MATH. SCAND. 65 (1989), 165–174

ON p-GROUPS AS GALOIS GROUPS

GUDRUN BRATTSTRÖM

The so-called Noether problem of determing which finite groups (all, conjecturally) can occur as Galois groups of extensions of the rational numbers has been studied extensively, not least in recent years – see for instance [S]. Naturally the same question can be asked for other fields than $\mathbf{Q}$. Given a field K and a finite group G, we say that G is *realizable over* K if there exists a Galois extension N of K whose Galois group is isomorphic to G; we shall sometimes call such an extension a G-extension of K. One can also look for pairs of finite groups G and H such that for any field K, the realizability of G implies that of H. The obvious example is when H is a homomorphic image of G. However, there are others, most of which can be found in [J]. For instance, if you can realize the cyclic group of odd prime order p over a field K, then you can realize all cyclic groups of order p^n, $n \geqq 1$. (See [W] and [K-L]). In this paper we consider the two non-abelian groups of order p^3, where p is an odd prime number. (For $p = 2$, see [J].) I wish to thank Professor Christian U. Jensen for suggesting this topic to me.

1.

The problem of realizing finite groups as Galois groups is closely related to what I shall call the "Galois embedding problem". Consider a finite Galois extension L/K, and let $G = \mathrm{Gal}(L/K)$. Let

$$1 \to A \to E \to G \to 1$$

be a group extension, where A is an abelian group with a fixed G-action, and let $\varepsilon \in H^2(G, A)$ be the corresponding cohomology class. The Galois embedding problem is then to find an E-extension N of K which contains L and is "compatible" with the group extension, i.e. there should exist a surjective homomorphism Φ making the following diagram commute:

$$\begin{array}{ccccccccc} & & & & & & \mathrm{Gal}(\bar{K}/K) & & \\ & & & & & \Phi \swarrow & \downarrow \phi & & \\ 1 & \to & A & \to & E & \to & G & \to & 1 \end{array}$$

Received October 31, 1988

where $\phi\colon \mathrm{Gal}(\bar{K}/K) \to G$ is the homomorphism given by restriction to L. We then say that the Galois embedding problem $(L/K, \varepsilon)$ is solvable. Without the condition that Φ be surjective this is a purely cohomological problem, and its solution is given by a theorem of Hoechsmann [Ho] stating that such a homomorphism Φ exists if and only if the element $\phi^*(\varepsilon) \in H^2(\mathrm{Gal}(\bar{K}/K), A)$ vanishes. The surjectivity of Φ generally has to be established by other means. In some cases it is however automatic in the sense that $\phi^*(\varepsilon) = 0$ implies the existence of a surjective Φ. This is so when G and E are p-groups of the same rank (when in fact all solutions Φ are surjective), and also when K is a number field ([Ho], Satz 2.3 and Satz 6.6 respectively). The two groups of order p^3 mentioned above are both central extensions of a cyclic group of order p by an abelian group of type (p, p), and both have rank two. If p is odd, which we shall henceforth be assuming, they are given by the relations

$$D_1\colon\ u^p = v^p = w^p = 1,\ uv = vuw,$$

$$D_2\colon\ u^{p^2} = v^p = 1,\ uv = vu^{1+p},$$

respectively. The center of D_i ($i = 1$ or 2) clearly equals the cyclic kernel of the extension, and since a normal subgroup of order p of a p-group is central, we see that a D_i-extension N/K contains a unique (p, p)-extension L/K. Whenever $x^p - 1$ splits in K and K has characteristic different from p, the letter ζ will throughout this paper denote a fixed non-trivial pth root unity in K. In this situation the extension L/K can be described explicitly as a Kummer extension: we have $L = K(\sqrt[p]{a}, \sqrt[p]{b})$, for some elements a and b of K^* whose images in the $\mathbb{F}_p$-vector space K^*/K^{*p} are linearly independent. In this case the Galois embedding problem has been solved completely by R. Massy; we have the following theorem (see [M], Corollaire pp. 523–524), with the notations and hypotheses of this paragraph.

