18.786: Topics in Algebraic Number Theory (spring 2006)
Problem Set 6, due Thursday, April 6

Reminder: this course has one in-class midterm, scheduled for Thursday, April 6, the same day as this problem set is due. The intent is for the midterm to be pretty easy: to that end, I'll allow open book and notes (but no computers), and the format will be something like "Do at least A of the following B problems now, and attach the remaining ones to the next problem set."

1. Janusz p. 78, exercise 2.

2. Janusz p. 81, exercise 5.

3. Let K be a number field, and let S be a finite set of nonzero primes in $\mathfrak{o}_K$, and write $\mathfrak{o}_{K,S}$ for the localization of $\mathfrak{o}_K$ at the multiplicative set generated by S (i.e., you take elements which generate ideals whose only prime factors are elements of S).

   (a) Prove that the torsion subgroups of $\mathfrak{o}_{K,S}^*$ and of $\mathfrak{o}_K^*$ are equal.

   (b) Prove that $\mathfrak{o}_{K,S}^*/\mathfrak{o}_K^*$ (which is torsion-free by (a)) is free of rank $\#S$. (Hint: every ideal has a power which is principal. That may not give you the entire quotient, but it's enough to prove the claim.)

   You have now extended Dirichlet's units theorem to cover "S-units".

4. Use Minkowski's bound to prove that the number field $\mathbb{Q}[x]/(x^3 - x^2 - x + 2)$ has class number 1. You may use SAGE to find the discriminant without further justification.

5. Let $P(x) \in \mathbb{Z}[x]$ be an irreducible monic polynomial whose discriminant D is squarefree. Prove that the splitting field of $P(x)$ contains and is everywhere unramified over $\mathbb{Q}(\sqrt{D})$. (This shows that Janusz, Theorem I.13.9 becomes quite false if you replace $\mathbb{Q}$ by a "random" quadratic number field.)

6. A *CM field* (for "complex multiplication") is a totally imaginary quadratic extension of a totally real number field.

   (a) Let K be a totally complex number field; then for each embedding $K \hookrightarrow \mathbb{C}$, complex conjugation on $\mathbb{C}$ induces an automorphism of K. Prove that these are all the same automorphism if and only if K is a CM field.

   (b) Prove that for any odd prime p, $\mathbb{Q}(\zeta_p)$ is a CM field.

   (c) Prove that every unit u in $\mathbb{Z}[\zeta_p]$ is equal to a power of ζ_p times a totally real element. (Hint: divide u by its conjugate.)

7. In class several lectures ago, I defined the *different* $\mathrm{Diff}(L/K)$ of an extension L/K of number fields as the ideal of $\mathfrak{o}_L$ inverse to the fractional ideal

$$\{x \in \mathfrak{o}_L : \mathrm{Trace}_{L/K}(xy) \in \mathfrak{o}_K \text{ for all } y \in \mathfrak{o}_L\}.$$

and I pointed out that it's generated by $f'_\alpha(\alpha)$ for all $\alpha \in \mathfrak{o}_K$, where f_α denotes the characteristic polynomial of multiplication-by-α on L as a K-vector space.

(a) Prove that $\mathrm{Disc}(L/K) = \mathrm{Norm}_{L/K}(\mathrm{Diff}(L/K))$.

(b) Let $M/L/K$ be a tower of number fields. Prove that as ideals of $\mathfrak{o}_M$,

$$\mathrm{Diff}(M/L)\,\mathrm{Diff}(L/K) = \mathrm{Diff}(M/K),$$

and deduce as a corollary that

$$\Delta(M/K) = \Delta(L/K)^{[M:L]}\,\mathrm{Norm}_{L/K}(\Delta(M/L)).$$

8. (a) Suppose K is a number field which contains and is unramified over the Gaussian rationals $\mathbb{Q}(i)$. Determine, up to sign, the absolute discriminant of K as a function of its absolute degree. (Hint: use the previous problem.)

   (b) Use (a) and the Minkowski discriminant bound to prove that $\mathbb{Q}(i)$ admits no nontrivial everywhere unramified extension.

9. Go to `http://www.mathpuzzle.com/`, look up the 14 Mar 2006 entry, and prove "Snevetz's Last Theorem". (Hint: guess what number field is defined by this polynomial.) Unfortunately, it's too late to collect the $500...