Math 113, Summer 2015 Prof. Haiman

Review guide and exercises

1. Outline of topics

Questions on the final exam will cover some subset of the topics listed below. Approximately one half of the exam will be on group theory and basic ring theory. The other half will be on further ring theory and field theory, which were not covered on the midterm exams.

I have deliberately omitted some topics from the textbook that go beyond what we covered in class (most of Section 3.5, for example), and some topics that we discussed or will discuss in class, but are more advanced than what I expect you to know for the exam, such as the proof of unsolvability of the quintic equation.

- Divisibility, prime factorization, GCD for integers. Modular arithmetic. Chinese Remainder Theorem.
- Groups, subgroups, cyclic subgroups, order of an element. Subgroup generated by a set of elements in a group. Cosets, index of a subgroup, Lagrange's theorem. Group homomorphisms, normal subgroups, quotient groups. Center of a group.
- Specific groups: cyclic groups $\mathbb{Z}$ and $\mathbb{Z}_n$; group of units $\mathbb{Z}_n^\times$ (called $\Phi(n)$ in Goodman). Permutation groups S_n; even and odd permutations; alternating groups A_n. Dihedral groups D_n; rotation groups of regular polyhedra. Groups of invertible matrices $GL(n)$. Automorphism group $\mathrm{Aut}(G)$ of a group.
- Partitions and equivalence relations.
- Homomorphism theorems for groups.
- Direct and semidirect products—external construction and internal characterization.
- Finitely generated abelian groups: invariant factor decomposition, elementary divisor decompostion. Use of Smith normal form to compute the invariant factor decompostion of a group presented as $\mathbb{Z}^n/K$.
- Group actions. Orbits and stablizers. Conjugacy classes and centralizers. Conjugacy classes in S_n. Burnside's Lemma and its applications. Cauchy's theorem. Solvability of finite p-groups.
- Divisibility, factorization into irreducibles, GCD for polynomials.
- Rings (commutative rings with identity only) and fields. Subrings. Group of units in a ring. Direct sum of rings. Ring homomorphisms, ideals, quotient rings. Ideal generated by a set of elements in a (commutative) ring.
- Polynomial rings and evaluation homomorphisms.
- Homomorphism theorem and factorization theorem for rings.
- Integral domains. Factorization, irreducible and prime elements, units and associates, GCD in an integral domain. Field of fractions of an integral domain.
- PID's and UFD's. Every PID is a UFD. Gauss's Lemma. Polynomial rings over a UFD are UFD's. Factorization and GCD in a UFD. Rational root test for a polynomial in $R[x]$ to have a root in $Q(R)$, when R is a UFD.
- Prime ideals and maximal ideals. Characterization of prime ideals by R/I being an integral domain; of maximal ideals by R/I being a field. Implications relating (p) prime, (p) maximal, p prime, and p irreducible in PID's and UFD's.

- Bases and dimension of finite-dimensional vector spaces over a field.
- Dimension of a field extension $K \subseteq L$. Finite and algebraic extensions. Formula $\dim_K(M) = \dim_K(L)\dim_L(M)$ for $K \subseteq L \subseteq M$. Minimal polynomial and description of $K(\alpha)$ for an element α algebraic over K. Adjoining algebraic elements to a field. How to calculate in $K(\alpha)$.
- Characteristic of a field. Existence of finite field $\mathbb{F}(q)$ of characteristic p and order $q = p^n$ for every prime p and positive integer n. Multiplicative group $\mathbb{F}(q)^\times$ is cyclic.
- Automorphism group $\mathrm{Aut}_K(L)$ of a field extension and fixed field $\mathrm{Fix}(H)$ of a subgroup $H \subseteq \mathrm{Aut}_K(L)$.
- Existence and uniqueness of splitting fields. Action of $\mathrm{Aut}_K(L)$ on the roots of $f(x)$ when L is the splitting field of $f(x)$ over K.
- Separable polynomials; derivative test.
- Galois extensions. Characterization of Galois extensions (Goodman 9.4.15-17). Galois correspondence (Goodman 9.5.4). You should understand the statements of these theorems and be able to apply them to examples involving fields contained in $\mathbb{C}$.

Note: the definition of a Galois extension $K \subseteq L$ is that $\mathrm{Fix}(\mathrm{Aut}_K(L)) = K$. For $K \subseteq L \subseteq \mathbb{C}$ this is Goodman 7.5.7; for the general case it's in the paragraph preceding Theorem 9.4.15.

2. Review exercises

Below are suggested exercises for review. Most of these exercises are similar to the sorts of questions I might ask on an exam. Some of the multi-part exercises have more parts than an exam question would have, although the individual parts might be typical of exam questions.

