Math 4130, Spring 2023

Note: This is just a guide, not an all-inclusive list. It is also recommended to look at the topics outlined on the *Weekly Schedule*.

Study guide: Midterm 1 (rings).

Definitions to memorize.

1. A *ring* R.
2. A *unit*, and a *zero divisor* of a ring.
3. An *ideal* of a ring R (left, right, and two-sided).
4. Types of rings: integral domain, division ring, field.
5. The *quotient ring* R/I for some two-sided ideal I, and how to add and multiply elements.
6. A *homomorphism* ϕ from a ring R to a ring S.
7. The *kernel* of a ring homomorphism.
8. A *principal ideal* and a *principal ideal domain* (PID).
9. A *maximal ideal* M of a ring R. [Best: $M \subseteq I \subseteq R \Rightarrow I = M$ or $I = R$.]
10. A *prime ideal* P of a ring R.
11. What it means for $a \mid b$, and for a and b to be *associates*.
12. What it means for an element to be *prime*, and *irreducible*.
13. What it means for a ring to be *Noetherian*.
14. What it means for a prime p in R_m to be *inert*, *split*, or *ramify*.
15. Two ideals that are *coprime*.

Useful facts and techniques.

1. Construct the subring lattice of a small finite ring, and be able to determine the ideals, subrings that aren't ideals, and subgroups that aren't subrings.
2. Examples of ideals, subrings that aren't ideals, and subgroups that aren't subrings, in various rings.
3. An ideal M is maximal iff R/M is a field. An ideal P is prime iff R/P is an integral domain.
4. Examples of both maximal ideals and prime ideals, prime ideals that aren't maximal.
5. Learn how to construct a finite field $\mathbb{F}_q$ of order $q = p^k$.
6. Know the statements of the fundamental homomorphism theorem and the correspondence theorem for rings and how to apply them.
7. The three equivalent conditions of a ring R being Noetherian (ACC, finitely generated ideals, maximal condition.)
8. Be able to state basic properties about divisibility into the language of ideals. [e.g., $a \mid b$ iff $(b) \subseteq (a)$.]
9. Be able to identify the GCD and LCM in the lattice of ideals.
10. Applying the *Sunzi remainder theorem* to show that a ring is isomorphic to a product.
11. Using Eisenstein's criterion to show that a polynomial is irreducible.

Proofs to learn.

1. If an ideal I of R contains a unit, then $I = R$.
2. The that if $\phi\colon R \to S$ is a ring homomorphism, then $\mathrm{Ker}(\phi)$ is a two-sided ideal of R.
3. Prove the isomorphism theorems for rings, assuming the results for groups.
4. The following are equivalent for commutative rings: (i) I is a maximal ideal, (ii) R/I is simple, (iii) R/I is a field.
5. An ideal P is prime iff R/P is an integral domain. [Translate the definition into the quotient ring.]
6. A ring R is an integral domain iff 0 is a prime ideal. [Just the definition.]
7. Every maximal ideal is prime. [Consider R/I.]

(8) Use Zorn's lemma to show that every ideal is contained in a maximal ideal.
(9) Show that if $m \in R$ is irreduicble, then (m) is maximal among principal ideals.
(10) Show that if $p \in R$ is prime, then it is irreducible. [Easier to work with ideals.]

Examples to know.

(1) The difference between $\langle S \rangle$ and (S). E.g., $\langle 2 \rangle$ vs. (2) in $\mathbb{Z}[x]$.
(2) The field of fractions for some basic rings (e.g., $\mathbb{Z}$, $F[x]$, $\mathbb{Z}[\sqrt{m}]$.
(3) Examples of where unique factorization fails, and how this is reflected into the language of ideals.
(4) Types of Euclidean domains:
   (a) Fields: $\mathbb{Z}_p$, $\mathbb{F}_q \cong \mathbb{Z}_p[x]/(f(x))$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{m})$.
   (b) Euclidean domains: $\mathbb{Z}$, $F[x]$, R_m $(m = -1, -3, -7, -11, 2, \dots)$
   (c) Principal ideal domains (PIDs): R_{-19}, all Eulidean domains, fields.
   (d) UFDs: $\mathbb{Z}[x]$, $F[x, y]$
   (e) non-UFDs: Most R_m (e.g., R_{-5}, R_{-14}, R_{-30}).
   (f) $2\mathbb{Z}$ is a counterexample for several results that require R to have unity.
(5) Maximal ideals and the resulting quotient field.
(6) Examples of a primes p in some R_m that are *inert*, *split*, and *ramify*.

Study guide: Midterm 2 (group extensions).

Definitions to memorize.

(1) A group G that is an *extension* of Q by N.
(2) An *exact sequence* $\cdots \xrightarrow{\phi_0} G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \xrightarrow{\phi_3} \cdots$.
(3) Different types of extensions: *abelian*, *central*, *simple*, and *split*.
(4) What it means for a short exact sequence to be *right split*, and *left split*.
(5) A *simple group*.
(6) A *subnormal series* of G.
(7) A *normal series* of G.
(8) A *composition series* of G, and the *composition factors*.
(9) The *commutator* of elements $x, y \in G$.
(10) The *commutator subgroup* of G, and the *abelianization*.
(11) The *derived series* of G.
(12) The *ascending central series* and *descending central series*.

Useful facts and techniques.

