A SIMPLE PROOF OF NOETHER'S THEOREM

by ROBIN J. CHAPMAN

(Received 13 July, 1994)

1. Introduction. We present an elementary proof of the theorem, usually attributed to Noether, that if L/K is a tame finite Galois extension of local fields, then $\mathfrak{O}_L$ is a free $\mathfrak{O}_K\Gamma$-module where $\Gamma = \mathrm{Gal}(L/K)$. The attribution to Noether is slightly misleading as she only states and proves the result in the case where the residual characteristic of K does not divide the order of Γ [**4**]. In this case $\mathfrak{O}_K\Gamma$ is a maximal order in $K\Gamma$ which is not true for general groups Γ. There is an elegant proof in the standard reference [**2**], but this relies on a difficult result in representation theory due to Swan. Our proof depends on a close examination of the structure of tame local extensions, and uses only elementary facts about local fields. It also gives an explicit construction of a generator element, and the same proof works both for localizations of number fields and of global function fields.

2. Definitions and terminology. Let K be a field equipped with a non-trivial discrete valuation. We denote its valuation ring by $\mathfrak{O}_K$ and we let $\mathfrak{P}_K$ be the maximal ideal of $\mathfrak{O}_K$. We say that K is a *local field* if K is complete with respect to its valuation, and its *residue field* $k = \mathfrak{O}_K/\mathfrak{P}_K$ is finite. We call the characteristic p of k, the *residual characteristic* of K. If L/K is a finite extension of local fields, then $\mathfrak{P}_K\mathfrak{O}_L = \mathfrak{P}_L^e$ for some positive integer e, the *ramification index* of L/K. A finite extension L/K is called *tame* if the residual characteristic p does not divide the ramification index e of L/K. We write actions of Galois groups exponentially, and consider Galois modules as right modules. We have the following theorem.

THEOREM 1. *Let L/K be a finite tame Galois extension of local fields, and let $\Gamma = \mathrm{Gal}(L/K)$. Then for all integers n, the fractional ideal $\mathfrak{P}_L^n$ is free of rank one as an $\mathfrak{O}_K\Gamma$-module.*

3. Proof of Theorem 1. We begin with a lemma which will help us to simplify the problem.

LEMMA 1. *If Theorem 1 is true for L' where L' is a finite unramified extension of L, then Theorem 1 is true for L.*

Proof. It is clear that L' is Galois over K. Let $\Sigma = \mathrm{Gal}(L'/K)$ and $\Delta = \mathrm{Gal}(L'/L) \le \Sigma$ so that $\Gamma \cong \Sigma/\Delta$. As L'/L is unramified we have for each n

$$\mathfrak{P}_L^n = \mathfrak{P}_{L'}^n \cap L = \mathfrak{P}_{L'}^n \cap L'^{\Delta} = (\mathfrak{P}_{L'}^n)^{\Delta}.$$

Now if $\mathfrak{P}_{L'}^n$ is free on α as an $\mathfrak{O}_K\Sigma$-module then $\mathfrak{P}_L^n$ is free on $\mathrm{Tr}_{L'/L}\alpha$ as an $\mathfrak{O}_K\Gamma$-module.

For convenience let $\mathfrak{o} = \mathfrak{O}_K$, $\mathfrak{O} = \mathfrak{O}_L$, $\mathfrak{p} = \mathfrak{P}_K$ and $\mathfrak{P} = \mathfrak{P}_L$. Fix a generator π of the $\mathfrak{o}$-ideal $\mathfrak{p}$, and let $q = |k|$. Let $k = \mathfrak{o}/\mathfrak{p}$, $k' = \mathfrak{O}/\mathfrak{P}$ and $f = |k':k|$. Let K'/K be the maximal unramified subextension of L/K, so that $\mathrm{Gal}(L/K') = \Gamma_0$, the inertia subgroup of Γ. By standard theory [**5** §IV.2, Corollary 1] the inertia group Γ_0 is isomorphic to a subgroup of k'^*. Hence L is, a Kummer extension of K' and as L/K' is totally ramified we have

$L = K'((u\pi)^{1/e})$ where $e = |\Gamma_0|$ and u is a unit in $\mathfrak{D}_{K'}$. We now put $u = \zeta v$ where ζ is a root of unity, and $v \equiv 1 \pmod{\mathfrak{P}}$. As e is coprime to p, then v is an eth power in K'. Hence the unramified extension $L' = L(\zeta^{1/e})$ satisfies $L = K''(\pi^{1/e})$ where $K'' = K'(\zeta^{1/e})$ is unramified over K. By Lemma 1 we may assume that $L = K'(\pi^{1/e})$ where K' is unramified of degree f over K, and e divides $q^f - 1$.

