Math 361 Quiz Material

Let R be a ring, and let L/K be an extension of fields.

- What does it mean to say $p \in R$ is *prime*? a *unit*?, *irreducible*?
- What does it mean to say that R is an *integral domain*.
- Let R be a integral domain, and let $a, b, c \in R$. Suppose that $a \neq 0$ and $ab = ac$. Prove that $b = c$. (Warning: since R is not a field, we can't assume that a has a multiplicative inverse. Also, where do we use the fact that R is a integral domain?)

- What does it mean to say that $I \subseteq R$ is an *ideal*?
- What does it mean to say that $I \subseteq R$ is *finitely-generated*?
- What does it mean to say that $I \subseteq R$ is a *principal ideal*?
- What is the general relationship between prime elements and irreducible elements of R? What if R is a PID?
- Let K be a field. State the *division algorithm* for $K[x]$.
- Let K be a field. Explain at a high level (i.e., assuming standard results from algebra) why $K[x]$ is a UFD.

Let L/K be an extension of fields.

- Let $\alpha \in L$. What is $K(\alpha)$ and what is $K[\alpha]$?
- What does it mean to say $\alpha \in L$ is *algebraic* over K?
- If $\alpha \in L$ is algebraic over K, what is the *minimal polynomial* for α over K?
- Suppose $\alpha \in L$ is algebraic over K, and let p be the minimal polynomial for α over K. What is $[L : K]$ in terms of p?
- If $[L : K] < \infty$ and $\alpha \in L$, is it necessarily true that α is algebraic over K?
- What is the set of *algebraic numbers* $\mathbb{A}$? What is the set of *algebraic integers* $\mathfrak{O}$?
- What does it mean to say M is a *finitely generated* R-module?
- Let M be a finitely generated R-module. What does it mean for M to be *free*. Up to isomorphism, what do finitely generated free R-modules look like?

- Let $A \subseteq B$ be an extension of domains, and let $\alpha \in B$.
  - What does it mean for α to be *integral* over A?z
  - Prove that if there exists a finitely generated A-module $M \subset B$ such that $\alpha M \subseteq M$, then α is integral over M. (Recall our theorem that gives two conditions that are equivalent to α being integral over A.)
- What does Gauss's lemma say about factorization of polynomials with integer coefficients?
- Why is an algebraic integer always algebraic over $\mathbb{Q}$? How can you characterize an algebraic integer in terms of its minimal polynomial?
- What is a *number field*? What is the *ring of integers* in a number field?
- State the *primitive element theorem.*
- Let $d \neq 0, 1$ be a square-free integer. Identify the ring of integers in $\mathbb{Q}(\sqrt{d})$?

- Let K be a number field. How would you describe all of the field embeddings $K \to \mathbb{C}$ using the primitive element theorem and minimal polynomials?
- Define the *discriminant* of a $\mathbb{Q}$-basis for a number field.
- Under what circumstance do we know the discriminant is an integer?
- State the change of basis formula for the discriminant.
- Let $K = \mathbb{Q}(\theta)$ be a number field of degree n. Find a nice form for $\Delta[1, \theta, \ldots, \theta^{n-1}]$.
- Theorem 1 in the lecture notes for Friday Week 3 shows that the ring of integers in a number field K is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.
  - What does it mean to be *a free $\mathbb{Z}$-module of rank n*?
  - What criterion does the beginning of the proof of Theorem 1 introduce to guarantee that a $\mathbb{Q}$-basis for K is actually a $\mathbb{Z}$-basis for the ring of integers?

Let K be a number field, and let $\alpha \in K$.

- What is the *field polynomial* for α?
- Define the *norm* and *trace* of α.
- Why is it the case that if $\alpha \in \mathfrak{O}_K$, then $N(\alpha), T(\alpha) \in \mathbb{Z}$? (Appeal to known properties of the field polynomial f_α.)

- If $\alpha \in \mathfrak{O}_K$, how can we use the norm to determine if α is a unit?
- Let $\zeta = e^{2\pi i/p}$ for some prime p, and consider the cyclotomic field $K = \mathbb{Q}(\zeta)$.
  1. What is $[K : \mathbb{Q}]$?
  2. What is the minimal polynomial f for ζ? What is the trick for showing f is irreducible?
  3. What is an integral basis for $\mathfrak{O}_K$?

- Let M be an R-module. What does it mean to say the M is *finitely generated* as an R-module?
- Let M be an R-module. What does it mean to say that M is *Noetherian*?
- What are the two conditions we proved are equivalent to M being Noetherian? (One was in terms of ascending chains of submodules and the other had to do finding maximal submodules.)
- What does it mean to say that a sequence of R-module mappings $M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$ is *exact* at M?
- What is a short exact sequence of R-modules?
- What can we say about the Noetherian property and short exact sequences?
- State the *Hilbert basis theorem.*

- What is a *Euclidean domain*?
- What does it mean for a domain to be *integrally closed*?
- What is a Dedekind domain and why do we care?
- What is a *fractional ideal*?

- What is the Smith normal form for an integer matrix?
- What is the structure theorem for finite abelian groups?
- Given a small integer matrix M, be able to find $\mathbb{Z}$-invertible matrices P and Q such that PMQ is diagonal.

- For simplicity, suppose that M is a square integer matrix. Using integer row and column operations, suppose you have reduced M to a diagonal matrix $D = \mathrm{diag}(s_1, \ldots, s_n)$. Using D describe the structure of $\mathrm{cok}(M)$ as a finitely generated abelian group. What does $\det(M)$ tell us in this context?

- How does the Smith normal form allow us to determine the structure of $\mathfrak{O}_K/\mathfrak{a}$ for an ideal $\mathfrak{a}$ in the number ring $\mathfrak{O}_K$?

  (i) What is the relevant commutative diagram that allows us to turn this question into a question about matrices?

  (ii) What is the size of $\mathfrak{O}_K/\mathfrak{a}$ in terms of this matrix?

- What is the norm of an ideal in a number ring?

- How does it related to the discriminant of the ideal?

- Why is the norm of an ideal and element of the ideal?

- Prove that if $\mathfrak{p}$ is a prime ideal in a number ring, then (i) $\mathfrak{p}$ contains a *unique* rational prime p, and (ii) $N(\mathfrak{p}) = p^m$ for where $1 \leq m \leq n$. (Here, n is the degree of the extension.)