Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Final Examination
Due in my mailbox Monday, December 10 by 5 PM

Instructions. Please submit solutions to at least eight of the following problems; your best eight problems will be counted. You *may*:

- Consult Neukirch, your own lecture notes, any handouts distributed in class, your graded problem sets, or the Magma documentation.
- Invoke the statement of any result from Neukirch, from lecture, or from the problem sets (submitted or not) without proof, as long as you specify where it came from.
- Consult me or Frank with questions.
- Use Magma (or a computer algebra system of your choice) where specified.

You *may not*:

- Discuss the exam questions with anyone other than me or Frank, until after you have submitted the exam.
- Use Magma or other computational device where not directed to do so.
- Consult any reference, print or electronic, other than those mentioned above.

Problems.

Throughout the problems, let ζ_n denote a primitive n-th root of unity.

1. (a) Prove that the field $\mathbb{Q}(\zeta_{13})$ contains a unique subfield K of degree 4 over $\mathbb{Q}$, generated by $x = \zeta_{13} + \zeta_{13}^3 + \zeta_{13}^9$.
   (b) Determine the minimal polynomial and the different of x. You may use Magma for this and the next part.
   (c) Exhibit an element of $\mathfrak{o}_K$ not contained in $\mathbb{Z}[x]$. (Hint: compute the discriminant of the minimal polynomial of x first to find a square factor that you can remove.)
2. Let α be an algebraic integer all of whose conjugates in $\mathbb{C}$ are real and lie in the interval $[-2, 2]$. Prove that $\alpha = 2\cos(2\pi r)$ for some $r \in \mathbb{Q}$. (Hint: reduce to Kronecker's theorem from Problem Set 2.)
3. (a) Show that the class number of $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-11})]$ is 1. (Hint: use the bounds from Problem Set 5 to reduce this to a finite computation.)
   (b) Find all integers $x, y \in \mathbb{Z}$ such that $y^2 = x^3 - 11$.

4. Find all solutions of the equation

$$x^3 + 5y^3 + 25z^3 - 15xyz = \pm 1$$

with $x, y, z \in \mathbb{Z}$. You may use Magma to search for some small solutions. (Hint: relate this to the unit group of $\mathbb{Q}(\sqrt[3]{5})$, whose ring of integers you may assume is $\mathbb{Z}[\sqrt[3]{5}]$ without proof.)

5. Let K be a finite unramified extension of $\mathbb{Q}_p$ with valuation ring $\mathfrak{o}_K$, and let $\mathfrak{m}_K$ be the maximal ideal of $\mathfrak{o}_K$. Let σ be the unique automorphism of K such that $x^\sigma \equiv x^p \pmod{\mathfrak{m}_K}$. Prove that for any $x \in \mathfrak{o}_K$ such that $x \equiv 1 \pmod{\mathfrak{m}_K}$, there exists $y \in \mathfrak{o}_K^*$ such that $y^\sigma / y^p = x$. (Hint: imitate one proof of Hensel's lemma.)

6. Determine the number and degrees of the irreducible factors of the polynomial $x^4 + 9x^2 - 2$ over $\mathbb{Q}_2$. (Hint: make sure to apply Hensel's lemma only when valid.)

7. Let L be a number field whose absolute discriminant is squarefree and let K be a subfield of L. Prove that $K = \mathbb{Q}$. (Hint: use properties of the relative discriminant to show that $K/\mathbb{Q}$ is unramified.)

8. Let $P(x) = x^6 - x^5 - x^4 + x + 1$. You may assume $P(x)$ is irreducible over $\mathbb{Z}$.

   (a) Compute the discriminant D of $P(x)$ using Magma, and check that it is 3^3 times a squarefree number.

   (b) Let K be the normal closure of $\mathbb{Q}[x]/(P(x))$. Prove that K is unramified over all primes of $\mathbb{Q}(\sqrt{D})$ not above (3).

   (c) Prove that K is also unramified over the prime of $\mathbb{Q}(\sqrt{D})$ above (3). (Hint: determine the decomposition and inertia groups for a prime of K above (3).)

9. Let n be a positive integer which is not a prime power. Prove that $1 - \zeta_n$ is a unit in $\mathbb{Z}[\zeta_n]$. (Hint: compute $\prod_{i=1}^{n-1}(1 - \zeta_n^i)$ and show that the terms where i is not coprime to n account for all of the prime factors. For starters, try the case $n = pq$.)

10. (a) Prove that the field $\mathbb{Q}(\zeta_{31})$ contains a unique subfield K of degree 5 over $\mathbb{Q}$.

    (b) Prove that 2 is unramified and splits completely in K.

    (c) Use (b) to prove that there does not exist $\alpha \in \mathfrak{o}_K$ such that $\mathfrak{o}_K = \mathbb{Z}[\alpha]$. (Hint: derive a contradiction from the splitting criterion that holds when $\mathfrak{o}_K = \mathbb{Z}[\alpha]$.)

11. Neukirch exercise III.2.1:

    (a) Let L/K be finite extensions of $\mathbb{Q}_p$. Prove that $\mathrm{Disc}(L/K)$ is generated by $\mathrm{Disc}(1, \alpha, \ldots, \alpha^{n-1})$, where α runs over all elements of $\mathfrak{o}_L$ such that $K(\alpha) = L$.

    (b) Prove that this statement does not hold for number fields, by showing that it fails for $K = \mathbb{Q}$ and $L = \mathbb{Q}[x]/(P(x))$, where $P(x) = x^3 - x^2 - 2x - 8$. You may use without proof the fact that the discriminant of P is -2012. (Hint: show that $1, x, (x^2 + x)/2$ is an integral basis of L.)