Addendum to the May 8, 2013 course

1. Dedekind property and finite field extensions

Proposition 1.1. *Let A be a Dedekind domain, $K := \mathrm{Frac}(A)$, $L \supset K$ be a finite field extension. Then $B :=$ integral closure of A in L is Dedekind.*

Proof. (Compare the proof here with
`http://www.math.uchicago.edu/~may/MISC/Dedekind.pdf`, Theorem 2.4)

From the course we know the proposition when $L \supset K$ is separable, and we know the only property where we used that $L \supset K$ is separable is to show: B is noetherian, which was implied by the fact that B is finitely generated as a A-module. We show the proposition in general. We know $L = \mathrm{Frac}(B)$. A finite field extension $L \supset K$ decomposes as $L \supset E \supset K$, where $E \supset K$ is separable and $L \supset E$ is purely inseparable. So we replace A by its integral closure in E, K by E and we may assume that $L \supset K$ is purely inseparable. Take $x \in L$. It fulfills an equation of the shape $x^{p^e} - a = 0$ for some $a \in K^\times$. On the other hand, $L \supset K$ is generated as a K-vector space by $y_1, \ldots, y_d$, with minimal equations $y_i^{p^{f_i}} - b_i = 0$ for some $b_i \in K^\times$. Thus $x = \sum_{i=1}^d \lambda_i y_i$ for some $\lambda_i \in K$, and, for $f = \max\{f_i\}$, $x^{p^f} = \sum_{i=1}^d (\lambda_i y_i)^{p^f} = \sum_{i=1}^d \lambda_i^{p^f} b_i^{p^{f-f_i}} \in K$. Set $q = p^f$. Then $x^q \in K$ for all $x \in L$ and $B = \{x \in L, x^q \in B \cap K = A\}$. Define $E = \{z \in \bar{K}, z^q \in K\}$, where $\bar{K}$ is an algebraic closure of K. Then $K \subset L \subset E$ is a composite field extension. Let R be the algebraic closure of A in E. Then $R = \{x \in E, x^q \in R \cap K = A\}$. Then the map $F : E \to K,\ x \mapsto x^q$ is a homomorphism of fields, thus is injective, and is surjective by construction, thus is an isomorphism. The image of R is A. Thus the ring R, which is isomorphic to A, is a Dedekind ring. So given a non-zero ideal $I \subset B$, the ideal $IR \subset R$ is invertible. Thus there are elements $a_i \in I,\ b_i \in (IR)^{-1},\ i = 1, \ldots, d$, such that $1 = \sum_{i=1}^d a_i b_i$. Thus $1 = \sum_{i=1}^d a_i \cdot a_i^{q-1} b_i^q$. By definition, $b_i^q \in K$, thus $c_i = a_i^{q-1} b_i^q \in L$. On the other hand, $c_i I = (a_i b_i)^{q-1} b_i I \in R$. Thus $c_i \in I^{-1}$. Thus for all $a \in I$ we have $a = \sum_{i=1}^d a_i a c_i$ and I is the ideal spanned by $a_i,\ i = 1, \ldots, d$. Thus B is noetherian.

□

2. Degree

Proposition 2.1. *Let A be a Dedekind domain, $K := \mathrm{Frac}(A)$, $L \supset K$ be a finite field extension, B be the integral closure of A in L, $\mathfrak{p}$ be in $\mathrm{Spec}\,(A)$. Then the dimension of $B/\mathfrak{p}B$ as a module over the field $A/\mathfrak{p}$ is finite equal to $[L : K]$.*

Proof. We have seen that for $S = A \backslash \mathfrak{p}$, $B/\mathfrak{p}B \xrightarrow{\cong} S^{-1}B/\mathfrak{p}S^{-1}B$ and $S^{-1}A/\mathfrak{p}S^{-1}A = (: A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})$ so we may assume that A is a DVR. As B is a subring of a field, it is torsion free, and we know it is finitely generated as a A-module. Thus, by the structure theorem of finitely generated modules over DVR, B is free over

