18.786 Problem Set 4 - Spring 2008

Due Thursday, Mar. 13 at 1:00

Adopt the notation $\zeta_n := e^{2\pi i/n}$ and $\tilde{\zeta}_n := \zeta_n + \zeta_n^{-1}$.

1. Exercise 4 on page 42 of Janusz.

2. Exercise 4 on page 51 of Janusz.

3. (Adapted from Milne) Let $K = \mathbb{Q}[\sqrt{7}, \sqrt{13}]$. You will show that the ring of integers $\mathcal{O}_K$ is strictly larger than $\mathbb{Z}[\alpha]$ for any algebraic integer $\alpha \in K$.

   (a) Define $\alpha_1, \dots, \alpha_4$ to be the set of algebraic integers
   $$\alpha_i := (1 \pm \sqrt{7})(1 \pm \sqrt{13})$$
   in some order. Show that $3 \mid \alpha_i\alpha_j$ for any $i \neq j$, but that $3 \nmid \alpha_i^k$ for any power k (calculate the trace $T(\alpha_i^k/3)$ for the latter claim).

   (b) Now suppose that $K[\alpha] = \mathcal{O}_K$ for some algebraic α with minimal polynomial $f(x)$. Let $f_i(x) \in \mathbb{Z}[x]$ be polynomials such that $f_i(\alpha) = \alpha_i$. Show that the observations in part (a) imply that $\overline{f}(x) \mid \overline{f_i f_j}(x)$ (where the polynomials have been reduced in $\mathbb{F}_3 = \mathbb{Z}/(3)$), but $\overline{f}(x) \nmid \overline{f_i}^k(x)$. Conclude that $\overline{f}(x)$ has at least 4 distinct, irreducible factors over $\mathbb{F}_3[x]$. Explain why this contradicts the fact that $f(x)$ has degree at most 4.

   (c) Prove a more general statement regarding $\mathcal{O}_K$ for biquadratic $K = \mathbb{Q}[\sqrt{d_1}, \sqrt{d_2}]$ (at the very least, find an infinite family of fields whose rings of integers do not have power bases).

4. Exercise 2 on page 57 of Janusz.

5. Determine which of the cyclotomic fields $\mathbb{Q}[\zeta_n]$ (now including composite n) are biquadratic.

6. It can be shown (using formal derivatives of minimal polynomials) that if L/K is an inseparable field extension of degree n, then $\mathrm{char}(P) = p > 0$, and $\alpha^{p^n} \in K$ for any $\alpha \in L$. Show that this holds for the following examples:

   (a) (Finite fields) $L = \mathbb{F}_q[x]/(x^q - \beta)$ with β not equal to a q-th power in $K = \mathbb{F}_q$, where $q = p^m$ for some m.

   (b) (Function fields) $L = \mathbb{F}_p(x, y)$ and $K = \mathbb{F}_p(x^p, y^p)$.

7. (Computational) Use SAGE or PARI/GP to compute integral bases for at least 5 different number fields (not all of degree 2!).