April 23th, 2014

Algebraic Number Theory

Prof. H. Esnault

Exercise sheet 2[1]

Exercise 1. Let A be an integral domain, K be its fraction field. Recall that a *fractional ideal* of A is a non-zero A-submodule $\mathfrak{a} \subseteq K$ such that $d\mathfrak{a} \subseteq A$ for some non-zero element $d \in A$. If $\mathfrak{a}$ is generated by one element as an A-module then it is called *principal*.

(1) Let $S \subseteq A$ be a multiplicatively closed subset and $\mathfrak{a}$ be a fractional ideal of A. Show that $S^{-1}\mathfrak{a}$ is a fractional ideal of $S^{-1}A$.

(2) Let $S \subseteq A$ be as in (1), $\mathfrak{a}$ and $\mathfrak{b}$ be two fractional ideals of A. Show that

$$S^{-1}(\mathfrak{a}\mathfrak{b}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b}).$$

(3) Let $\mathfrak{a}$ be a fractional ideal of A. Set

$$\mathfrak{a}' = \{a \in K | a\mathfrak{a} \subseteq A\}.$$

Prove that $\mathfrak{a}'$ is a fractional ideal of A. Let $S \subseteq A$ be as in (1). Show that

$$\begin{aligned} S^{-1}\mathfrak{a}' &= \{a \in K | a\mathfrak{a} \subseteq S^{-1}A\} \\ &= \{a \in K | aS^{-1}\mathfrak{a} \subseteq S^{-1}A\} = (S^{-1}\mathfrak{a})'. \end{aligned}$$

if A is Noetherian.

(4) Let A be a Dedekind domain. Show that $\mathfrak{a}\mathfrak{a}' = A$. (Hint: otherwise $\mathfrak{a}\mathfrak{a}'$ would be contained in a maxiaml ideal $\mathfrak{p} \subset A$. Take $S := A \setminus \mathfrak{p}$ and localize, then $(S^{-1}\mathfrak{a})(S^{-1}\mathfrak{a}')$ is contained in the maxiaml ideal of $S^{-1}A = A_{\mathfrak{p}}$. But $A_{\mathfrak{p}}$ is a DVR and in a DVR we have $(S^{-1}\mathfrak{a})(S^{-1}\mathfrak{a})' = A_{\mathfrak{p}}$. A contradiction!)

Exercise 2. Let A be a Dedekind domain. Recall that the set of fractional ideals of A forms an abelian group and this group is denoted by $\mathrm{Id}(A)$. The set of principal fractional ideals of A is a subgroup of $\mathrm{Id}(A)$ and is denoted by $\mathrm{P}(A)$. The quotient group $\mathrm{Cl}(A) := \mathrm{Id}(A)/\mathrm{P}(A)$ is called the *ideal class group*. Let A^* (resp. K^*) be the group of invertible elements of A (resp. K). Show that

(1) the following sequence of abelian groups (with canonical maps)

$$1 \to A^* \to K^* \to \mathrm{Id}(A) \to \mathrm{Cl}(A) \to 1$$

[1] If you want your solutions to be corrected, please hand them in just before the lecture on April 30th. 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.

is exact; (Recall that a squence of abelian groups $G_1 \xrightarrow{\phi} G_2 \xrightarrow{\varphi} G_3$ is called *exact* if the image of ϕ is equal to the kernel of φ.)

(2) the following conditions are equivalent:
   (a) $\mathrm{Cl}(A)$ is the trivial group;
   (b) $\mathrm{Id}(A) = \mathrm{P}(A)$;
   (c) A is a PID;
   (d) A is a UFD.

Exercise 3. Let m be a square free integer, i.e. $m \in \mathbb{Z}$ and there is no prime number $p \in \mathbb{N}^+$ such that $p^2|m$. Let $A = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m}|a, b \in \mathbb{Z}\}$.

(1) Prove that there is a surjective map of $\mathbb{Z}$-algebras
$$\phi : \mathbb{Z}[X]/(X^2 - m) \to \mathbb{Z}[\sqrt{m}]$$
sending $X \mapsto \sqrt{m}$ and deduce from this that A is a Noetherian ring. (Recall that if R is a Noetherian ring then $R[X]$ is also Noetherian and so are the quotients of R.) Show that ϕ is an isomorphism when $m \neq 1$.

(2) Let P be a non-zero prime ideal of A. Show that $\mathfrak{p} := P \cap \mathbb{Z}$ is a non-zero prime ideal of $\mathbb{Z}$.

(3) Deduce from (2) that P is a maximal ideal of A. (Hint: A/P a finite $\mathbb{Z}/\mathfrak{p}$-algebra. But $\mathbb{Z}/\mathfrak{p}$ is a field. So A/P is Artinian. Since A/P is also an integral domain, it must be a field.)

(4) Show that A is Dedekind if and only if A is integrally closed.

Exercise 4. Let $A = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}|a, b \in \mathbb{Z}\}$. Let $N(\alpha) := a^2 + 5b^2$ for $\alpha = a + b\sqrt{-5} \in A$.

(1) Show that A is a Dedekind domain. (Hint: one has to prove that A in integrally closed. Let $\alpha = r + s\sqrt{-5}$ ($r, s \in \mathbb{Q}$) be an element in $\mathbb{Q}(\sqrt{-5})$ which is integral over $\mathbb{Z}[\sqrt{-5}]$. Show that $f(X) = X^2 - 2rX + r^2 + 5s^2$ is an element in $\mathbb{Q}[X]$ of smallest degree such that $f(\alpha) = 0$. Since α is integral over $\mathbb{Z}[\sqrt{-5}]$, it is also integral over $\mathbb{Z}$. (You don't have to prove this. If you don't know then just accept it.) Show that $f(X)$ has $\mathbb{Z}$-coefficients, i.e. $2r, r^2 + 5s^2 \in \mathbb{Z}$. Then deduce that $r \in \mathbb{Z}, s \in \mathbb{Z}$.)

(2) Show that $\alpha \in A$ is an invertible element (i.e. $\alpha \in A^*$) if and only if $N(\alpha) = 1$. What is the group A^*?

(3) Show that if $N(\alpha) = 9$ then α is irreducible in A. Thus $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ are irreducible.

(4) Is $(9) = (3) \cdot (3)$ a prime ideal decomposition in A? Justify your conclusion!