I have also thrown in a few questions that are longer or more difficult than I would put on an exam, but which serve to illustrate some interesting or important point.

Express the greatest common divisor of 42, 70, and 105 as a linear combination of these three integers.

Prove that if $a^2 \equiv b^2 \pmod{n}$, and $a \not\equiv \pm b \pmod{n}$, then n is composite (*i.e.*, not prime). Given such an a and b, how can you find a proper factor of n?

Let a, b be elements of a group G, with orders $\mathrm{ord}(a) = k$, $\mathrm{ord}(b) = l$.

(a) Prove that if $ab = ba$ then $\mathrm{ord}(ab)$ divides the least common multiple of k and l.

(b) Show that the conclusion of (a) does *not* have to hold if a and b don't commute, by finding elements a of order 2 and b of order 3 in S_4 such that ab has order 4.

Prove that if G is a group of order 20, then $a \in G$ satisfies $a^4 = 1$ if and only if $a = b^5$ for some $b \in G$. Hint for "only if:" what is a^5?

Show that no two of the groups $(\mathbb{Q}, +)$, $(\mathbb{Q}^\times, \cdot)$ and $(\mathbb{Q}_{>0}, \cdot)$ are isomorphic. Hint: describe the elements of finite order and the elements of the form x^2 (or $2x$ if written additively) in each group.

Let $\phi\colon G \to H$ and $\psi\colon H \to K$ be group homomorphisms. Prove that the kernel of $\psi \circ \phi$ is $\phi^{-1}(K)$, where $K = \ker(\psi)$.

What are all the elements of the subgroup of $\mathbb{Q}^\times$ generated by 2 and 3? Show that this subgroup is isomorphic to $\mathbb{Z} \times \mathbb{Z}$.

Show that $(1\,2)(3\,4)$ and $(3\,4\,5)$ do not generate S_5.

(a) Find the largest conjugacy class in S_4.
(b) Find an element of S_4 whose centralizer is as small as possible, and find this centralizer.

In the permutation group S_6, define $s = (1\,2\,3\,4\,5\,6)$ and $t = (1\,6)(2\,5)(3\,4)$.
(a) Show that $tst = s^{-1}$.
(b) What is the order of the subgroup $\langle s, t\rangle$ generated by s and t?
(c) Find an isomorphism between $\langle s, t\rangle$ and some more familiar group.
(d) How would you generalize the results of this exercise with 6 replaced by any positive integer n?

Show that the map sending $[x]_{n^2}$ to $[x]_n$ is a well-defined, surjective homomorphism from $\mathbb{Z}_{n^2}^\times$ to $\mathbb{Z}_n^\times$.

Show that the map sending $[x]_n$ to $[1 + nx]_{n^2}$ is a well-defined, injective homomorphism from $(\mathbb{Z}_n, +)$ to $\mathbb{Z}_{n^2}^\times$, and that its image is equal to the kernel of the homomorphism in the previous exercise.

Are the rotation groups of the cube and the octahedron isomorphic? Why or why not?

Show that the set $SL(n, \mathbb{Z})$ of $n \times n$ integer matrices with determinant 1 is a subgroup of $GL(n)$.

Show that the upper triangular matrices in $SL(2, \mathbb{Z})$ form a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}$.

(a) Find a group of order 24 in which every element has order 1, 2, 3 or 6.
(b) Find a group of order 24 in which every element has order 1, 2, 3 or 4.

Prove that if $g_1H, \ldots, g_nH$ are all the distinct left cosets of a subgroup $H \subseteq G$, and $h_1K, \ldots, h_mK$ are all the distinct left cosets in H of a subgroup $K \subseteq H$, then g_ih_jK are all the distinct left cosets of K in G. Deduce that if $K \subseteq H \subseteq G$ are subgroups, and $[G : H]$ and $[H : K]$ are finite, then $[G : K] = [G : H][H : K]$, even if G is not a finite group.

Let $Z(G)$ denote the center of G. Prove that if N is a normal subgroup of G, then $Z(G)N/N$ is contained in the center of G/N. Find an example in which $Z(G/N)$ is strictly larger than $Z(G)N/N$.

Prove that if $G = N \rtimes K$ is a semidirect product, and the action of K on N by conjugation is trivial, then $G = N \times K$. In other words, the semidirect product is a direct product in this case.

(a) Show that multiplication in $\mathbb{Z}_n$ defines an action $\alpha\colon \mathbb{Z}_n^\times \to \mathrm{Aut}(\mathbb{Z}_n)$ of $\mathbb{Z}_n^\times$ on $\mathbb{Z}_n$ by group automorphisms.
(b) Show that the matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},$$

where $a \in \mathbb{Z}_n^\times$ and $b \in \mathbb{Z}_n$, form a subgroup of the group of invertible matrices with entries in $\mathbb{Z}_n$.
(c) Show that the semidirect product $\mathbb{Z}_n \rtimes_\alpha \mathbb{Z}_n^\times$ constructed from the action in (a) is isomorphic to the group of matrices in (b).

