Andrea Gadotti 12/01/2015

Exercise 63. Let L/K be an algebraic function field, $x \in L$ transcendent over K, $[L : K(x)] = n < \infty$ and $y \in L$ with $L = K(x, y)$. Then:

1. There exists an irreducible polynomial $f \in K[X, Y] \setminus K$, uniquely determined up to factors from $K^\times$, such that $f(x, y) = 0$.

2. Let $\overline{K}$ be an algebraic closure of K, $C = \mathcal{V}_{\overline{K}} \subseteq \overline{K}^2$ the associated curve, and $x_C, y_C \in K(C)$ the coordinate function of C. Then there is a unique K-isomorphism $\Phi : L \to K(C)$ with $\Phi(x) = x_C$ and $\Phi(y) = y_C$.

Proof.

1. Since $L = K(x, y)$, we have $[K(x, y) : K(x)] = n$, i.e. the minimal polynomial of y over $K(x)$ has degree n. This means that there exists $g \in K(x)[Y]$ irreducible such that

$$g(y) = a_n y^n + \ldots + a_0 = 0,$$

   where $a_0, ..., a_n \in K(x)$. Let m be the least common multiple of the denominators of $a_0, ..., a_n$. By multiplying g by m, we get $f(X, Y) \in K[X, Y] \setminus K$ such that $f(x, y) = 0$. Thus $(f) \subseteq \mathcal{J}(V)$. We want to show that the equality holds. Suppose to the contrary that there exists $f' \in K[X, Y] \setminus K$ such that $f'(x, y) = 0$. Then $f'(x, Y) \in K(x)[Y] \setminus K$ is such that $f'(x, y) = 0$, i.e. y is a root of $f'(x, Y)$, and thus $f'|g$. But since g is irreducible, this means $f' = ag$ for some $a \in K(x)$. Since $f' \in K[X, Y] \setminus K$, by definition of m we must have $m|a$, i.e. $f|f'$, which finally means $f' \in (f)$.

   So $\mathcal{J}(V) = (f)$. Since V is a singleton, it is trivially irreducible (but we should show that it is a variety!!!). Thus, by Exercise 51, $\mathcal{J}(V)$ is a prime ideal. Therefore f is irreducible, and of course it is uniquely determined up to a constant of $K^\times$.

2. First, observe that if such a K-isomorphism exists, then it is trivially unique, since $L = K(x, y)$ and thus every K-homomorphism is uniquely determined by its behaviour on x and y (should be explained better).
   Now consider

$$\begin{aligned} \varphi : K[X, Y] &\to K[x, y] \\ X &\mapsto x \\ Y &\mapsto y. \end{aligned}$$

φ is obviously a well defined K-homomorphism. It is also trivially surjective. Now observe that

$$h \in \ker\varphi \iff h(x,y) = 0 \iff h \in \mathcal{J}(\{(x,y)\}) = \mathcal{J}(V),$$

i.e. $\ker\varphi = \mathcal{J}(V)$. So $K[x,y] \simeq K[X,Y]/\mathcal{J}(V)$. But

$$\mathcal{J}(C) = \mathcal{J}(\mathcal{V}_{\overline{K}}(f)) = \sqrt{(f)} = (f) = \mathcal{J}(V)$$

and thus $K[x,y] \simeq K[X,Y]/\mathcal{J}(C) =: K[C]$, whereby easily follows $K(x,y) \simeq K(C)$.
Finally, it's easy to show that the isomorphism between $K(x,y)$ and $K(C)$ inducted by φ is precisely Φ.

□

Exercise 64.

1. We already know that $(R[H],+)$ is an abelian group. The associativity of $\cdot$ follows easily by the one of R's multiplication. It is also clear that $\cdot$ is commutative. Also the distributivity is immediate. We only have to check that X^0 is the unit element:

$$(f\cdot X^h)(z) = \sum_{\substack{(x,y)\in H\times H\\ x+y=z}} f(x)X^0(y) = \sum_{\substack{(x,0)\in H\times\{0\}\\ x=z}} f(x) = f(z).$$

   As for $\theta : R \to R[H]$, it's easy to show that it's a ring homomorphism. It is also injective since

$$\theta(a) \equiv 0 \Rightarrow \theta(a)(0_H) = 0_R \Rightarrow a = 0_R.$$

   As for the map $h \mapsto X^h$, observe that

$$(X^h\cdot X^k)(z) = \sum_{\substack{(x,y)\in H\times H\\ x+y=z}} X^h(x)X^k(y) = \begin{cases} 1_R, & \text{if } z = h+k,\\ 0_R, & \text{otherwise,}\end{cases}$$

   i.e. $X^h \cdot X^k = X^{h+k}$. So $h \mapsto X^h$ is a semigroup homomorphism. The injectivity is trivial.

