18.786: Topics in Algebraic Number Theory (spring 2006)
Problem Set 4, due Thursday, March 16

Reminder: a ring extension S/R is *monogenic* if $S \cong R[x]/(P(x))$ for some polynomial $P(x) \in R[x]$. Also, $\mathfrak{o}_K$ denotes the ring of integers in a number field K.

1. Janusz p. 40, exercise 3.
2. Janusz p. 42, exercise 4.
3. Janusz p. 47, exercise 1.
4. Janusz p. 57, exercise 1.
5. Janusz p. 57, exercise 2.
6. Janusz p. 57, exercise 3.
7. Show by an example that a rational prime p can be totally ramified in two different number fields K_1 and K_2 without being totally ramified in the compositum K_1K_2. (Hint: you can do this with two quadratic extensions.)
8. (Note: after this problem set was issued, this problem was postponed to Problem Set 7.) Let $R_1 \subseteq R_2$ be an inclusion of DVRs, with R_2 finite integral over R_1, such that the residue field extension $R_2/\mathfrak{m}_{R_2}$ of $R_1/\mathfrak{m}_{R_1}$ is separable. Prove that R_2 is a monogenic extension of R_1. (Hint: first check the unramified case, where $\mathfrak{m}_{R_2} = \mathfrak{m}_{R_1}R_2$, and the totally ramified case, where $R_2/\mathfrak{m}_{R_2} = R_1/\mathfrak{m}_{R_1}$. Then combine the arguments in those two cases.)
9. (a) Let K be a number field such that $\mathfrak{o}_K$ is monogenic over $\mathbb{Z}$. Prove that for each rational prime p, there are at most p primes $\mathfrak{q}$ of $\mathfrak{o}_K$ lying over (p) with $f(\mathfrak{q}/(p)) = 1$.
   (b) Use (a) to produce an example of a number field K such that $\mathfrak{o}_K$ is not monogenic over $\mathbb{Z}$.
   (c) For your example in (b), exhibit a rational integer N such that $(\mathfrak{o}_K)[1/N]$ is monogenic over $\mathbb{Z}[1/N]$, then determine the splitting and ramification of all primes p dividing N.
10. Let K be the number field $\mathbb{Q}[x]/(x^3 - x + 2)$. Use SAGE to determine, among the primes $p < 10000$, how many have each of the possible splitting types. Then make a guess about the asymptotics (which will be confirmed by the Chebotarev Density Theorem).