6370-001 - FALL 2021 - WEEK 4 (9/14, 9/16)

Exercise 1

(1) Set up PARI or Sage on your computer or sign up for an account on CoCalc.
(2) Let $K = \mathbb{Q}[x]/x^3 + 3x + 12$. Use a computer algebra system to compute the factorization of (2) in $\mathcal{O}_K$.
(3) Explain why the result implies $\mathcal{O}_K$ is not monogenic over $\mathbb{Z}$ (i.e. not of the from $\mathbb{Z}[b]$ for some $b \in \mathcal{O}_K$). [In fact, it even implies the integral closure of $\mathbb{Z}_{(2)}$ in K is not monogenic over $\mathbb{Z}_{(2)}$ – why? The next exercise may help].
Can you give a geometric interpretation of your argument?
(4) Use a computer algebra system to compute the discriminant of $K/\mathbb{Q}$. Try doing it by hand!
(5) What else can your computer do? Experiment.

Exercise 2

(1) For $L/K/\mathbb{Q}$ finite extensions, show that if p ramifies in K then p ramifies in L.
(2) For p an odd prime and

$$p^* = (-1)^{\frac{p-1}{2}} p = \begin{cases} p & \text{if } p \equiv 1 \mod 4 \\ -p & \text{if } p \equiv 3 \mod 4, \end{cases}$$

show that $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$. *Hint: compute the discriminants of these fields if you didn't do those exercises already!*

Exercise 3

(1) (Milne 2-7) Let A be an integrally closed domain with field of fractions K, and let L be a finite extension of K. Let B be the integral closure of A in L. Show that, for any multiplicative system $S \subset A$, the integral closure of $S^{-1}A$ in L is $S^{-1}B$.
(2) Let A be a Dedekind domain, let $\mathfrak{p}$ be a prime ideal of A, and let $S = A\backslash\mathfrak{p}$. Explain why the factorization of $\mathfrak{p}$ in B is "the same" as the factorization of $\mathfrak{p}A_{\mathfrak{p}}$ in $S^{-1}B$.

Exercise 4

Let A be a Dedekind domain with fraction field K, and let L be a finite extension of K. Let B be the integral closure of A in L. Then B is also a Dedekind domain (the proof is very similar to the proof in the video lectures in the case of a finite extension of $\mathbb{Q}$). **In this exercise we explain a way to factorize all but finitely many primes, even when B is not monogenic over A.**

(1) Let $\mathfrak{p}$ be a prime ideal of A and $S = A\backslash\mathfrak{p}$. Suppose $b \in B$ is such that[1] $\mathrm{disc}(1, b, \ldots, b^{n-1})$ is not in $\mathfrak{p}$. Show that $S^{-1}B = A_{\mathfrak{p}}[b]$ (by exercise 3, this is the integral closure of $A_{\mathfrak{p}}$ in L)
(2) For b as above, let $f(x)$ be its minimal polynomial over K. Explain how to obtain the factorization of $\mathfrak{p}$ in B from the factorization of $f(x)$ in $A/\mathfrak{p}[x]$.
(3) Explain why this gives a strategy to find the factorization of all but finitely many of the primes of A in B.
(4) Use a computer algebra system to verify the computations of Examples 3.48-3.51 in Milne.

Note that this does not typically work for *all* primes of A – for example, this will not lead to a factorization of (2) in $\mathcal{O}_K$ for $K = \mathbb{Q}[x]/(x^3 + 3x + 12)$. We will discuss how to resolve this later.

[1]Here for any elements $e_1, \ldots e_n$ in L we write $\mathrm{disc}(e_1, \ldots, e_n) = \det(\mathrm{Tr}_{L/K}(e_i e_j)) \in K$ — see also Exercise 8.

Exercise 5
Which primes p can be written as $y^2 = a^2 + 3b^2$ for $a, b \in \mathbb{Z}$? (Caution: $\mathbb{Z}[\sqrt{-3}]$ is *not* the ring of integers in $\mathbb{Q}(\sqrt{-3})$.)

Exercise 6
Verify the computation in Milne - Example 3.5.2 by hand and in a computer algebra system, then answer the question Milne poses.

Exercise 7

(1) Suppose $f(x) \in \mathbb{Z}[x]$ is Eisenstein at p. Show that p is totally ramified in $K = \mathbb{Q}[x]/f(x)$, i.e. that there is a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ such that $(p) = \mathfrak{p}^{[K:\mathbb{Q}]}$. What are generators for $\mathfrak{p}$?
(2) Generalize this to replace $\mathbb{Z}$ with an arbitrary Dedekind domain (see Prop. 3.53 in Milne if you get stuck).

Exercise 8
The structure theory of finitely generated modules over a PID admits a nice generalization to finitely generated modules over a Dedekind domain. In particular, if A is a Dedekind domain and M is a torsion-free finitely generated A-module such that $M \otimes \mathrm{Frac}(A)$ is an n-dimensional vector space over $\mathrm{Frac}(A)$, then

$$M \cong A^{n-1} \bigoplus \mathfrak{a}$$

for a nonzero ideal $\mathfrak{a}$ of A, uniquely determined up to its equivalence class in the class group $\mathrm{Cl}(A)$. There is also a nice version of the invariant factors theorem.

(1) Read the 1-page section "Modules over Dedekind domains" in Chaper 3 of Milne, then try to prove as much of this as you can on your own before following the references.
(2) When $A = \mathbb{C}[x, y]/f(x, y)$ is the ring of functions on a non-singular plane curve, what is the geometric meaning of the classification?

Exercise 9
Let A be a Dedekind domain with fraction field K, and let L be a finite extension of K. Let B be the integral closure of A in L. We define the *relative* discriminant of B/A to be the *ideal* of A generated by

$$\mathrm{disc}(e_1, \dots, e_n) := \det(\mathrm{Tr}(e_i e_j))$$

where we vary over all bases $e_1, \dots, e_n$ for L as a K-vector space such that $e_i \in B \; \forall\, i$.

(1) Show that when $A = \mathbb{Z}$ and $K/\mathbb{Q}$, this recovers our previous definition of the discriminant.
(2) Why does the previous definition not work in general? When does it work and, in that case, where does the resulting quantity live?
(3) Using (2), explain how to compute the prime factorization of the relative discriminant.
(4) Show that a prime ideal $\mathfrak{p}$ of A ramifies in L if and only if $\mathfrak{p}$ divides the relative discriminant.