THEOREM 1 (Massy). *Let K and the elements a and b be fixed; let $L = K(\sqrt[p]{a}, \sqrt[p]{b})$. Then*

(i) *the extension L/K can be embedded in a D_1-extension if and only if b is a norm from $K(\sqrt[p]{a})$ to K, and*

(ii) *the extension L/K can be embedded in a D_2-extension if and only if there exist α and β in K such that $L = K(\sqrt[p]{\alpha}, \sqrt[p]{\beta})$ and such that $\zeta\beta$ is a norm from $K(\sqrt[p]{\alpha})$ to K.*

We wish to prove the following.

THEOREM 2. *If D_1 is realizable over K then so is D_2. If K has characteristic p or if $x^{p^2} - 1$ splits in $K(\mu_p)$, then the converse also holds.*

PROOF. If K has characteristic p then the realizability of a p-group G over

K depends only on the rank of G (see [Wi], Satz p. 237), so D_1 and D_2 both having rank two, the theorem follows. From now on let us assume $\operatorname{char}(K) \neq p$.

If $x^{p^2} - 1$ splits in K, then the conditions (i) and (ii) in Massy's theorem are equivalent, so the realizability of one of the groups D_i implies that of the other, with the same intermediate field L.

Now suppose that $x^p - 1$ splits in K but $x^{p^2} - 1$ does not. Suppose that N is a Galois extension of K with $\operatorname{Gal}(N/K)$ isomorphic to D_1, and let $L = K(\sqrt[p]{a}, \sqrt[p]{b})$ be the intermediate field. The images of a and b in K^*/K^{*^p} are linearly independent and therefore cannot both be contained in the line generated by the image of ζ. Suppose for instance that the image of a lies outside this line. Then the extension $L = K(\sqrt[p]{a}, \sqrt[p]{\zeta})$ satisfies condition (ii) of Massy's theorem, and we conclude that D_2 is realizable over K.

Finally, let us drop the assumption that $x^p - 1$ splits in K. Suppose that N is a Galois extension of K such that $\operatorname{Gal}(N/K)$ is isomorphic to D_1. Then so is $\operatorname{Gal}(N(\mu_p)/K(\mu_p))$. Hence it follows from what we have already proved that there exists a D_2-extension M of $K(\mu_p)$. Moreover, if $x^{p^2} - 1$ splits in $K(\mu_p)$, then we may choose M such that its intermediate (p,p)-subextension is the same as that of $N(\mu_p)$; as before we call this field L. We know that $L = L'(\mu_p)$, where L' is the intermediate (p,p)-subextension of N/K. It now follows from a theorem by R. Gillard ([G], Théorème 5; see also section 2 below) that L' is contained in a D_2-extension of K. The converse follows similarly.

If $x^{p^2} - 1$ does not split in $K(\mu_p)$, let L_1 and L_2 be the intermediate (p,p)-subextensions of $N(\mu_p)/K(\mu_p)$ and $M/K(\mu_p)$ respectively. Then $L_1 = K(\mu_p)(\sqrt[p]{a}, \sqrt[p]{b})$ for some a and b in $K(\mu_p)$, and we may choose M so that (interchanging a and b if necessary) $L_2 = K(\mu_p)(\sqrt[p]{a}, \sqrt[p]{\zeta})$. Note that L_1, being the composite of $K(\mu_p)$ and a (p,p)-extension of K, is abelian over K. In particular $K(\mu_p)(\sqrt[p]{a})$ is abelian over K. So is $K(\mu_p)(\sqrt[p]{\zeta}) = K(\mu_{p^2})$. Hence L_2 is also an abelian extension of K, and since p does not divide $[K(\mu_p): K]$ there has to exist a (p,p)-extension L'_2 of K such that $L_2 = L'_2(\mu_p)$. Thus we can use Gillard's theorem again, and we are done.

