

18.786: Topics in Algebraic Number Theory (spring 2006)
Problem Set 3, due Thursday, March 9

The last problem set was pretty tough and theoretical, so I'm putting some more concrete problems on this set. In particular, I'm going to start suggesting problems involving the most basic examples of number fields, the quadratic fields and the cyclotomic fields.

1. Janusz p. 28, exercise 3. (Hint: if you think FOO is the integral closure of BAR, to prove this you might want to first argue that FOO is integral over BAR and then that FOO is itself integrally closed.)
2. Prove that $\mathbb{F}_p(x^{1/p}, y^{1/p})$ is not a monogenic extension of $\mathbb{F}_p(x, y)$. (Hint: look at the p -th power of a putative generator.)
3. Do Janusz p. 32, exercise 6. Then describe explicitly which primes fall into which cases for $d = -1$. Optional (but recommended): do likewise for $d = 2$.
4. Janusz p. 51, exercise 4.
5. Prove that for any prime number p , the polynomial $(x^p - 1)/(x - 1)$ is irreducible over $\mathbb{Z}/p^2\mathbb{Z}$; deduce then that it's irreducible over \mathbb{Z} and also over \mathbb{Q} . (Hint: substitute $y = x - 1$ and then look up "Eisenstein's irreducibility criterion".)
6. (You may postpone this to the next pset if you prefer.) Let p be a prime and put $\zeta_p = \exp(2\pi i/p)$. Prove that $\mathbb{Z}[\zeta_p]$ is integrally closed in $\mathbb{Q}(\zeta_p)$. (Hint: as in the virtual office hours hint on PS2, get an upper bound for the integral closure using the trace pairing and then refine. Or peek ahead to Janusz I.9.)
7. (A theorem of Kronecker) Let $P(x) \in \mathbb{Z}[x]$ be a monic polynomial whose roots in \mathbb{C} all have absolute value 1. Prove that $P(x)$ divides $x^n - 1$ for some n . (Hint: for each integer m , look at the polynomial P_m whose roots are the m -th powers of the roots of P . What can you say about the coefficients of P_m ?)
8. For each squarefree integer d , find all of the roots of unity in $\mathbb{Q}(\sqrt{d})$. (Hint: if there is a p -th root of unity in $\mathbb{Q}(\sqrt{d})$, then $\mathbb{Q}(\sqrt{d})$ must contain $\mathbb{Q}(\zeta_p)$ and this usually causes dimension problems.)
9. Prove that for every prime $p < 100$, there exists a monic polynomial $P(x) \in \mathbb{Z}[x]$ whose roots in \mathbb{C} all have absolute value \sqrt{p} , such that the ratio of no two of the roots of P is an algebraic integer. These are examples of *Weil polynomials*, which occur in the study of zeta functions of function fields. (Hint: first write down some examples that work for a general class of primes. Then search by hand or computer for examples in the remaining cases. Oh, and note that the condition on the ratios can be simplified...)