Final Review

Trustin Nguyen

May 14, 2023

Review 1

1. **Groups and Homomorphisms**: Binary operations, Definition of groups, Order of Group, Aberlian Group, Subgroups

   Results:

   (a) Identity is unique, Inverses are unique, $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$.

   (b) Subgroup criteria I and II

   (c) Subgroups of $(\mathbb{Z}, +)$ are in $n\mathbb{Z}$.

2. **Homomorphisms**: Functions, Composition, injective, surjective, bijective, definition of homomorphisms, isomorphisms, image, and kernel.

   Results:

   (a) $f(e_G) = e_H$, $f(a^{-1}) = f(a)^{-1}$

   (b) Compositions of homomorphisms is a homomorphism

   (c) Inverse of an Isomorphism is an Isomorphsim

   (d) Image and kernel are subgroups

   (e) If $a \in G$, $k \in \ker f$, then $ak^{-1}a \in \ker f$.

   (f) Injective iff $\ker f = \{e\}$

   (g) Surjective iff $\text{Im}\{f\} = H$ where $f : G \to H$

3. **Cyclic Groups**: Definiton of a cyclic, C_n, order of an element, exponent of a group,

   Results:

   (a) $\forall a \in G : \text{ord}(a) = |\langle a \rangle|$

   (b) Cyclic $\to$ Abelian.

4. **Dihedral Groups**: Definition of dihedral groups D_{2n} (Symmetries of a regular n-gon).

5. **Direct Product of Groups**: Definition of direct products

   (a) $C_m \times C_n \cong C_{nm}$ iff $\gcd(n, m) = 1$

   (b) Direct Product Theorem

6. **Symmetric groups**: Permutations, Symmetric group of a set X, Row and cycle notation, $k-$cycles and transpositions, cycle type/shape, sign of permutations, Alternating subgroups.

   Results:

   (a) Sym X is a group

   (b) Disjoint cycles commute

(c) Any $\sigma \in S_n$ is uniquely a product of disjoint cycles.

(d) $\text{ord}(\sigma)$, $\sigma \in S_n$ is the lcm of the lengths in the disjoint cycle representation of σ.

(e) Every $\lambda \in S_n$ is a product of transpositions.

(f) The number of transpositions is always either even or odd in the result above.

(g) $\forall n \geq 2$, $\text{sgn} : S_n \to \{\pm 1\}$ is a homomorphism.

(h) σ is an even permutation $\text{sgn}(\sigma) = 1$ iff the number of cycles of even length is even.

(i) Every subgroup of S_n contains either no odd permutations or exactly half.

7. **Lagrange**: Cosets, Partitions of a set, Index of subgroups, equivalence relations and equivalence classes, Euler totient function

   Results:

   (a) Lagrange's Theorem

   (b) Left cosets partition G and all cosets have the same size

   (c) $\text{ord}(a) \mid |G|$

   (d) $\forall a \in G : a^{|G|} = e$

   (e) Groups of prime order are cyclic

   (f) Fermat-Euler Theorem

   (g) Every group of order 4 is either C_4 or $C_2 \times C_2$

   (h) Any group of order 6 is either cyclic or dihedral.

8. **Quotient Groups**: Normal subgroups, quotient groups, simple groups

   Results:

   (a) Index of 2 implies that the group is a normal subgroup

   (b) Subgroups of abelian groups are normal

   (c) Kernals are normal

   (d) If $K \triangleleft G$, left cosets of K form a group

   (e) Natural projection $G \to G/K$ is a surjective group homomorphism

   (f) Quotient of cyclic is cyclic

   (g) Isomorphism theorem: $G/\ker f \cong \text{Im}\{f\}$

   (h) Any cyclic group is $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$

9. **Group Actions**: Group action, Kernel of action, faithful action, orbit, stabilizer, transitive action, conjugation of an element, conjugacy classes, centralizers, center, normalizer.

   Results:

   (a) Criteria for group actions

   (b) Stabilizer of X is a subgroup

   (c) Orbits partition your set X

   (d) Orbit-Stablizer Theorem: $|\text{Orb}(x)||\text{Stab}(x)| = |G|$

   (e) Important Actions: Left regular action, Conjugation action, Cayley's Theorem, Normal subgroups are unions of conjugacy classes, G acts on its subgroups

   (f) Stabilizers of elements in the same orbit are conjugate

(g) Cauchy's Theorem

Review 2

1. **Rings**: Rings, commutative rings, subrings, unit in a ring, field, product of rings, polynomials, polynomial rings, degree of a polynomial, monic poly, power series, Laurent series and polys.