Let G be the set of $n \times n$ real matrices A such that A has exactly one non-zero entry in every row and column. Let $T \subseteq G$ be the set of invertible diagonal matrices. Let $W \subseteq G$ be the set of matrices with exactly one entry equal to 1 in every row and column, and all other entries equal to 0.

(a) Show that G is a subgroup of $GL(n)$.

(b) Show that T and W are subgroups of G, and that T is a normal subgroup.

(c) Show that W is isomorphic to S_n.

(d) Show that G is a semidirect product $G = T \rtimes W$.

Let N be the subgroup of $\mathbb{Z}_8 \times \mathbb{Z}_{12}$ generated by $([6]_8, [6]_{12})$. Find a direct product of cyclic groups isomorphic to $(\mathbb{Z}_8 \times \mathbb{Z}_{12})/N$.

(a) Find the invariant factor decompostion of $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3$.

(b) Find the Smith normal form of the diagonal matrix

$$\begin{pmatrix} 8 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

without performing any matrix computations.

Prove that if A is an abelian group of order 20, then A is cyclic if and only if A has an element of order 4.

Find a chain of normal subgroups

$$\{e\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = D_8$$

such that each N_i/N_{i-1} is abelian (such a chain must exist, since D_8 has order 2^4). What is the smallest possible value k for the number of steps in such a chain?

Suppose the alternating group A_5 acts transitively (*i.e.*, with just one orbit) on a set X of size $|X| = 12$. Show that the stabilizer of each $x \in X$ is a cyclic subgroup generated by a 5-cycle.

How many ways are there to color the vertices of a 10-gon red and blue with 5 of each color, up to symmetry by rotations in the plane, but not flips?

Goodman Exercise 5.3.7(b)

Compute the gcd of $f(x) = 9x^3 + 2x - 1$ and $g(x) = 6x^2 - 8x + 2$ in $\mathbb{Q}[x]$. Express it as a linear combination of $f(x)$ and $g(x)$.

Compute the gcd of $f(x) = 9x^3 + 2x - 1$ and $g(x) = 6x^2 - 8x + 2$ in $\mathbb{Z}[x]$. Is it possible to express it as a linear combination of $f(x)$ and $g(x)$?

Goodman Exercise 6.2.6

Goodman Exercise 6.5.8

First two sentences of Goodman Exercise 6.5.17

Goodman Exercise 6.5.21

Prove that $x^3y - 2xy + x^5$ is irreducible in $\mathbb{R}[x, y]$. Hint: observe that it is irreducible in $\mathbb{R}(x)[y]$.

Let a and b be non-zero elements of a UFD R, and let d be a gcd of a and b. Show that $m = ab/d$ is a least common multiple of a and b. That is, both a and b divide m, and m divides every common multiple of a and b.

Note that the expression ab/d denotes an element of the fraction field of R, but since d divides ab, this element is actually in R.

Prove that if f and g are relatively prime elements of a UFD R, then the intersection of the principal ideals (f) and (g) is equal to (fg).

Show that if a and b are elements of a field K, and $a \neq b$, then the ring $K[x]/((x-a)(x-b))$ is isomorphic to $K \oplus K$. Start by finding a homomorphism from $K[x]$ to $K \oplus K$ whose kernel is $((x - a)(x - b))$.

Show that the condition $a \neq b$ in the previous exercise cannot be omitted, by proving that the rings $K[x]/((x - a)^2)$ and $K \oplus K$ are not isomorphic. Hint: consider elements r satisfying $r^2 = 0$ in each ring.

Let $\phi\colon \mathbb{Q}[x, y] \to \mathbb{Q}[t]$ be the evaluation homomorphism $p(x, y) \mapsto p(t^2, t^3)$.

(a) Show that the image S of ϕ consists of all polynomials $f(t)$ in which t^1 has coefficient zero. In particular, this set S is a subring of $\mathbb{Q}[t]$.

(b) Show that the ideal $(y^2 - x^3)$ is contained in the kernel of ϕ, and use this to define a surjective homomorphism $\overline{\phi}\colon \mathbb{Q}[x, y]/(y^2 - x^3) \to S$

(c) Show that every element of $\mathbb{Q}[x, y]/(y^2 - x^3)$ can be expressed in the form $a(x) + yb(x)$ (more precisely, as the congruence class of $a(x) + yb(x)$).

(d) Show that $\overline{\phi}$ is injective, and therefore $\mathbb{Q}[x, y]/(y^2 - x^3) \cong S$.