2. We have

$$f = \sum_{h\in\operatorname{supp}(f)} f(h)X^h,$$

   thus, defining $a_h := f(h)$ for all $h \in H$ and recalling that $|\operatorname{supp}(f)| < \aleph_0$, follows that every $f \in R[H]$ has a representation like the one in the statement. It is trivially unique.

3. The statement about the sum is trivial. The statement about the product is trivial by definition of X^h and $f \cdot g$, since $a_x = f(x)$ and $g(y) = b_y$.

Exercise 65. Let $f \in R[G]$ be

$$f = \prod_{i=1}^{l} (X^{g_i} - a_i),$$

where by a_i we actually mean $\theta(a_i)$.
We have already proved that $(R[H], +, \cdot)$ is a commutative ring (with unit element X^0), and that $X^h \cdot X^k = X^{h+k}$. So we can write f as

$$f = X^{\sum_{g\in S} g} + \ldots + \prod_{i=1}^{l} a_i = X^{\sum_{g\in S} g} + \ldots + X^0 \cdot \prod_{i=1}^{l} a_i.$$

Let's evaluate the last expression in 0_H. By the last line of the first point of Exercise 64, we have

$$\left(X^0 \cdot \prod_{i=1}^{l} a_i \right) (0_H) = \prod_{i=1}^{l} a_i.$$

Furthermore, all the other terms are 0_R when evaluated in 0_H, because in all the other terms there is a term of the form $X^{\sum_{g\in I} g}$ for some $I \subseteq S$, which is necessarily $\neq X^0$ because S is zero-sum free, and so they all are 0_R when evaluated in 0_H.
Therefore $f(0) = \prod_{i=1}^{l} a_i \neq 0$ since R is a domain, and thus $f \neq 0$.

Exercise 66.

1. By the same argument of Exercise 7 it follows that 2 is irreducible (since, if $d < -2$, then $a^2 - db^2 \neq 2$ for all $a, b \in \mathbb{Z}$).
   In order to show that 2 is not prime, we consider two different cases:
   - If d is even: then $2 \mid -d = -\sqrt{d}\sqrt{d}$, but 2 does not divide any of the two factors.
   - If d is odd: then $2 \mid 1 - d = (1 + \sqrt{d})(1 - \sqrt{d})$, but 2 does not divide any of the two factors.

2. "$\Rightarrow$": If $x \in K_d^\circ$, then $x = \frac{y}{z}$ with $y, z \in R_d$. Let q, r be the quotient and the rest of y divided by z. We have

$$|N_{K_d/\mathbb{Q}}(x - q)| = \left| N_{K_d/\mathbb{Q}} \left(\frac{y}{z} - q \right) \right| = \frac{|N_{K_d/\mathbb{Q}}(y - zq)|}{|N_{K_d/\mathbb{Q}}(z)|} = \frac{|N_{K_d/\mathbb{Q}}(r)|}{|N_{K_d/\mathbb{Q}}(z)|} < 1.$$

"$\Leftarrow$": Let $y, z \in R_d$. Then $x := \frac{y}{z} \in K_d$. Let $q \in R_d$ be such that $|N_{K_d/\mathbb{Q}}(x - q)| < 1$. Then we obtain (same computations of above):

$$\frac{|N_{K_d/\mathbb{Q}}(y - zq)|}{|N_{K_d/\mathbb{Q}}(z)|} < 1.$$

By defining $r := y - zq$ we have $y = zq + r$ with $|N_{K_d/\mathbb{Q}}(r)| < |N_{K_d/\mathbb{Q}}(z)|$, as wanted.

