

NMAG436 - HW1

Jan Oupický

1

By definition of L being AFF given by $f(\alpha, \beta) = 0$ we know that f is irreducible in \mathbb{Q} and $L = \mathbb{Q}(\alpha, \beta)$.

- (a) Using proposition 4.7 we know that α is transcendental over \mathbb{Q} because $\deg_y(f) = 2 > 0$ and also that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$. In other words, the basis A has 2 elements. Let $A = (1, \beta)$ (first element of basis A is 1 and the second is β). We can see that 1 and β are linearly independent:

$$\begin{aligned} c_1, c_2 \in \mathbb{Q}(\alpha) : 1c_1 + \beta c_2 = 0 &\stackrel{?}{\iff} c_1 = 0 = c_2 \\ 1c_1 + \beta c_2 = 0 &\iff \beta c_2 = -c_1 \stackrel{c_2 \neq 0}{\iff} \beta = \frac{-c_1}{c_2} \in \mathbb{Q}(\alpha) \\ \implies &\text{contradiction with } [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2 \implies c_1 = 0 = c_2 \end{aligned}$$

We know the basis has 2 elements and therefore A is a basis.

- (b) Using the same reasoning (β is also transcendental over \mathbb{Q}) using symmetry (we can just replace y with x) we get that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] = \deg_x(f) = 3$. Therefore the basis B has 3 elements. Let $B = (1, \alpha, \alpha^2)$. Following the proof of lemma 4.6 let $m(x) := f(x, \beta) \in \mathbb{Q}(\beta)[x]$. The proof shows that $m(x) = -x^3 - 2x^2 - 1 + \beta^2$ is a minimal polynomial of α over $\mathbb{Q}(\beta)$.

We want to prove that elements of B are linearly independent $\iff (b_0 + b_1\alpha + b_2\alpha^2 = 0 \text{ where } b_1, b_2, b_3 \in \mathbb{Q}(\beta) \iff b_1 = 0, b_2 = 0, b_3 = 0)$. Assume that there exists $b_1 + b_2\alpha + b_3\alpha^2 = 0$ where at least one $b_i \neq 0$. That would mean that α is a root of a non zero polynomial $\in \mathbb{Q}(\beta)[x]$. Since $m(x)$ is a minimal polynomial of $\alpha \implies m(x) | b_1 + b_2x + b_3x^2$ which is impossible since $\deg_x(m) = 3 > \deg_x(b_1 + b_2x + b_3x^2)$. That's a contradiction therefore $1, \alpha, \alpha^2$ are linearly independent and form a basis.

- (c) We will use equalities given by $f(\alpha, \beta) = 0 \implies \beta^2 = \alpha^3 + 2\alpha^2 + 1, \alpha^3 = \beta^2 - 2\alpha^2 - 1$.

$$\begin{aligned} [\alpha^3\beta^3]_A : \alpha^3\beta^3 &= \alpha^3((\alpha^3 + 2\alpha^2 + 1)\beta) = \beta(\alpha^6 + \alpha^5 + \alpha^3), (\alpha^6 + \alpha^5 + \alpha^3) \in \mathbb{Q}(\alpha) \\ A = (1, \beta) &\implies [\alpha^3\beta^3]_A = (0, \alpha^6 + \alpha^5 + \alpha^3) \\ [\alpha^3\beta^3]_A : \alpha^3\beta^3 &= (\beta^2 - 2\alpha^2 - 1)\beta^3 = 1(\beta^5 - \beta^3) + \alpha^2(-2\beta^3) \\ B = (1, \alpha, \alpha^2) &= (\beta^5 - \beta^3, 0, -2\beta^3) \end{aligned}$$

