G/H is a group (Theorem 9.2)
Cauchy's Theorem on Abelian Groups (Theorem 9.5)
If H, K normal, $HK = G$, $H \cap G = \{e\}$ then $G \approx H \times K$ (example in 9)
Every group of order p^2, p prime, is $\mathbf{Z}_{p^2}$ or $\mathbf{Z}_p \times \mathbf{Z}_p$ (Theorem 9.7)
Image, inverse image of normal subgroup is normal (Theorem 10.2)
First Isomorphism Theorem (Theorem 10.3)
$|\phi(G)|$ divides $|G|$ (Corollary to 10.3)
$G/Z(G) \approx \mathrm{Inn}(G)$ (Theorem 9.4)
Fundamental Theorem of Finite Abelian Groups (Theorem 11.1)
  alternate version: $G \approx \mathbf{Z}_{r_1} \times \mathbf{Z}_{r_2} \times \cdots \times \mathbf{Z}_{r_s}$, where r_i divides r_{i-1} (11)
G abelian, if $m \mid |G|$, then G has subgroup of order m (Corollary to 11.1)
Additional operations' properties in rings (Theorem 12.1)
In an integral domain, $ab = ac$ implies $b = c$ (Cancellation Theorem 13.1)
S is a subring if $a + b, -a, ab \in S$ for every $a, b \in S$ (Theorem 12.3)
$\mathbf{Z}_n$ is an integral domain if and only if n is prime (13)
Finite integral domain is a field (Theorem 13.2)
In a ring with unity, $\mathrm{char}\, R = |1|$, essentially (Theorem 13.3)
Characteristic of an integral domain is prime (Theorem 13.4)

Proofs

If H is normal, then G/H is a group (Theorem 9.2)
If H, K normal, $HK = G$, $H \cap G = \{e\}$ then $G \approx H \times K$ (example in 9)
First Isomorphism Theorem (Theorem 10.3)
$\mathbf{Z}_n$ is an integral domain if and only if n is prime (13)
In a ring with unity, $\mathrm{char}\, R = |1|$, essentially (Theorem 13.3)
Characteristic of an integral domain is prime (Theorem 13.4)

B-problems

section 9: 22, 24, 41&53, 63, 64, 67, 72
section 10: 8, 12, 41&42, 45, 54, 65, 66
section 11: 1&2&3, 6&7&8, 11, 22, 32
section 12: 11, 15&17, 30, 40&41, 47, 48
section 13: 5&7, 16, 24&25, 30, 39&40, 45, 51, 54, 61, 65

Modern Algebra 1 — Handout
MAT 514/614, Spring 2025 — D. Ivanšić

Test Knowledge

Sections 14–17

Definitions

Ideal, principal ideal $\langle a \rangle$, ideal generated by $a_1, \dots, a_n$ (14)
Prime ideal, maximal ideal (14)
Ring homomorphism (15)
Evaluation homomorphism $R[x] \to R$, $f \mapsto f(a)$ (15)
Field of quotients (15)
Polynomial ring $R[x]$, $F[x]$ (16)
When $g \in D[x]$ divides $f \in D[x]$, factor of a polynomial (16)
Multiplicity of a zero of $f \in D[x]$ (16)
Irreducibility, reducibility over D, F (17)

