MATH 7230 Homework 5 - Fall 2018

Due Wednesday, Oct. 17 at 1:30

https://www.math.lsu.edu/%7Emahlburg/teaching/2018F-MATH7230.html

You are required to turn in at least **one** of the following problems, and must complete a total of **20** by semester's end. Group work is allowed, but your solutions must be written up individually.

The notation "Ash A.B.C" means Problem C from Section A.B in the textbook.

Problems 1 – 2 are Ash's proof that p ramifies in L if and only if $p \mid \mathrm{Disc}_{L/\mathbb{Q}}$; we also filled in most of the details in lecture.

1. (a) Ash 4.2.1.
   (b) Ash 4.2.2.
   (c) Ash 4.2.3.
2. (a) Ash 4.2.4.
   (b) Ash 4.2.5.
   (c) Ash 4.2.6.
3. In this problem you will verify the prime ideal factorizations discussed in lecture for the ring $B = \mathbb{Z}[\zeta_5]$ (which are the algebraic integers in $L = \mathbb{Q}(\zeta_5)$; it turns out that the class number is $h_L = 1$, so all ideals are principal).
   (a) First, show that $(5)B = P^4$, where $P = (1 - \zeta_5)\, B$. In particular, calculate directly that
   $$(1 - \zeta_5)^4 \left(-1 - \zeta_5 + \zeta_5^3\right) = 5.$$
   Furthermore, show that $1 + \zeta_5 - \zeta_5^3$ is a unit by multiplying by $(1 + \zeta_5^2)^2$.
   (b) Part (a) shows that $(5)B \subset P^4$. Why can you also conclude that $P^4 \subset (5)B$?
   Hint: Use the efg-relation from Theorem 4.1.6.
   (c) Show that $(2)B = P$; i.e., that 2 is inert in B. Using Theorem 4.3.1, this requires showing that $\min_{\zeta_5,\mathbb{Q}}(X)$ is irreducible modulo 2.
4. In this problem you will consider ideal factorization in $B = \mathbb{Z}[\sqrt[3]{2}]$, which is the ring of algebraic integers in $L = \mathbb{Q}(\sqrt[3]{2})$.
   (a) Calculate the field discriminant of L.
   (b) Find the prime factorizations of $(2)B$ and $(3)B$.
   (c) Ash 4.3.3. It is also a fact that the class number of this ring is one, so all ideals are principal. You **must** write the prime ideals in your factorization as principal ideals.
   Furthermore, this is an example of a non-Galois field extension. Show that $(5) = P_1P_2$ with relative degrees $f_1 = 1$ and $f_2 = 2$ (showing that Corollary 8.1.3 does not hold).

In Problems 5 – 7 you will explore rings of algebraic integers that are somewhat more more complicated than seen in the small, typical examples of quadratic or cyclotomic extensions. In particular, you will consider examples of *biquadratic* fields $L = \mathbb{Q}(\sqrt{m}, \sqrt{\ell})$ (with m, ℓ squarefree) and see that the rings of integers B can have "unexpected" denominators, and also, do not necessarily have power bases.

5. (a) First, consider $L = \mathbb{Q}(\sqrt{2}, i)$. Recall that the rings of integers in the subextensions $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$ are $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[i]$, respectively. Show that $B \supsetneq \mathbb{Z}[1, \sqrt{2}, i, i\sqrt{2}]$.
   Hint: There are complex roots of unity other than $\{\pm 1, \pm i\}$ *in* L.

   (b) Now let $L = \mathbb{Q}(\sqrt{2}, \sqrt{6})$. It is easy to see that $\sqrt{12}$ should **not** be part of the integral basis, as instead in $\mathbb{Q}(\sqrt{12})$ one immediately has $\sqrt{3}$. But even this is not enough, as $B \supsetneq \mathbb{Z}[1, \sqrt{2}, \sqrt{6}, \sqrt{3}]$.
   Prove this by showing that $\alpha := \frac{\sqrt{2}+\sqrt{6}}{2}$ is an algebraic integer.

   (c) Continuing from part (b), it turns out α generates a power basis, so $B = \mathbb{Z}[\alpha] = \langle 1, \alpha, \alpha^2, \alpha^3 \rangle_{\mathbb{Z}}$. Prove that $\sqrt{2}, \sqrt{3}, \sqrt{6} \in \mathbb{Z}[\alpha]$.

6. [Adapted from Milne 2.2-6] In Problem 5, both examples have power bases, so $B = \mathbb{Z}[\alpha]$ for some α. However, this is not true of all number fields, as you will see in this problem. Let $L = \mathbb{Q}(\sqrt{7}, \sqrt{10})$, with ring of algebraic integers $B = \mathcal{O}_L$.

   (a) Define a set of (conjugate) algebraic integers by

   $$\alpha_1 := (1+\sqrt{7})(1+\sqrt{10}), \qquad \alpha_2 := (1+\sqrt{7})(1-\sqrt{10}),$$
   $$\alpha_3 := (1-\sqrt{7})(1+\sqrt{10}), \qquad \alpha_4 := (1-\sqrt{7})(1-\sqrt{10}).$$

   Denote the corresponding principal ideals by $P_i := (\alpha_i)$.

   Prove that for any $1 \le i < j \le 4$, $3 \mid \alpha_i \alpha_j$, so $(3)_B \mid P_i P_j$.

   (b) Calculate the trace $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i)$.

   (c) Use part (a) to show that $(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^k \equiv \alpha_1^k + \alpha_2^k + \alpha_3^k + \alpha_4^k \pmod 3$. Conclude that $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i^k) \equiv 1 \pmod 3$.
   Conclude that $\frac{\alpha_i^k}{3}$ is not an algebraic integer for any k; i.e., that $(3)_B \nmid P_i^k$.

7. This is a continuation of Problem 6. You will now show that B does not have a power basis.

   (a) Assume to the contrary that $B = \mathbb{Z}[\theta]$, with $f(X) := \min_{\theta,\mathbb{Q}}(X)$. Use the fact that

   $$\mathbb{Z}[\theta]/(3) \cong \mathbb{Z}[X]/(3, f(X)) \cong (\mathbb{Z}/3\mathbb{Z})[X]/(f(X))$$

   to conclude that for $g(X) \in \mathbb{Z}[X]$, $g(\theta) \equiv 0 \pmod 3$ if and only if $\overline{f}(X) \mid \overline{g}(X)$, where $\overline{f}$ indicates the reduction modulo 3.

   (b) Let $g_i(X)$ be defined such that $g_i(\theta) = \alpha_i$. Now use Problem 6 and part (a) to show that $\overline{f} \mid \overline{g_i g_j}$, but $\overline{f} \nmid \overline{g_i}^k$.
   Thus the factorization of $f(X)$ has at least 4 distinct factors, $f(X) \equiv f_1(X) f_2(X) f_3(X) f_4(X) f_5(X) \cdots \pmod 3$. Use degree considerations to obtain a contradiction?

(c) Give an infinite family of biquadratic fields $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ such that B does not have a power basis.

Remark: In fact, here an integral basis is

$$B = \left\langle 1, \sqrt{7}, \sqrt{10}, \frac{\sqrt{10} + \sqrt{70}}{2} \right\rangle_{\mathbb{Z}}.$$