18.786: Topics in Algebraic Number Theory (spring 2006)
Take-home final exam, due Thursday, May 18 at the end of lecture

Please submit exactly *eight* of the following problems. As usual, each numbered item constitutes a single problem, even if it is broken up into lettered subparts, and each problem has equal value.

You may consult any resources except a human being other than me (so in particular, you may not collaborate with others in the class). This includes Janusz, other books, anything on the Internet, SAGE, other software, notes from class, problem sets, and anything else I didn't think of.

Note that I did allow for the possibility of asking me for help. Any response (including corrections if any are found) will be copied to virtual office hours so everyone receives the benefit of it.

1. Let $P(x) \in \mathbb{Z}[x]$ be a monic polynomial whose roots are all real and lie in the interval $[-2, 2]$. Prove that each root of P has the form $2\cos(2\pi r)$ for some $r \in \mathbb{Q}$.

2. (a) Put $\alpha = \sum_{i=0}^{2} \zeta_{13}^{3^i}$. Prove that $\mathbb{Z}[\alpha]$ is not the ring of integers of $\mathbb{Q}(\alpha)$.
   (b) Put $\beta = \sum_{i=0}^{4} \zeta_{31}^{2^i}$. Prove that 2 splits completely in $\mathbb{Q}(\beta)$.
   (c) Prove that the ring of integers of $\mathbb{Q}(\beta)$ is not monogenic over $\mathbb{Z}$.

3. Let $\alpha_1, \dots, \alpha_n$ be algebraic numbers such that $\alpha_1^i + \cdots + \alpha_n^i \in \mathbb{Z}$ for all positive integers i. Prove that $\alpha_1, \dots, \alpha_n$ are algebraic integers. (Hint: what is the radius of convergence of the formal power series
$$\sum_{j=1}^{n} \frac{1}{1 - \alpha_j t}$$
over $\mathbb{Q}_p$?)

4. Let K be a number field whose absolute discriminant is squarefree. Prove that K contains no proper subfield other than $\mathbb{Q}$.

5. (a) Show that the class number of $\mathbb{Q}(\sqrt{-11})$ is 1. (You may not simply take SAGE's word for this.)
   (b) Find all integers x, y such that $y^2 = x^3 - 11$.

6. Let K be the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_n)$. Let $\mathfrak{a}$ be an ideal of $\mathfrak{o}_K$ such that $\mathfrak{a}\mathbb{Z}[\zeta_n]$ is principal. Prove that $\mathfrak{a}$ is already principal.

7. Let $P(x) \in \mathbb{Z}[x]$ be a monic polynomial of *prime* degree n which is irreducible modulo some prime p, and which has exactly two nonreal roots. Prove that the Galois closure of the extension $K = \mathbb{Q}[x]/P(x)$ over $\mathbb{Q}$ has Galois group S_n.

8. Let K be a finite extension of $\mathbb{Q}_3$, and let L/K be a Galois extension with group S_3 (the symmetric group on three letters). Prove that K is wildly ramified, that is, $e(L/K)$ is divisible by 3.

9. Let K be the completion of the maximal unramified extension of $\mathbb{Q}_p$.

   (a) Prove that there is a unique continuous automorphism σ of K which induces the Frobenius $x \mapsto x^p$ on the residue field of K.

   (b) Prove that for each $x \in \mathfrak{o}_K^*$, there exists $y \in \mathfrak{o}_K^*$ such that $y^\sigma/y = x$.

10. (a) Let k be an imperfect field of characteristic $p > 0$, and suppose $c \in k \setminus k^p$. Find the integral closure R of $k[[t]]$ in

$$k((t))[z]/(z^p - z - ct^{-p})$$

   and determine $e(R/k[[t]])$ and $f(R/k[[t]])$. (Hint: the field extension is Galois.)

   (b) Exhibit an example of a finite integral extension S/R of DVRs which is not monogenic, but for which $\operatorname{Frac}(S)/\operatorname{Frac}(R)$ is separable. (Hint: if the residue field extension is not monogenic, then S/R can't be either.)