2

- (a) Let $\gamma := (1, 2)^T \in \mathbb{Q}^2$. By calculating derivatives $\frac{\partial f}{\partial x}(\gamma) = -7, \frac{\partial f}{\partial y}(\gamma) = 4$ we get $t_\gamma(f) = -7(x - 1) + 4(y - 2) = -7x + 4y - 1$. Let $(a_1, a_2) := (-7, 4)$ from lemma 5.6. Using lemma 5.6 we know we are looking for $\sigma := \theta_A \tau_{-\gamma}$ where A is a regular rational matrix of the form $A = \begin{pmatrix} b_1 & b_2 \\ -7 & 4 \end{pmatrix}$. From definition of σ we get $\sigma(1, 2)^T =$

$$A(0,0)^T = 0.$$

Let $(b_1, b_2) = (1, 0)$ for example. We can see that A is regular. We now have to calculate the polynomial \hat{f} following the proof of lemma 5.6. We will first calculate $\tilde{f}(x, y)$.

$$\begin{aligned} p(x, y) &:= \tilde{f}(x-1, y-2) = f(x, y) - t_\gamma(f) = y^2 - x^3 - 2x^2 + 7x - 4y \\ \tilde{f}(x, y) &\stackrel{\text{substitution}}{=} p(x+1, y+2) = y^2 - x^3 - 5x^2 \\ A^{-1} &= \begin{pmatrix} 1 & 0 \\ \frac{7}{4} & \frac{1}{4} \end{pmatrix} \implies \theta_{A^{-1}}^*(p(x, y)) = p(x, \frac{7}{4}x + \frac{1}{4}y) \\ \hat{f}(x, y) &= \theta_{A^{-1}}^*(\tilde{f}(x, y)) = \tilde{f}(x, \frac{7}{4}x + \frac{1}{4}y) = -x^3 - \frac{31x^2}{16} + \frac{7xy}{8} + \frac{y^2}{16} \\ &\implies h(x) := -x^3 - \frac{31x^2}{16}, g(x, y) := \frac{7x}{8} + \frac{y}{16} \\ \sigma^*(p(x, y)) &= p(x-1, -7x+4y-1) \end{aligned}$$

We can check $\sigma^*(\hat{f} + y) = \sigma^*(h(x) + yg(x, y) + y) = f$. The desired map is σ , where A is for example written above.

- (b) From the lemma 5.6 we know σ has the form $\sigma := \theta_A \tau_{-\gamma}$, where $A = \begin{pmatrix} b_1 & b_2 \\ -7 & 4 \end{pmatrix}$ is regular $\iff \det(A) \neq 0$. We will now calculate $\sigma(0, 0)^T$:

$$\begin{aligned} A &= \begin{pmatrix} b_1 & b_2 \\ -7 & 4 \end{pmatrix}, \sigma(0, 0)^T = A \begin{pmatrix} -1 \\ 2 \end{pmatrix} = -1 \begin{pmatrix} b_1 \\ -7 \end{pmatrix} - 2 \begin{pmatrix} b_2 \\ 4 \end{pmatrix} = \begin{pmatrix} -b_1 - 2b_2 \\ -1 \end{pmatrix} \\ \text{we want } \det(A) &\neq 0 \iff 4b_1 + 7b_2 \neq 0 \iff b_1 \neq \frac{-7}{4}b_2 \\ \text{in other words } \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} &\in \mathbb{Q}^2 \setminus \text{Span}_{\mathbb{Q}} \begin{pmatrix} -7 \\ 4 \end{pmatrix} \end{aligned}$$

To sum it up. There exists σ satisfying given conditions if and only if $\mathbf{a} = \begin{pmatrix} -b_1 - 2b_2 \\ -1 \end{pmatrix}$ where $(b_1, b_2)^T$ is not in the span of the vector $(-7, 4)$.

3

ν is a normalized DV of L , by definition that means there exists $R \subseteq L$ DVR with a maximal ideal M and uniformizing element $t \in M : (t) = M$ and $\nu := \nu_t$. We also know that $R = \theta_M$ (notation). We also know that $\nu(\alpha - 1) > 0, \nu(\beta - 2) > 0$.

Theorem 5.8 tells us (using $\gamma = (1, 2)$) that there exists exactly one $P \in \mathbb{P}_{L/K}$ s.t. $\nu_P(\alpha - 1) > 0, \nu_P(\beta - 2) > 0$. By definition $P = (p), p \in P$ and $\nu_P := \nu_p$. Theorem 2.15 (2) tells us that $\theta_M = \theta_P \implies \nu = \nu_P$. So from now on we can work with this uniquely defined DV ν .