(1) How to encode an extension of Q by N as a short exact sequence.
(2) If short exact sequence $N \hookrightarrow G \twoheadrightarrow Q$ is right split, then $G \cong N \rtimes Q$, and if it is left split, then $G \cong N \times Q$.
(3) Be able to recognize when $G \cong N \rtimes H$ and $G \cong N \times H$ just from the subgroup lattices (lattice complements).
(4) The alternating group A_n is simple for $n \neq 4$.
(5) Several equivalent characterizations of solvable groups: (all composition factors are cyclic; there is a subnormal series with abelian factors; the derived series reaches the bottom).
(6) How to construct the derived series from the subgroup lattice, by inspection.
(7) How to construct the ascending and descending central series from the subgroup lattice, by inspection. The chutes and ladders diagram is a great way to practice.
(8) If G is nilpotent, then the ascending and descending series will have the same length.
(9) Understand what the Jordan-Hölder theorem says, and how to interpret it in terms of the subgroup lattice.

Proofs to learn.

(1) If $N \xrightarrow{\iota} G \xrightarrow{\pi} Q$ is exact, then ι is injective and π is surjective.
(2) G is solvable iff G/N and N are solvable.
(3) p-groups are nilpotent
(4) nilpotent groups are solvable.
(5) the equivalence of the three characterizations of solvable groups (see above).
(6) $G' \trianglelefteq G$ and G/G' is abelian.
(7) $\phi([x, y]) = [\phi(x), \phi(y)]$ and $\phi([H, K]) = [\phi(H), \phi(K)]$
(8) The central series lemma: If $N \leq H \leq G$, and $N \leq G$, then $H/N \leq Z(G/N)$ iff $[G, H] \leq N$.
(9) If $[G, H] \leq N$ and $[G, K] \leq N$, then $[G, HK] \leq N$. (Use the central series lemma).

Examples to know.

(1) All nilpotent groups are solvable.
(2) All p-groups are nilpotent (and hence solvable).
(3)
(4) Learn the 6-7 equivalent conditions of a finite group G being nilpotent.
(5) The smallest nonabelian simple groups (A_5, $\mathrm{GL}_3(\mathbb{Z}_2)$, A_6, ...)
(6) The smallest nonsolvable groups are A_5 (simple, order 60), S_5, $A_5 \times C_2$, $\mathrm{SL}_2(\mathbb{Z}_5)$ (order 120), $\mathrm{GL}_3(\mathbb{Z}_2)$ (simple, order 168), $A_5 \times C_3$ (order 180), and eight groups of order 240.

(7) The 3-4 smallest nonnilpotent groups (these are more common).
(8) Be able to construct series (composition, derived, ascending, descending) of examples of groups (e.g., abelian, simple, A_n, S_n, D_n, etc.)
(9) How to interpret a solvable or nilpotent group as a being constructed as a sequence of extensions.

Study guide: Final exam (field and Galois theory portion).

Definitions to memorize.

(1) A *field* F.
(2) A *field automorphism* of F.
(3) The *degree* $[E:F]$ of a field extension E of F.
(4) What it means for a number $\alpha \notin \mathbb{Q}$ to be *algebraic*.
(5) What it means for a field to be *algebraically closed*.
(6) The *Galois group* of a field extension, and of a polynomial.
(7) The *minimal polynomial* of a number $r \notin F$.
(8) A *primitive element* α of a field extension.
(9) What it means for an extension field E of F to be *normal*.

Useful facts and techniques.

(1) Use Eisenstein's criterion to show that a particular polynomial is irreducible.
(2) The degree of an extension $\mathbb{Q}(r)$ is the degree of the minimal polynomial of r.
(3) Every finite extension of $\mathbb{Q}$ has a primitive elemente.
(4) The Galois group of $f(x)$ acts on its n roots, and so $\mathrm{Gal}(f(x)) \leq S_n$. If $f(x)$ is irreducible, then this action has only one orbit.
(5) $|\mathrm{Gal}(f(x))| = [K:\mathbb{Q}]$, where K is the splitting field of $f(x)$.
(6) Know the statement of the Fundamental Theorem of Galois theory.
(7) Summarize in a few sentences how to construct a degree-5 polynomial that is not solvable by radicals.

Proofs to learn.

(1) If $\phi \in \mathrm{Gal}(K:\mathbb{Q})$, then $\phi(x) = x$ for every $x \in \mathbb{Q}$.

Examples to know.

(1) Know the Galois groups of the following field extensions and be able to describe the explicit automorphisms: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, $\mathbb{Q}(\sqrt[4]{2}, i)$, and $\mathbb{Q}(\zeta_n)$, where ζ_n is an n^{th} root of unity.
(2) Be able to construct the subfield lattices of the above fields, and demonstrate the Galois correspondence with subgroups of $\mathrm{Gal}(f(x))$, for some $f(x) \in \mathbb{Q}[x]$.
(3) Given a familiar subgroup and subfield lattice, identitfy which subgroups are normal, and which subfields are normal.
(4) Know the Galois groups of the following polynomials: $f(x) = x^n - 1$, $f(x) = x^2 - 2$, $f(x) = (x^2-2)(x^2+1)$, $f(x) = x^3 - 2$, $f(x) = x^4 - 2$, $f(x) = x^5 - 2$, $f(x) = x^6 - 2$, $f(x) = x^8 - 2$.