(e) Deduce that $(y^2 - x^3)$ is a prime ideal in $\mathbb{Q}[x, y]$.

Prove that $(x^2 - 2, y - 1)$ is a maximal ideal in $\mathbb{Q}[x, y]$.

(a) Show that $x^3 + 2x + 2$ is irreducible in $\mathbb{Q}[x]$ and has only one real root.

(b) Let $L = \mathbb{Q}[x]/(x^3 + 2x + 2)$. Show that L is a field isomorphic to $\mathbb{Q}(\beta)$, where β is the real root of $x^3 + 2x + 2$.

(c) Show that $\mathrm{Aut}_{\mathbb{Q}}(L)$ is the trivial group. In particular, L is not a Galois extension of $\mathbb{Q}$.

There are eight monic polynomials of degree 4 over $\mathbb{Z}_2$, of which three are irreducible.

(a) Find the irreducible ones by eliminating the five which factor.

(b) Since $\mathbb{F}(16)^\times$ is isomorphic to $\mathbb{Z}_{15}$, there are $\phi(15) = 8$ elements $\alpha \in \mathbb{F}(16)$ such that α has order 15 in $\mathbb{F}(16)^\times$, *i.e.*, such that α generates $\mathbb{F}(16)^\times$ as a cyclic group. These eight elements must be the roots of two of the degree 4 irreducible polynomials in (a) (four roots each), with the roots of the third one having order less than 15 in $\mathbb{F}(16)^\times$.

Which one of the three irreducible polyomials in (a) has roots of order less than 15 and what is their order in $\mathbb{F}(16)^\times$?

(a) Show that no expression involving only rational numbers, arithmetic operations (addition, subtraction, multiplication and division) and square roots can be equal to $\sqrt[3]{2}$.

(b) Show the same for $\sqrt[n]{2}$ if n is not a power of two.

Goodman Exercise 7.3.11

Goodman Exercise 7.4.3(b).

Let $\omega = e^{2\pi i/5}$.

(a) Show that $\mathbb{Q} \subset \mathbb{Q}(\cos 2\pi/5) \subset \mathbb{Q}(\omega)$ and that no two of these fields are equal. (To show that $\cos 2\pi/5$ is irrational, find its minimal polynomial and show that it is irreducible over $\mathbb{Q}$.)

(b) Deduce from (a) that the minimal polynomial of ω over $\mathbb{Q}$ has degree at least 4.

(c) Show that ω is a root of $f(x) = x^4 + x^3 + x^2 + x + 1$. Hint: use $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$. Deduce that $f(x)$ is the minimal polynomial of ω.

(d) Find all the complex roots of $f(x)$ and show that $\mathbb{Q}(\omega)$ is its splitting field.

(e) Determine the Galois group $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega))$ and its action on the roots of $f(x)$.

Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

(a) Show that L is the splitting field over $\mathbb{Q}$ of $f(x) = (x^2 - 2)(x^2 - 3)$, hence $\mathbb{Q} \subseteq L$ is a Galois extension.

(b) Find a basis of L over $\mathbb{Q}$ and give the rule for multiplying two elements of L expressed as linear combinations of the basis elements.

(c) Find the Galois group $\mathrm{Aut}_{\mathbb{Q}}(L)$ and describe its action on the roots of $f(x)$.

(d) Find all intermediate fields $\mathbb{Q} \subseteq E \subseteq L$.

(e) Find the $\mathrm{Aut}_{\mathbb{Q}}(L)$ orbit of $\alpha = \sqrt{2} + \sqrt{3}$.

(f) Use (e) to find the minimal polynomial of α over $\mathbb{Q}$

(g) Deduce from (e) or (f) that $L = \mathbb{Q}(\alpha)$.

Let $Q = \mathbb{Z}_p(u)$ be the field of rational functions in one variable u over $\mathbb{Z}_p$, that is, the fraction field of $\mathbb{Z}_p[u]$.

(a) Show that $f(x) = x^p - u$ is irreducible in $\mathbb{Z}_p[u, x]$, and therefore also in $Q[x] = \mathbb{Z}_p(u)[x]$ by Gauss's Lemma.

(b) Show that in $Q(u^{1/p}) = Q[x]/(f(x))$, the element $u^{1/p}$ is a root of $f(x)$ of multiplicity p, that is, $f(x) = (x - u^{1/p})^p$. Deduce that $Q(u^{1/p})$ is the splitting field of $f(x)$ over Q, even though $f(x)$ has only one root in this field. In particular, $Q(u^{1/p})$ is not a Galois extension of Q.

(c) Part (b) implies that $f(x)$ is not a separable polynomial over Q. Verify that the derivative test also shows this.