Harvard Math 129: Algebraic Number Theory

Sketches of Solutions to the Midterm

William Stein

March 16, 2005

These are sketches of solutions to the exam. I have written them so that you, having worked on the exam, can easily see what the answer is to each question. (Note: These solutions are slightly more abbreviated than I would have liked for your solutions.)

1. (20 points) Let R be a noetherian integral domain, and let $K = \mathrm{Frac}(R)$ be the field of fractions of R. Let $\overline{K}$ be an algebraic closure of K. Let $\overline{R}$ be the set of $\alpha \in \overline{K}$ such that there is a nonzero monic polynomial $f(x) \in R[x]$ with $f(\alpha) = 0$. Is $\overline{R}$ necessarily a ring? Prove or give a counterexample.

   This is true. The proof is exactly like the one we gave in the book for $R = \mathbb{Z}$, but everywhere that we put $\mathbb{Z}$ and $\overline{\mathbb{Z}}$ there put R and $\overline{R}$.

2. (10 points) Let $\mathcal{O}_K$ be the ring of integers of a number field K, and suppose K has exactly $2s$ complex embeddings. Prove that the sign of the discriminant of $\mathcal{O}_K$ is $(-1)^s$.

   We proved in class that

   $$d_K = \det(A)^2 = ((-2i)^{-s} \cdot \mathrm{Vol}(V/\sigma(\mathcal{O}_K)))^2$$

   The right hand side is

   $$((-2)^{-s} \cdot \mathrm{Vol}(V/\sigma(\mathcal{O}_K)))^2 \cdot i^{-2s} = \alpha \cdot i^{-2s} = \alpha \cdot (-1)^s,$$

   where α is a positive real number, since it is the square of a real number. Thus the sign of d_K is $(-1)^s$.

3. Suppose K is a number field. For any finite extension L of K, define set-theoretic maps

$$\Psi_L : C_K \to C_L, \qquad [I] \mapsto [I\mathcal{O}_L]$$
$$\Phi_L : C_L \to C_K, \qquad [I] \mapsto [I \cap \mathcal{O}_K],$$

where $[I]$ denotes the class of the nonzero integral ideal I.

(a) (10 points) Is Ψ_L a group homomorphism? Prove or give a counterexample.

Yes, Ψ_L is a group homomorphism. It is well defined because $I = (\alpha)$ maps to $\alpha\mathcal{O}_L$, which is principal. It is a homomorphism since $I\mathcal{O}_L J\mathcal{O}_L = IJ\mathcal{O}_L$.

(b) (10 points) Is Φ_L a group homomorphism? Prove or give a counterexample.

The map Φ_L is not even well defined, so it can't be a group homomorphism. It does induce a set-theoretic map on ideals. However, it need not send principal ideals to principal ideals. For example, suppose $\wp \subset \mathcal{O}_K$ is a prime ideal that is not principal. Then (as we'll see below), there is an extension L of K such that $I = \wp\mathcal{O}_L = (\alpha)$ is principal. But $I \cap \mathcal{O}_K = \wp$, since $\wp$ is contained in this intersection, and $\wp$ is maximal. Thus the image of a principal need not be principal.

(c) (20 points) Prove that there is a number field L such that Ψ_L is the 0 map, i.e., Ψ_L sends every element of C_K to the identity of C_L. [Hint: Use finiteness of C_K in two ways.]

Let $I \in \mathcal{O}_K$ be a nonzero ideal. The class group C_K is finite, so there is an integer n such that $[I]^n$ is trivial, so $I^n = (\alpha)$ is principal. Let $L = K(\alpha^{1/n})$. Let $J = I\mathcal{O}_L$. Then

$$(J/(\alpha^{1/n}\mathcal{O}_L))^n = J^n/(\alpha\mathcal{O}_L) = (I^n\mathcal{O}_L)/(\alpha\mathcal{O}_L) = \alpha\mathcal{O}_L/\alpha\mathcal{O}_L = \mathcal{O}_L,$$

where we've used that our observation that the process of extending an ideal to $\mathcal{O}_L$ preserves multiplication to see that $J^n = I^n\mathcal{O}_L$. By unique factorization of ideals in $\mathcal{O}_L$ and the fact that the fractional ideals are a torsion free group, we see that $J/(\alpha^{1/n}\mathcal{O}_L)$ is the unit ideal (since its nth power is the unit ideal). Thus $J = (\alpha^{1/n}\mathcal{O}_L)$ is principal, which proves the claim.

(Note: I wonder, is there always an L such that Φ_L is the 0 map? This question just occured to me while writing this exam. If you find an answer and tell me the answer, I'll be very thankful, though this is not part of the official exam. This question is related to "visibility of Mordell-Weil groups", which I just wrote a paper about.)

This question is meaningless since Φ_L is not well defined. Also as mentioned above the induced map on sets of fractional ideals is surjective.

4. A number field is *totally real* if every embedding is real, i.e., $s = 0$, and a number field is *totally complex* if every embedding is complex, i.e., $r = 0$.

   (a) (15 points) Find with proof the possible degrees of totally real fields.

   Every degree appears. The field $\mathbb{Q}$ is totally real, so it suffices to prove that every degree > 1 occurs. Let $K = \mathbb{Q}(\zeta_n + 1/\zeta_n)$ where n is a primitive nth root of unity. Then for $3 \geq 2$, K has degree $\varphi(n)/2$, and is a Galois extension of $\mathbb{Q}$ with cyclic Galois group, so there is a subfield of K of degree d for each divisor d of $\varphi(n)/2$. If p^r is a prime power, then $p^r \mid \varphi(p^{r+1})$, etc., so we see pretty easily that if m is any integer then there exists n such that $m \mid \varphi(n)/2$.

   (b) (15 points) Find with proof the possible degrees of totally complex fields.

   Since $n = r + 2s$, if $r = 0$ then n is even. In fact every even degree appears. If K is totally real and $i = \sqrt{-1}$, then $K(i)$ is totally complex, since there is no real number α with $\alpha^2 = -1$, so there's no way to embed $K(i)$ into $\mathbb{R}$. The degree of $K(i)$ is twice the degree of K. As we saw in the previous part of this problem, every possible degree occurs for totally real fields, so twice every degree occurs for totally complex fields.