A, of degree equal to the degree of $B \otimes_A K$ over $A \otimes_A K = K$. On the other hand one has the surjective K-linear map $B \otimes_A K \to K \cdot B = L$ defined by $b \otimes \lambda \mapsto \lambda b$. I claim it is injective as well: let b_i be a basis of B over A. An element $\sum_i b_i \otimes \frac{\lambda_i}{\mu}, \lambda_i \in A, \mu \in A \setminus \{0\}$ maps to 0 if $\sum_i b_i \frac{\lambda_i}{\mu} = 0$, which, in the field L, it equivalent to $\sum_i b_i \lambda_i = 0$, which, by freeness, implies $\lambda_i = 0$. Thus $B \otimes_A K = L$. Since B is a free A-module of rank $[L : K]$, the module $B/\mathfrak{p}B = B \otimes_A A/\mathfrak{p}$ is also free of rank $[L : K]$ over $A/\mathfrak{p}$.

□

On the way, we showed

Proposition 2.2. *If in the above proposition A is a DVR, then B is a free A-module, and $B \otimes_A K = L$.*

3. $\bar{f}$ IRREDUCIBLE

Proposition 3.1. *Let A be a DVR with maximal ideal $\mathfrak{m}$, residue field k. Let $f = X^n + a_1 X^{n-1} + \ldots + a_n \in A[X]$ of degree ≥ 1 such that its reduction $\bar{f} \in k[X]$ mod $\mathfrak{m}$ is irreducible. Set $B = A[X]/(f)$. Then B is a DVR.*

Proof. We had seen that B has only one maximal ideal $\mathfrak{m}_B = \mathfrak{m}B$, thus is spanned by a uniformizer π of $\mathfrak{m}$. So B is generated as a A-algebra by the uniformizer of A, thus is noetherian as well. All we were left with was to show that B is a domain. If $0 \neq x \in B$ is a 0-divisor, it has to lie in $\mathfrak{m}_B$ thus is of the shape $\pi^n \cdot u,\ n \in \mathbb{N} \setminus \{0\}$, where $u \in B^\times$. Let $y \in B$ with $xy = 0$. y can't be a unit, thus $y = \pi^M v, M \in \mathbb{N} \setminus \{0\}$ and $v \in B^\times$. Thus $A \ni \pi^{N+M} = 0$, which is a contradiction, as A is a domain. □

Corollary 3.2. *With the above assumption, let $K = \mathrm{Frac}(A)$. Then $f \in K[X]$ is irreducible, and B is the integral closure of A in the field $L = K[X]/(f)$.*

Proof. As B is a domain, $B \otimes_A K$ is a domain: any element is of the shape $b \otimes \frac{1}{\pi^N}$ for some $N \in \mathbb{N} \setminus \{0\}$. So $L := K[X]/(f) = B \otimes_A K$ is a domain, so is a field, so $f \in K[X]$ is irreducible, and L is the field of fractions of B. Let B' be the integral closure of A in L. Since B is finite over A we have $B \subset B'$. On the other hand any element in B' is in particular integral over B, which is integrally closed (being a DVR), hence $B' \subset B$. Thus $B' = B$.

□

4. f EISENSTEIN

Proposition 4.1. *Let A be a DVR with maximal ideal $\mathfrak{m}$, residue field k, and field of fractions K. Let $f \in A[X]$ be a Eisenstein polynomial. Then $B = A[X]/(f)$ is a domain, $f \in K[X]$ is ireducible and B is the integral closure of A in $L = K[X]/(f)$.*

Proof. We had seen B is local with maximal ideal $\mathfrak{m}_B = (x)$, where x is the residue class of X in B. So the uniformizer π of A can be written as $\pi = x^N u, u \in B^\times$, so again a 0-divisor is of the shape $y = \pi^M v, v \in B^\times, M \in \mathbb{N} \setminus \{0\}$, thus π^M is a 0-divisor, thus again it produces an equation of the shape $\pi^{N+M} = 0$ in A for some $N \in \mathbb{N}$, which is impossible as A is a domain. Now as in Corollary 3.2, $B \otimes_A K = K[X]/(f)$ is a domain, thus is a field, and is $K \cdot B = L$, thus as $B \subset L$ is the integral closure of A in L and L is the field of fractions of B. $\square$

Hélène Esnault