3. Consider the basis $\mathbf{u} = \big((1,0),(0,\sqrt{d})\big)$ for K_d over $\mathbb{Q}$. Let $\alpha = a + b\sqrt{d} \in K_d$, i.e. $a, b \in \mathbb{Q}$. Then $\mu_\alpha : K_d \to K_d$ given by $\mu_\alpha(\beta) = \alpha\beta$ is such that

$$\mathcal{M}_{\mathbf{u},\mathbf{u}}(\mu_\alpha) = \begin{pmatrix} a & bd \\ b & a \end{pmatrix},$$

and so $N_{K_d/\mathbb{Q}}(\alpha) = \det(\mu_\alpha) = a^2 - db^2$.
Now, in order to prove that R_d is an Euclidean ring it is sufficient to show that for any $\alpha \in K_d$ there exists $q = q_1 + q_2\sqrt{d} \in R_d$ such that

$$1 > |N_{K_d/\mathbb{Q}}(\alpha - q)| = |(a - q_1)^2 - d(b - q_2)^2|.$$

Let's define q_1 and q_2 as follows:

$$q_1 := \begin{cases} \lfloor a \rfloor & \text{if } 0 \le a - \lfloor a \rfloor < \frac{1}{2}, \\ \lceil a \rceil & \text{if } -\frac{1}{2} < a - \lceil a \rceil \le 0, \end{cases} \quad \text{and} \quad q_2 := \begin{cases} \lfloor b \rfloor & \text{if } 0 \le b - \lfloor b \rfloor < \frac{1}{2}, \\ \lceil b \rceil & \text{if } -\frac{1}{2} < b - \lceil b \rceil \le 0. \end{cases}$$

Of course q_1 and q_2 are well-defined and are such that $a - q_1 <$ and $b - q_2 < 1/2$.
Before the conclusion, we introduce the following notation:
Notation: Given $r_1, r_2, s_1, s_2, t \in \mathbb{Q}$, we define $[r_1, r_2] + t[s_1, s_2] := \{h = r + ts \mid r \in [r_1, r_2], s \in [s_1, s_2]\}$.
So q_1 and q_2 are such that $(a - q_1)^2 \in [0, 1/4]$ and $(b - q_2)^2 \in [0, 1/4]$. Now:

- $d = -1$. We have $|(a - q_1)^2 + (b - q_2)^2| < 1$, since $[0, 1/4] + [0, 1/4] = [0, 1/2] \subseteq (-1, 1)$.
- $d = -2$. We have $|(a - q_1)^2 + 2(b - q_2)^2| < 1$, since $[0, 1/4] + 2[0, 1/4] = [0, 3/4] \subseteq (-1, 1)$.
- $d = 2$. We have $|(a - q_1)^2 - 2(b - q_2)^2| < 1$, since $[0, 1/4] - 2[0, 1/4] = [-1/2, 1/4] \subseteq (-1, 1)$.
- $d = 3$. We have $|(a - q_1)^2 - 3(b - q_2)^2| < 1$, since $[0, 1/4] - 3[0, 1/4] = [-3/4, 1/4] \subseteq (-1, 1)$.

Exercise 68

1. We must show that φ is a K-vector space iff $\varphi_{|K} = \mathrm{id}_K$.
"$\Rightarrow$" Let $\lambda \in K$. Then $\varphi(\lambda) = \varphi(\lambda 1_L) = \lambda\varphi(1_L) = \lambda 1_{L'} = \lambda$.
"$\Leftarrow$" Let $\lambda, \mu \in K$ and $u, v \in L$. Then $\varphi(\lambda u + \mu v) = \varphi(\lambda)\varphi(u) + \varphi(\mu)\varphi(v) = \lambda\varphi(u) + \mu\varphi(v)$.

2. By first point, the element of $\mathrm{Gal}(L/K)$ are precisely the K-vector space endomorphisms of L, and it is well known that they form a group under composition.

3. Trivial.

4. If L/K is of finite degree, then L is a finite-dimension K-vector space, and thus (by the first point and by Rank-Nullity Theorem) an injective K-endomomorphism must be also surjective, i.e. it is an isomorphism.
If L/K is not of finite degree (which is possible!), then I don't know (and I even guess it's not true).

Exercise 69. Consider the following collection:

$$\Omega := \{N \subsetneq M \mid N \text{ subm. and } N \text{ is not a finite intersection of irreducible submodules}\}.$$

Suppose towards a contradiction that $\Omega \neq \emptyset$. Then Ω has a maximal element Q, since M is noetherian (because it's finitely generated over a noetherian ring).
Of course Q is not irreducible. This means that there exist N_1, N_2 such that $Q = N_1 \cap N_2$ with $Q \neq N_1$ and $Q \neq N_2$, i.e. $Q \subsetneq N_1, N_2 \neq M$. By maximality of Q, this means that N_1 and N_2 can be written as a finite intersection of irreducible submodules, and thus Q as well, contradiction.