MATH 0430, Review sheet for final exam

Kiumars Kaveh

December 9, 2011

- The final exam is 1 hour and 50 minutes. The format is similar to the midterms. It is slightly longer than midterms. It is more focused on the second half of the course.
- You are responsible to know the homework problems, some problems in the test will be from homeworks or similar to them.
- There will be proof problems (like the ones in the homeworks).
- Definitions (groups): Group, subgroup, isomorphism, abelian group, cyclic group, order of an element in a group, cyclic subgroup generated by an element, generating set, permutation, cycle, transposition, odd and even permutations, symmetric group and alternating group, symmetry group of a figure, coset, direct product, homomorphism, normal subgroup. homomorphism, kernel, normal subgroup, factor group, simple group, center of a group, group G acting on a set X, stabilizer (isotropy) subgroup G_x, orbit $G \cdot x$.
- Important examples of groups: $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n^*, \times)$, dihedral group, Klein group V, symmetric group S_n, alternating group A_n, group of invertible $n \times n$ matrices (denoted by $\mathrm{GL}(n, \mathbb{R})$), direct product of groups.
- Some examples of group homomorphisms: Natural homomorphism $\phi : G \to G/H$ defined by $\phi(g) = gH$, where H is a normal subgroup, e.g. reduction mod n homomorphism $\mathbb{Z} \to \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ (Example 13.10). Sign of a permutation $\phi : S_n \to \mathbb{Z}_2$ (Example 13.3). Determinant (Example 13.6).
- Definitions (rings): ring, field, homomorphism and isomorphism of rings, unit element, divisor of zero, integral domain, characteristic of a ring/field, field of quotients of an integral domain, ring of polynomials, irreducible polynomial, evaluation homomorphism, maximal ideal, prime ideal, principal ideal domain (PID), unique factorization domain (UFD), extension field, algebraic and transcendental elements, irreducible polynomial of an algebraic element.
- Important examples of rings: $\mathbb{Z}$, $\mathbb{Z}_n$, $n \times n$ matrices, polynomials $F[x]$ where F is a field, all functions from $\mathbb{R}$ to $\mathbb{R}$, direct product of rings.

- Some examples of ring homomorphisms: evaluation homomorphism $\phi_\alpha : F[x] \to E$ where E is a field containing F and α (Theorem 22.4). Reduction mod n homomorphism $\mathbb{Z} \to \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

- Important examples of fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (complex numbers), $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$, fields obtained by adjoining an algebraic element to $\mathbb{Q}$, e.g. $\mathbb{Q}(\sqrt{2})$, quotient of a ring by a maximal ideal, e.g. $F[x]/\langle f \rangle$ where f is an irreducible polynomial over F.

- Skills:

  - Verifying whether a given set and operation is a group/subgroup.
  - Determining whether two groups are isomorphic, or whether a given map is an isomorphism.
  - Decomposing a permutation as a product of disjoint cycles, as well as a product of transpositions.
  - Determining the symmetry group of a simple figure e.g. square, hexagon (usually a dihedral group).
  - Determine/prove whether a given map between groups is a homomorphism.
  - Writing the list of all non-isomorphic finite abelian groups of a given order n.
  - Finding the factor group a group (i.e. quotient by a normal subgroup) e.g. Example 14.12 or some examples in the homeworks.
  - Checking if a group G is simple, e.g. a product $G_1 \times G_2$ is not simple because $G_1 \times \{e\}$ and $\{e\} \times G_2$ are normal subgroups, or S_n is not simple because A_n is a normal subgroup. Also it is a well-known (and very important fact in applications) that A_n is a simple group for $n > 4$.
  - Counting the number of orbits of a group action (examples in Section 17).
  - Verifying a given set of a ring/field is a subring/subfield, e.g. $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$, and $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$.
  - Writing a field $F(\alpha)$ obtained by adjoining an algebraic element α to F as a factor ring $F[x]/\langle f(x) \rangle$ where $f(x)$ is the irreducible polynomial of α over F, using evaluation homomorphism $\phi_\alpha : F[x] \to F(\alpha)$. The kernel of this homomorphism is exactly the principal ideal generated by $f(x)$.

- Statement and content of theorems:

  - Elementary properties of groups and subgroups (Theorems 4.15-4.18 and 5.14, 5.17, 7.4)

- Properties of cyclic groups (Theorems 6.1, 6.6, 6.10, 6.16)
- Permutations (Theorem 8.5, 9.8, 9.12, 9.15, 9.20)
- Cayley's theorem
- Cosets (Theorems 10.1, 10.10-10-12)
- Direct products and finitely generated abelian groups (Theorems 11.2, 11.9)
- Fundamental theorem of finitely generated abelian groups (Theorem 11.12).
- Properties of homomorphisms (Theorem 13.12, 13.15 and Corollary 13.18).
- Kernel of a homomorphism is a normal subgroup (Corollary 13.20).
- Factor group (Theorem 14.4 and Corollary 14.5).
- Fundamental Homomorphism Theorem (Theorem 14.9 and 14.11).
- Equivalent conditions for a subgroup to be normal (Theorem 14.13).
- Normal subgroups in direct product (Theorem 15.8).
- A_n is a simple group if $n \geq 5$ (Theorem 15.15).
- Group actions (Theorem 16.12 and 16.14), Obrit-Stabilizer Theorem (Theorem 16.16), and Burnside's formula (Theorem 17.1).
- Elementary properties of rings (Theorem 18.8, 19.5).
- Divisors of zero in $\mathbb{Z}_n$, and $\mathbb{Z}_p$ is a field (Theorem 19.3 and Corollary 19.12).
- Field of quotients (Lemma 21.2, Theorem 21.5).
- Polynomials: Division Algorithm (Theorem 23.1), Factor Theorem (Corollary 23.3).
- Unique factorization in the ring of polynomials $F[x]$ (Theorem 23.20).
- Fundamental Homomorphism Theorem for rings (Theorem 26.16 and Theorem 26.17)
- Quotient by a maximal ideal is a field (Theorem 27.9) and quotient by a prime ideal is integral domain (Theorem 27.15).
- A field F has no ideals except $\{0\}$ and F itself (Theorem 27.5 and Corollary 27.6)
- Ideals in $\mathbb{Z}$: the ring $\mathbb{Z}$ is a PID and hence a UFD (Corollary 45.18).
- Ideals in $F[x]$: the ring $F[x]$ is a PID, and hence a UFD (Theorem 27.24 and Corollary 23.20).
- Maximal ideals in $F[x]$ (Theorem 27.25).
- Maximal ideals in $\mathbb{Z}$.
- Kronecker's Theorem (Theorem 29.3).

- Every PID is a UFD (Theorem 45.17)

- Proof of theorems:
  - Theorem 13.15 which states that if H is the kernel of a homomorphism ϕ then $\phi(x) = \phi(y)$ if and only if x, y lie in the same left coset of H (similarly right coset).
  - Proof of the fact that $F[x]$ is a PID (Theorem 27.24)
  - Proof of the fact that $\mathbb{Z}$ is a PID.
  - Proof of the fact that a field F has no ideals except $\{0\}$ and F (Theorem 27.5 and Corollary 27.6).