Using 2) from 5.8 we can assume that $l(\gamma) = 0$ since we are only looking for l_0, l_1, l_2 when $\nu(l(\alpha, \beta)) > 0$. Let $(u, v) := \bar{\sigma}(\alpha, \beta)$ as in the proof of 5.8 with $(b_1, b_2) = (1, 0)$.

In the proof we see that $l(\alpha, \beta) \in \text{Span}(u, v)$ if $l(\gamma) = 0$, that means $\exists k_1, k_2 \in \mathbb{Q} : l(\alpha, \beta) = k_1u + k_2v$. Using definition of ν_p we see that $(p|l(\alpha, \beta)) \iff p|k_1u + k_2v \implies \nu(l(\alpha, \beta)) = \nu(k_1u + k_2v)$.

We also know using proposition 5.5 that $\nu(u) = 1$ and $\nu(v) = m > 1$ where $m := \text{mult}(h) = \text{mult}(-x^3 - \frac{31x^2}{16})$ from exercise 2 $\implies \nu(v) = 2$.

Now using properties of valuation (assuming $k_1, k_2 \neq 0$): $\nu(k_1u) = \nu(k_1) + \nu(u) = 0 + 1 = 1$, $\nu(k_2v) = \nu(k_2) + \nu(v) = 0 + 2 = 2 \xrightarrow{2.13} \nu(k_1u + k_2v) = \min(\nu(k_1u), \nu(k_2v)) = \min(1, 2) = 1$.

$\nu(k_1u + k_2v) = 1 \iff k_1 \neq 0, k_2 \in \mathbb{Q}$. If $k_2 = 0$ then we have $\nu(k_1u) = 1$ as stated above.

Similarly we can see that $\nu(k_1u + k_2v) = 2 \iff k_1 = 0, k_2 \neq 0$. Also by choosing any combination of $k_1, k_2 \in \mathbb{Q}$ we cannot get $\nu(k_1u + k_2v) = 3$.

Now we have constraints on $k_1, k_2 \in \mathbb{Q}$ and we can "transform" these elements ($k_1u + k_2v$) to a α, β representation using $\bar{\sigma}(\alpha) = u, \bar{\sigma}(\beta) = v$. $\bar{\sigma}^{-1} := \tau_{-\gamma}^{-1}\theta_A^{-1} = \tau_\gamma\theta_{A^{-1}}$ with the values from exercise 2. We see that $\bar{\sigma}^{-1}(k_1u + k_2v) = k_1 + k_1\alpha + 2k_2 + \frac{7}{4}k_2\alpha + \frac{1}{4}k_2\beta$. When we rearrange these elements we can form $l(\alpha, \beta) = l_0 + l_1\alpha + l_2\beta$ where (using vector notation for simplicity):

$$\begin{pmatrix} l_0 \\ l_1 \\ l_2 \end{pmatrix} = k_1 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + k_2 \begin{pmatrix} 2 \\ \frac{7}{4} \\ \frac{1}{4} \end{pmatrix}$$

We defined conditions on k_1, k_2 based on valuation value and now we have expressed l_0, l_1, l_2 using k_1, k_2 . To sum it if then:

$$\begin{aligned} \nu(l(\alpha, \beta)) = 1 &\iff \begin{pmatrix} l_0 \\ l_1 \\ l_2 \end{pmatrix} = k_1 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + k_2 \begin{pmatrix} 2 \\ \frac{7}{4} \\ \frac{1}{4} \end{pmatrix}, k_1 \in \mathbb{Q} \setminus \{0\}, k_2 \in \mathbb{Q} \\ \nu(l(\alpha, \beta)) = 2 &\iff \begin{pmatrix} l_0 \\ l_1 \\ l_2 \end{pmatrix} = k_2 \begin{pmatrix} 2 \\ \frac{7}{4} \\ \frac{1}{4} \end{pmatrix}, k_2 \in \mathbb{Q} \setminus \{0\} \end{aligned}$$

and $\nu(l(\alpha, \beta)) \neq 3$ for any values l_0, l_1, l_2 .