Math 361 Quiz topics

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.

- 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* $\mathfrak{O}$?
- Let M be a finitely generated R-module. What does it mean for M to be *free*. Up to isomorphism, what do finitely generated 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?

- 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?