Theorems

R/A is a ring if and only if A is an ideal (Theorem 14.2)
R/A is an integral domain if and only if A is prime (Theorem 14.3)
R/A is a field if and only if A is maximal (Theorem 14.4)
Properties of ring homomorphisms (Theorem 15.1)
First isomorphism theorem for rings (Theorem 15.3)
$\exists$ ring homomorphism $\mathbf{Z}_n \to R$, $1 \mapsto a$ iff $|a|$ divides n and $a^2 = a$ (15)
$\exists$ ring homomorphism $\mathbf{Z} \to R$, $1 \mapsto a$ iff $a^2 = a$ (Theorem 15.5)
If $\operatorname{char} R = n$, R contains $\mathbf{Z}_n$;
  if $\operatorname{char} F = p$, F contains $\mathbf{Z}_p$; if $\operatorname{char} F = 0$, F contains $\mathbf{Q}$ (Corollary to 15.5)
Every integral domain is contained in a field (Theorem 15.6)
If D is an integral domain, so is $D[x]$ (Theorem 16.1)
If $f, g \in F[x]$, $g \neq 0$ then $f = gq + r$ where $\deg r < \deg g$ (Theorem 16.2)
$f(a)$ is remainder in division by $x - a$,
  a is a zero if and only if $x - a$ is a factor of f (Corollares to 16.2)
Polynomial of degree n in $F[x]$ has at most n zeroes (Theorem 16.3)
In $F[x]$, every ideal is a principal ideal $\langle f \rangle$ (Theorem 16.4)
$\deg 2, 3$ polynomials in $F[x]$ are reducible iff they have a zero (Theorem 17.1)
For $f \in \mathbf{Z}[x]$, if f is reducible over $\mathbf{Q}$, then f is reducible over $\mathbf{Z}$ (Theorem 17.2)
For $f \in \mathbf{Z}[x]$, if $f \mod p$ is irred. over $\mathbf{Z}_p$, then f is irred. over $\mathbf{Q}$ (Theorem 17.3)
Eisenstein's Criterion (Theorem 17.4)
$x^{p-1} + x^{p-2} + \cdots + x + 1$ is irred. over $\mathbf{Q}$ for prime p (Corollary to 17.4)
For $f \in F[x]$, $\langle p \rangle$ is maximal iff p is irreducible over F (Theorem 17.5)
For $f \in F[x]$, $\langle p \rangle$ is maximal iff p is irreducible over F (Theorem 17.5)
Unique factorization in $\mathbf{Z}[x]$ (Theorem 17.6)

Proofs

R/A is a ring if and only if A is an ideal (Theorem 14.2)
Every integral domain is contained in a field (Theorem 15.6)
Every integral domain is contained in a field (Theorem 15.6)
If $f, g \in F[x]$, $g \neq 0$ then $f = gq + r$ where $\deg r < \deg g$ (Theorem 16.2)
In $F[x]$, every ideal is a principal ideal $\langle f \rangle$ (Theorem 16.4)
For $f \in \mathbf{Z}[x]$, if $f \mod p$ is irred. over $\mathbf{Z}_p$, then f is irred. over $\mathbf{Q}$ (Theorem 17.3)

B-problems

section 14: 6, 11, 22, 35, 39, 40, 48, 63, 64, 65
section 15: 7iso&61, 10&50, 12, 21, 32&33, 56, 57, 58, 59, 63
section 16: 14&24, 23, 26, 35&38, 39&40, 49, 55
section 17: 14bd, 15, 16, 17&25, 31, 35, 36

Test Knowledge

Sections 20, 32

Definitions

- Extension field (20)
- Smallest subfield containing F and $a_1, \ldots, a_n$: $F(a_1, \ldots, a_n)$ (20)
- $f \in F[x]$ splits in E over F, splitting field of f over F (20)
- Degree $[E : F]$ of extension E over F (32, 21 in book)
- Galois group $\mathrm{Gal}(E/F)$ of E over F (32, 21 in book)
- Fixed field of a subgroup $H \leq \mathrm{Gal}(E/F)$ (32)
- Mappings between subgroups of $\mathrm{Gal}(E/F)$ and fields K, $F \subseteq K \subseteq E$ (32)
- Solvability by radicals of $f \in F[x]$ over F (32)
- Solvable group (32)

Theorems

- For $f \in F[x]$ there is an extension field of F in which f has a zero (Theorem 20.1)
- For $f \in F[x]$ there exists a splitting field of f over F (Theorem 20.2)
- Technical lemma about extending isomorphisms $F \to F'$ to $F(a) \to F'(b)$ and extension fields (Lemma and Theorem 20.4)
- Every two splitting fields over F of an $f \in F[x]$ are isomorphic (Corollary to Theorem 20.4)
- Fundamental Theorem of Galois Theory (Theorem 32.1)
- For splitting field E of $x^n - a$ over F, $\mathrm{Gal}(E/F)$ is solvable (Theorem 32.2)
- Quotient group of a solvable group is solvable (Theorem 32.3)
- If G/N and N are solvable, then so is G (Theorem 32.4)
- Theorem 32.5
- Example of a polynomial of degree 5 that is not solvable by radicals over $\mathbf{Q}$ (32)

Proofs

- For $f \in F[x]$ there is an extension field of F in which f has a zero (Theorem 20.1)
- Example of a polynomial of degree 5 that is not solvable by radicals over $\mathbf{Q}$ (32)

B-problems

section 20: 5, 8&9&10, 13, 16, 20, 25, 28, 36, 42

section 32: 6, 9, 16, 17, 27, 32