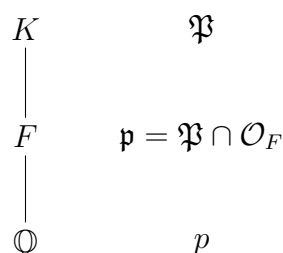


**Corrigé DM 2 : "Autour de la loi de réciprocité quadratique."**

**Exercice.**

1.



En notant  $e_{K/F}$  l'indice de ramification de  $\mathfrak{P}$  dans l'extension  $K/F$ ,  $e_{F/\mathbb{Q}}$  l'indice de ramification de  $\mathfrak{p}$  dans l'extension  $F/\mathbb{Q}$ , et  $e_{K/\mathbb{Q}}$  l'indice de ramification de  $\mathfrak{P}$  dans l'extension  $K/\mathbb{Q}$ , on a la relation (vue en cours)

$$e_{K/\mathbb{Q}} = e_{K/F} e_{F/\mathbb{Q}}. \quad (1)$$

En particulier, si  $\mathfrak{P}$  est non ramifié dans l'extension  $K/\mathbb{Q}$ , alors  $e_{K/\mathbb{Q}} = 1$  et a fortiori  $e_{F/\mathbb{Q}} = 1$ .

2. Pour tout  $x \in \mathcal{O}_F$ , on a  $\sigma_{\mathfrak{P}}(x) - x^p \in \mathfrak{P} \cap \mathcal{O}_F = \mathfrak{p}$ . L'automorphisme  $\sigma_{\mathfrak{P}}|_F$  vérifie donc la propriété caractérisant  $\sigma_{\mathfrak{p}}$ ; il lui est donc égal.

**Problème.**

- Comme  $G$  est isomorphe à  $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ , il est cyclique d'ordre  $p-1$  pair et contient donc un unique sous groupe  $H$  d'ordre  $\frac{p-1}{2}$ , qui est également l'unique sous-groupe d'indice 2 de  $G$ . Dans l'identification de  $G$  avec  $(\mathbb{Z}/p\mathbb{Z})^\times$ ,  $H$  correspond au sous-groupe des carrés de  $(\mathbb{Z}/p\mathbb{Z})^\times$ , c'est-à-dire au noyau de l'homomorphisme  $x \mapsto x^{\frac{p-1}{2}}$  de  $(\mathbb{Z}/p\mathbb{Z})^\times$  dans  $\{\pm 1\}$ .
- On sait (vu en cours), que  $p$  est totalement ramifié dans  $K$ . Autrement dit, avec les notations de l'exercice,  $p\mathcal{O}_K = \mathfrak{P}^{p-1}$ , et en particulier  $e_{K/\mathbb{Q}} = p-1$ . La relation (1) mentionnée plus haut montre alors que l'on a nécessairement  $e_{F/\mathbb{Q}} = 2$  (sinon  $e_{K/\mathbb{Q}} = e_{K/F} \leq \frac{p-1}{2}$ ). Ainsi,  $p$  est ramifié dans  $F$ . Inversement, si  $q$  est un premier ramifié dans  $F$ , alors, toujours en vertu de (1), il est également ramifié dans  $K$ . Or  $p$  est le seul premier ramifié dans l'extension  $K/\mathbb{Q}$ , donc  $q = p$ . Par ailleurs,  $F$  étant une extension quadratique de  $\mathbb{Q}$ , elle peut s'écrire  $F = \mathbb{Q}(\sqrt{d})$  pour un entier  $d$  sans facteurs carrés. Tenant compte du fait que

les premiers ramifiés dans  $F$  sont exactement les facteurs premiers du discriminant de  $F$ , qui vaut  $d$  ou  $4d$  selon que  $d \equiv 1 \pmod{4}$  ou pas, on conclut que la seule possibilité pour que  $p$  soit le seul premier ramifié dans  $F = \mathbb{Q}(\sqrt{d})$  est que  $d = p$  si  $p \equiv 1 \pmod{4}$  et  $d = -p$  si  $p \equiv 3 \pmod{4}$  (le cas  $p \equiv 2 \pmod{4}$  est exclu puisque  $p$  est impair).

3. Le groupe de Galois de  $F/\mathbb{Q}$  s'identifie à  $G/H$ ; la restriction d'un élément  $\sigma$  de  $G$  à  $F$  est donc égale à l'identité si et seulement si  $\sigma \in H$ . En vertu de l'identification de  $G$  (resp.  $H$ ) à  $(\mathbb{Z}/p\mathbb{Z})^\times$  (resp. au sous-groupe des carrés de  $(\mathbb{Z}/p\mathbb{Z})^\times$ ) via l'application  $j$ , on voit que la restriction de  $\sigma_\Omega$  à  $F$  est triviale si et seulement si  $j(\sigma_\Omega)$  est un carré modulo  $p$ , c'est-à-dire si et seulement si  $\left(\frac{q}{p}\right) = +1$ .
4. Le groupe de décomposition  $D_q$  est engendré par  $\tau_q$ . Il est donc trivial si et seulement si  $\tau_q$  est égal à l'identité. Par ailleurs, la trivialité de  $D_q$  équivaut au fait que  $q$  soit décomposé dans l'extension galoisienne  $F/\mathbb{Q}$ <sup>1</sup>.
5. C'est une application directe du résultat établi dans l'exercice.
6. On a les équivalences

$$\sigma_\Omega|_F = \text{Id}_F \Leftrightarrow \left(\frac{q}{p}\right) = +1 \quad (2)$$

$$\tau_q = \text{Id}_F \Leftrightarrow q \text{ décomposé dans } F/\mathbb{Q} \Leftrightarrow \left(\frac{d}{q}\right) = +1 \quad (3)$$

Ces deux équivalences, jointes à la relation  $\sigma_\Omega|_F = \tau_q$  montrent donc bien que  $\left(\frac{q}{p}\right) = \left(\frac{d}{q}\right)$ .

7. La formule  $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$  est claire, car  $a \in \mathbb{F}_q^\times$  est un carré si et seulement si  $a^{\frac{q-1}{2}} = 1$ . Comme le symbole de Legendre est multiplicatif, et que  $d = (-1)^{\frac{p-1}{2}} p$ , on obtient donc

$$\left(\frac{q}{p}\right) = \left(\frac{d}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right). \quad (4)$$

---

<sup>1</sup>en notant  $g$  le nombre d'idéaux premiers au-dessus de  $q$ ,  $e$  et  $f$  les indices de ramification et degré résiduel communs à tous ces idéaux, on a  $|D_q| = fe$ , ce qui, joint à la relation  $efg = [F : \mathbb{Q}] = 2$ , montre que  $q$  est décomposé si et seulement si  $D_q$  est trivial.