Bordeaux 1 University
Mathematics

MHT 933 - master 2
2009-2010

Exercises for Chapter 5

Exercise 1 – [Dedekind's criterion]

We want first to give a proof of the Dedekind's criterion seen in course. Recall the result.

Theorem 1. *Let p be a prime number. Let $K = \mathbb{Q}(\theta)$, and $T \in \mathbb{Z}[X]$ be the monic, minimal polynomial of θ. Suppose that*

$$T \equiv \prod_i P_i^{e_i} \pmod{p\mathbb{Z}[X]},$$

where the P_i are monic, irreducible and distinct modulo p. Let

$$g = \prod P_i, \quad h = \prod P_i^{e_i - 1}, \quad f = (T - gh)/p \in \mathbb{Z}[X].$$

1. *Then $\mathbb{Z}[\theta]$ is p-maximal if and only if $\gcd(\overline{f}, \overline{g}, \overline{h}) = 1$ in $\mathbb{F}_p[X]$.*
2. *Moreover let $\mathcal{O}' = (I_p : I_p)$ where I_p is the p-radical of $\mathbb{Z}[\theta]$. If U is a monic lift of $\overline{T}/\gcd(\overline{f}, \overline{g}, \overline{h})$ to $\mathbb{Z}[X]$, we have*

$$\mathcal{O}' = \mathbb{Z}[\theta] + \frac{1}{p} U(\theta)\mathbb{Z}[\theta]$$

and if $m = \deg \gcd(\overline{f}, \overline{g}, \overline{h})$ then $[\mathcal{O}' : \mathbb{Z}[\theta]] = p^m$ hence $\mathrm{disc}\mathcal{O}' = \mathrm{disc}T/p^{2m}$.

1. Prove that

$$p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta] \subset I_p.$$

2. Using the fact that $\overline{T}$ is the minimal polynomial of θ over $\mathbb{F}_p$, show that in fact

$$I_p = p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta].$$

3. Let $x \in \mathcal{O}'$. Show that there exists $A \in \mathbb{Z}[X]$ such that $x = A(\theta)/p$.

4. Show that $xp \in I_p$ if and only if $\overline{g} \mid \overline{A}$ and that, if k is a monic lift of $\overline{g}/(\overline{f}, \overline{g})$ to $\mathbb{Z}[X]$, then $xg(\theta) \in I_p$ if and only if $\overline{hk} \mid \overline{A}$.

5. Deduce from this part 2 of the theorem and then part 1.

6. With the same notation, let R_i be the remainder of the Euclidean division of T by P_i. Set $d_i = 1$ if $e_i \geq 2$ and $R_i \in p^2\mathbb{Z}[X]$, $d_i = 0$ otherwise. Show that in the above theorem we can take $U = \prod P_i^{e_i - d_i}$ and that $\mathbb{Z}[\theta]$ is p-maximal if and only if $R_i \notin p^2\mathbb{Z}[X]$ for every i such that $e_i \geq 2$.

Exercise 2 – [PURE CUBIC FIELDS]

Let $K = \mathbb{Q}(m^{1/3})$ be a pure cubic field, where m is a cubefree integer not equal to ± 1. Write $m = ab^2$ with a, b squarefree and coprime. Let θ be the cube root of m belonging to K.

1. Show that if $a^2 \not\equiv b^2 \bmod 9$ then $\mathbb{Z}_K$ admits

$$\left(1, \theta, \frac{\theta^2}{b}\right)$$

as a $\mathbb{Z}$-basis.

2. Show that if $a^2 \equiv b^2 \bmod 9$ then $\mathbb{Z}_K$ admits

$$\left(1, \theta, \frac{\theta^2 + ab^2\theta + b^2}{3b}\right)$$

as a $\mathbb{Z}$-basis.

3. Let p a prime which does not divide b in the first case and does not divide $3b$ in the second case. Find the decomposition of $X^3 - m \bmod p$ and deduce from this the decomposition of $p\mathbb{Z}_K$ as product of prime ideals.

Exercise 3 – [QUARTIC FIELDS]

Let m, n be distinct squarefree integers different from 1 and let K be the quartic field $\mathbb{Q}(\sqrt{m}, \sqrt{n})$.

1. Compute a $\mathbb{Z}$-basis of $\mathbb{Z}_K$.

2. Find the explicit decomposition of prime numbers in K.

Exercise 4 – [AROUND KUMMER]

We want now to prove the weak version of Kummer's theorem (which is true even if $\mathbb{Z}[\theta]$ is not necessarily p-maximal). Recall the statement.

Theorem 2. *Let $K = \mathbb{Q}(\theta)$, $T \in \mathbb{Z}[X]$ the monic minimal polynomial of θ. If*

$$T \equiv \prod_i P_i^{e_i} \pmod{p\mathbb{Z}[X]},$$

where the P_i are monic, irreducible and distinct modulo p. Then

$$p\mathbb{Z}_K = \prod_i \mathfrak{a}_i,$$

where the $\mathfrak{a}_i = p\mathbb{Z}_K + P_i^{e_i}(\theta)\mathbb{Z}_K$ are pairwise coprime ideals. Furthermore, if f_i is the degree of P_i we have $N(\mathfrak{a}_i) = p^{e_i f_i}$ and all prime ideals dividing $\mathfrak{a}_i$ are of residual degree divisible by f_i.

1. Prove that

$$\mathfrak{a}_i^{-1} = \Big(1, \prod_{j \neq i} T_j^{e_j}(\theta)/p\Big).$$

2. Following the proof of Kummer's theorem, establish the above result.

Exercise 5 – [UNITS AND CLASS GROUP]

Compute the class group, the regulator and a system of fundamental units for the number fields defined by the polynomials

1. $P = X^2 - 10$,
2. $Q = X^3 + X + 1$,
3. $R = X^4 - 3X - 5$.