   Results:

   (a) equivalents from group theory

2. **Homomorphisms, Ideals, Quotients, Isomorphisms**: Homomorphisms of rings, isomorphisms, kernels, images, ideals, proper ideals, generators of ideals, principle ideals, quotient rings, characteristic

   Results:

   (a) $\varphi : R_1 \to R_2$ injective iff $\ker \varphi = \{0\}$

   (b) surjective iff $\mathrm{Im}\{\varphi\} = R_2$

   (c) $\ker \varphi$ is an ideals

   (d) the quotient is a ring R/I and the projection $\pi : R \to R/I$ is a surjective homomorphism with $\ker \pi = I$.

   (e) Euclidean division algorithm for polynomials over a field. Euclidean function is the degree.

   (f) First isomorphism theorem: $\varphi : R_1 \to R_2$ and $R_1/\ker \varphi \cong \mathrm{Im}\{\varphi\}$

   (g) Second isomorphism thoerem: $R \leq S$, $J \triangleleft S$, then $J \cap R \triangleleft R$ and $\frac{R+J}{J} \leq \frac{S}{J}$

   $$\frac{R+J}{J} \cong \frac{R}{R \cap J}$$

   (h) Third isomorphism thoerem: $I \triangleleft R$, $J \triangleleft R$, $I \subseteq J$:

   $$J/I \triangleleft R/I$$

   and

   $$(R/I)/(J/I) \cong R/J$$

3. **Integral domains, Field of fractions, Maximal ideals**: Integral domain, zero divisor, field of fractions, maximal ideals, prime ideals

   Results:

   (a) finite ID $\to$ field

   (b) R ID $\to R[x]$ is an ID

   (c) every ID has a field of fractions

   (d) $R \neq \{0\}$ is a field iff the only ideals are $\{0\}$ and R.

   (e) $I \triangleleft R$ is maximal iff R/I is a field

   (f) $I \triangleleft R$ is prime iff R/I is an ID

   (g) Every maximal ideal is prime

   (h) characteristic is 0 or prime

4. **Factorization in IDs**: Units, division, associates, irreducibles, primes, euclidean functions, euclidean domains, principal ideal domains, unique factorization domains, ascending chain condition, noetherian rings, greatest common divisor

   Results:

   (a) (r) is prime iff $r = 0$ or r is prime

   (b) prime $\rightarrow$ irreducible but the converse is not always true in an ID

   (c) Euclidean domain $\rightarrow$ PID

   (d) In PIDs irreducibles $\rightarrow$ prime

   (e) PIDs satisfy the ascending chain condition (ACC)

   (f) So PID $\rightarrow$ UFD

   (g) In UFDs, gcds exists and is unique up to associates

5. **Factorization in Polynomial Rings**: Content, primitive polynomials, polynomials in several variables

   Results:

   (a) R is a UFD, f, g are primitive, then fg is primitive

   (b) $c(f)c(g)$ is an associated of $c(fg)$

   (c) Gauss's lemma

   (d) R is a UFD $\rightarrow R[x]$ is a UFD

   (e) Eisenstein's criterion for irreducibility.

6. **Gaussian integers**: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$

   Results:

   (a) A prime p in $\mathbb{Z}$ is prime in $\mathbb{Z}[i]$ iff $p \neq a^2 + b^2, a, b \in \mathbb{Z} \backslash \{0\}$.

   (b) If p is prime, in $\mathbb{Z}$, and $F_p = \mathbb{Z}/p\mathbb{Z}$, then $F_p^* = F_p \backslash \{0\}$ is cyclic of order $p - 1$

   (c) Primes in $\mathbb{Z}[i]$ up to associates

   (d) We have p is prime, $p \equiv 3 \pmod 4$

   (e) $z \in \mathbb{Z}[i]$, $N(z) = z\overline{z} = p$ for some prime p, $p = 2$ or $p \equiv 1 \pmod 4$

   (f) A non-negative $n \in \mathbb{Z}$ is a sum of squares iff $n = \prod p_i^{n_i}$, p_i are distinct, then $p_i \equiv 3 \pmod 4 \rightarrow n_i$ is even.

7. **Algebraic Integers**: Algebraic integers, $\mathbb{Z}(\alpha)$ for algebraic integers α, minimal polynomial

   Results:

   (a) $\ker(ev_\alpha) \triangleleft \mathbb{Z}[x]$ is principal, generated by the minimal polynomial

   (b) $\alpha \in \mathbb{Q}$ is algebraic $\rightarrow \alpha \in \mathbb{Z}$