June 4th, 2014

Algebraic Number Theory

Prof. H. Esnault

Exercise sheet 8[1]

Exercise 1. Let k be an algebraically closed field, $K := k(t)$ the degree 1 purely transcendental extension of k. Let

$$f(t, X) \in k[t, X] = k[t][X] \subseteq K[X]$$

be an irreducible monic polynomial over K with coefficients in $k[t]$. Then $L := K[X]/(f(t, X))$ is a finite field extension of K.

(1) Show that given any solution $(a, b) \in k\times k$ for the equation $f(t, X) = 0$ we obtain a maximal ideal $(t - a, X - b)$ of $k[t, X]$ containing the ideal $(f(t, X)) \subseteq k[t, X]$, hence a maximal ideal of $k[t, X]/(f(t, X))$. Moreover, if $(a', b') \in k \times k$ is a different solution of $f(t, X) = 0$ then we get a different maximal ideal. (In fact the converse is also true, i.e. any maximal ideal of the ring $k[t, X]/(f(t, X))$ is of the form $(t - a, X - b)$ for some solution $(a, b) \in k \times k$ of $f(t, X) = 0$. This comes from Hilbertnullstellenstatz. Thus we have a one to one correspondence between the solutions of $f(t, X) = 0$ and the maximal ideals of $k[t, X]/(f(t, X))$.)

If the extension $K \subseteq L$ is also separable, then we can take the integral closure of $k[t]$ in L, and it is still a Dedekind domain. Let us denote it by B.

(2) Show that there is a natural injection $k[t, X]/(f(t, X)) \hookrightarrow B$.

There is a so called "Jacobian criterion" to determine when the natural injection is an isomorphism. The criterion says: the natural injection is an isomorphism if and only if the following $(1 \times 2)-$matrix with entries in k

$$(\frac{\partial f}{\partial t}(a, b), \frac{\partial f}{\partial X}(a, b))$$

is of rank 1 for any solution $(a, b) \in k \times k$ of $f(t, X) = 0$. The proof of this criterion uses techniques from algebraic geometry and is not quite easy, so we will only assume the result and do applications.

(3) Use Jacobian criterion to show that the following rings are Dedekind.

(a) $\mathbb{C}[t, X]/(X^2 - t^3 - 1)$;

(b) $\mathbb{C}[t, X]/(X^2 - t^3 - at - b)$ with $a, b \in \mathbb{C}$ and $4a^3 + 27b^2 \neq 0$;

[1] If you want your solutions to be corrected, please hand them in just before the lecture on June 11. If you have any questions concerning these exercises you can contact Lei Zhang via l.zhang@fu-berlin.de or come to Arnimallee 3 112A.

(c) $\bar{\mathbb{F}}_p[t,X]/(X^p - X - t)$, where $\mathbb{F}_p$ is the finite field of p elements, and $\bar{\mathbb{F}}_p$ is its algebraic closure.

Remark 1. You might have already observed that there is a strong analogy between the ring of integer numbers $\mathbb{Z}$ and the complex polynoimal ring in one variable $\mathbb{C}[t]$. In fact, the maximal ideals of $\mathbb{Z}$ are analogous to the points on the complex plan $\mathbb{C}$, both of which correspond to the maximal ideals of the respective rings. From the exercise you should see more analogy from the behavior of the finite extensions of the fields $\mathbb{Q}$ and $\mathbb{C}(t)$. The maximal ideals of the ring of integers of a number field is analogues to the set of solutions of $f(t,X) = 0$ for a finite extension of the form $K \subseteq K(X)/(f(t,X))$ where $K = \mathbb{C}(t)$. That's partially the reason why we did some generalities on Dedekind domains in the course instead of only treating the ring of integers of number fields.

Exercise 2. (1) Determine the ramification behavior of the ideal $(t - c) \subseteq \mathbb{C}[t]$, where $c \in \mathbb{C}$, under the extension

$$\mathbb{C}[t] \subseteq \mathbb{C}[t,X]/(X^2 - t^3 - at - b)$$

with a, b and $4a^3 + 27b^2 \neq 0$ and conclude that for any such a, b there are always three maximal ideals of $\mathbb{C}[t]$ which ramify under such an extension.

(2) Determine the ramification behavior of the ideal $(t - c) \subseteq \bar{\mathbb{F}}_p[t]$ where $c \in \bar{\mathbb{F}}_p$, under the extension

$$\bar{\mathbb{F}}_p[t] \subseteq \bar{\mathbb{F}}_p[t,X]/(X^p - X - t),$$

and conclude that there is not a single maximal ideal of $\bar{\mathbb{F}}_p[t]$ which ramifies under such an extension.

Remark 2. It is always true that if k is an algebraically closed field of characteristic 0, then for any *non-trivial* finite extension of $k(t)$ there is always (at least) one ramified maximal ideal in $k[t]$. This is an analogy of Theorem 4.9. in `http://jmilne.org/math/CourseNotes/ANT.pdf` which is proved in the lecture. But the technique of the proof of this analog is beyond what we could afford in this course.

Exercise 3. (1) Use *Minkowski Bound* in Theorem 4.3. to prove that the ring of Gauss integers $\mathbb{Z}[i]$ is a principal ideal domain. (Hint: Use Ex. 7.1 to calculate the discriminant for the extension $\mathbb{Q} \subseteq \mathbb{Q}[i]$.)

(2) For an odd prime number $p \in \mathbb{Z}$, show that the following statements are equivalent

(a) $p \equiv 1 \bmod 4$;

   (b) (p) splits in $\mathbb{Z}[i]$;
   (c) there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.

(3) Determine the ramification behavior of (2) in $\mathbb{Z}[i]$.

Exercise 4. Let $K := \mathbb{Q}(\sqrt{-5})$. Find a set of representatives of the class group $\mathrm{Cl}(O_K)$ and determine the group structure of it.