With these assumptions we see that Γ is a semidirect product. Let $\eta \in K'$ be a primitive eth root of unity and let $\rho = \pi^{1/e}$. It is plain that the set of K-conjugates of ρ in L is $\{\eta^j\rho : 0 \le j < e\}$. The K'-automorphism γ of L defined by $\rho^\gamma = \eta\rho$ is a generator of Γ_0. We also define a K-automorphism φ of L, as follows; its restriction to K' is the Frobenius automorphism of the unramified extension K'/K, and $\rho^\varphi = \rho$. It is now clear that

$$\Gamma = \{\varphi^i\gamma^j : 0 \le i < f, 0 \le j < e\}.$$

By Nakayama's Lemma (see e.g., [**3**, Chapter 1, §2, Theorem 2.3]) it suffices to show that $\mathfrak{P}^n/\pi\mathfrak{P}^n$ is a free $k\Gamma$-module, as any free generator of this module will lift immediately to a free $\mathfrak{o}\Gamma$-generator of $\mathfrak{P}^n$. Now

$$\mathfrak{P}^n/\pi\mathfrak{P}^n = \mathfrak{P}^n/\mathfrak{P}^{n+e} = k'\bar{\rho}^n \oplus k'\bar{\rho}^{n+1} \oplus \ldots \oplus k'\bar{\rho}^{n+e-1}.$$

Let $a = \bar{\rho}^n + \bar{\rho}^{n+1} + \ldots + \bar{\rho}^{n+e-1}$. We calculate

$$a^{\gamma^j} = \sum_{i=n}^{n+e-1} \bar{\eta}^{ij}\bar{\rho}^i$$

and so, by the invertibility of the Vandermonde matrix, the elements $a, a^\gamma, a^{\gamma^2}, \ldots, a^{\gamma^{e-1}}$ are linearly independent over k'. Note that $a^\varphi = a$.

Let α be a normal basis for k' over k, i.e., the elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{f-1}}$ are linearly independent over k. (Such an element exists by the normal basis theorem [**1**, Chapter 5, Theorem 7.5].) I claim that αa is a free generator of $\mathfrak{P}^n/\pi\mathfrak{P}^{n+e}$ as a $k\Gamma$-module. It suffices to prove that the set $\{(\alpha a)^\delta : \delta \in \Gamma\}$ is linearly independent over k. We first note that

$$(\alpha a)^{\varphi^i\gamma^j} = \alpha^{q^i}a^{\gamma^j}.$$

It follows that if $\beta_{i,j} \in k$ with

$$\sum_{i=0}^{f-1}\sum_{j=0}^{e-1} \beta_{i,j}(\alpha a)^{\varphi^i\gamma^j} = 0,$$

then

$$\sum_{j=0}^{e-1}\left(\sum_{i=0}^{f-1} \beta_{i,j}\alpha^{q^i}\right)a^{\gamma^j} = 0.$$

The inner sum vanishes for all j by the k'-linear independence of the a^{γ^j}, and so each $\beta_{i,j} = 0$ as the α^{q^i} are linearly independent over k. This concludes the proof.

REFERENCES

1. P. M. Cohn, *Algebra, vol.* 3 (2nd ed.) (Wiley, 1991).
2. A. Fröhlich, *Galois module structure of algebraic integers* (Springer, 1983).

3. H. Matsumura, *Commutative ring theory* (Cambridge University Press, 1986).

4. E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, *J. Reine Angew. Math.* **167** (1932), 147–152.

5. J.-P. Serre, *Local fields* (Springer, 1979).

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF EXETER
EXETER EX4 4QE
UK