

Exercices de théorie de Galois :

Corrigé d'une question de l'exercice 9

Exercice 9. Soit $A = \mathbb{Z}$ et $K = \mathbb{Q}$ son corps de fractions.

1. (c) Démontrez que tout élément $x \in K^\times$ possède une écriture $x = up_1^{a_1} \cdots p_n^{a_n}$ avec $u \in A^\times$, $n \geq 0$, $p_i \in \mathcal{P}$ et $a_i \in \mathbb{Z} \setminus \{0\}$, unique à l'ordre près des facteurs.

Existence. Soit $x \in K^\times$. Choisissons une écriture sous forme de fraction $x = ua/b$ avec $u \in \{\pm 1\}$ et a, b entiers naturels non nuls et premiers entre eux. Notons P_+ l'ensemble des nombres premiers qui divisent a et P_- l'ensemble des nombres premiers qui divisent b . Posons $P(x) = P_+ \cup P_-$. Ces ensembles sont finis (peut-être vides) et disjoints puisque a et b sont premiers entre eux. Les décompositions en facteurs premiers de a et b ont la forme $a = \prod_{p \in P_+} p^{r_p}$ et $b = \prod_{p \in P_-} p^{s_p}$ avec $r_p, s_p > 0$. On a obtenu une écriture :

$$x = u \prod_{p \in P_+} p^{r_p} \prod_{p \in P_-} p^{-s_p}.$$

Si l'on énumère $P(x) = \{p_1, \dots, p_n\}$, ceci est bien une écriture de la forme $x = up_1^{a_1} \cdots p_n^{a_n}$ où les entiers r_p sont les exposants $a_i > 0$ et les entiers $-s_p$ sont les exposants $a_i < 0$.

Unicité. Considérons deux écritures $x = up_1^{a_1} \cdots p_n^{a_n} = vq_1^{b_1} \cdots q_m^{b_m}$ dans lesquelles les p_i sont tous distincts, et les q_j sont tous distincts. Alors $u = v = \text{sgn}(x)$. Notons :

$$\begin{aligned} I_+ &= \{i \in \{1, \dots, n\} \mid a_i > 0\} & I_- &= \{i \in \{1, \dots, n\} \mid a_i < 0\} \\ J_+ &= \{j \in \{1, \dots, m\} \mid b_j > 0\} & J_- &= \{j \in \{1, \dots, m\} \mid b_j < 0\}. \end{aligned}$$

De l'égalité $p_1^{a_1} \cdots p_n^{a_n} = q_1^{b_1} \cdots q_m^{b_m}$ on tire une égalité où tous les exposants sont > 0 :

$$\prod_{i \in I_+} p_i^{a_i} \prod_{i \in J_-} q_i^{-b_i} = \prod_{i \in I_-} p_i^{-a_i} \prod_{j \in J_+} q_j^{b_j}.$$

Comme les p_i sont tous distincts, le lemme d'Euclide montre que chaque p_i avec $i \in I_+$ apparaissant dans le membre de gauche est égal à un q_j avec $j \in J_+$ du membre de droite, et que les exposants (multiplicités) de p_i et q_j sont égales. La même chose vaut avec les p_i avec $i \in I_-$, qui sont associés à un unique q_j avec $j \in J_-$. On construit ainsi deux bijections $\sigma_+ : I_+ \rightarrow J_+$ et $\sigma_- : I_- \rightarrow J_-$ d'où une bijection unique

$$\sigma : I_+ \amalg I_- = \{1, \dots, n\} \rightarrow J_+ \amalg J_- = \{1, \dots, m\},$$

telle que $p_i = q_{\sigma(j)}$ et $a_i = b_{\sigma(j)}$ pour tout i . Ceci est exactement dire que l'écriture est « unique à l'ordre près des facteurs ».