The following example shows that the converse of our theorem need not hold in the case when $x^p - 1$, but not $x^{p^2} - 1$ splits in $K(\mu_p)$.

EXAMPLE. Let l be a prime which is congruent to 1 (mod p) but not (mod p^2), and let $K = \mathbb{Q}_l$. Then

$$\dim_{\mathbb{F}_p} K^*/K^{*^p} = 2,$$

and therefore by local class field theory

$$\dim_{\mathbb{F}_p}[\mathrm{N}_{K(\sqrt[p]{a})/K}(K(\sqrt[p]{a})^*)/K^{*^p}] = 1$$

for any $a \in K^* \setminus K^{*p}$. On the other hand, a is a norm from $K(\sqrt[p]{a})$ to K, so there cannot exist b in $\mathsf{N}_{K(\sqrt[p]{a})/K}(K(\sqrt[p]{a})^*)$ such that the images of a and b in K^*/K^{*p} are linearly independent. Hence by Massy's theorem, D_1 is not realizable over K. However, K does possess extensions of type D_2: consider $L = K(\sqrt[p]{a}, \sqrt[p]{\zeta})$, where ζ is a non-trivial pth root of unity (note that our assumptions on l imply that ζ is in K^* but not in K^{*p}) and $a \in K^* \setminus \mu_p K^{*p}$. By Massy's theorem L is contained in a D_2-extension of K. More explicitly, an example of such an extension is $L(\sqrt[p^2]{a}) = K(\mu_{p^2})(\sqrt[p^2]{a})$.

2.

This section is devoted to a somewhat more detailed investigation of the problem of "descending" from a D_i-extension of $K(\mu_p)$ to one of K. We are assuming the field K to have characteristic different from p. Gillard's theorem, which we used in the proof of Theorem 2, is the following:

THEOREM 3 (Gillard). *Let L/K be a Galois extension with $G = \mathrm{Gal}(L/K)$ of type (p, p), and let A be a cyclic group of order p. Let $\varepsilon \in H^2(G, A)$ correspond to a non-abelian group of order p^3. Then the embedding problem $(L/K, \varepsilon)$ is solvable if and only if $(L(\mu_p)/K(\mu_p), \theta^*(\varepsilon))$ is, where θ^* is induced by the isomorphism θ: $\mathrm{Gal}(L(\mu_p)/K(\mu_p)) \xrightarrow{\sim} \mathrm{Gal}(L/K)$.*

REMARK. Gillard's paper is for the most part concerned with number fields, but this particular argument can be carried out using only Galois cohomology and Satz 2.3 in [Ho].

If N/K is a solution to the problem $(L/K, \varepsilon)$, then one of the solutions to $(L(\mu_p)/K(\mu_p), \theta^*(\varepsilon))$ is $N(\mu_p)/K(\mu_p)$. Note, however, that neither solution is uniquely determined by ε. Indeed, given one solution Φ: $\mathrm{Gal}(\bar{K}/K) \to E$ to $(L/K, \varepsilon)$, the others are given by $\Phi\Psi$ (pointwise multiplication), where $\Psi \in \mathrm{Hom}(\mathrm{Gal}(\bar{K}/K), A) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(\bar{K}/K), E)$; $\ker(\Phi)$ and $\ker(\Phi\Psi)$ need not be equal. The analogous statement holds for $L(\mu_p)/K(\mu_p)$. In particular, it is not immediately clear how to construct an explicit solution to $(L/K, \varepsilon)$ from one to $(L(\mu_p)/K(\mu_p), \theta^*(\varepsilon))$. This is however the object of the present section.

The following lemma is standard.

LEMMA. *Let E/F be a finite Galois extension, where F has characteristic different from p and contains the* pth *roots of unity. Let $x \in E^*$ and let $M = E(\sqrt[p]{x})$. Then M is Galois over F if and only if for all $\sigma \in \mathrm{Gal}(E/F)$ there exists an integer m such that $\sigma(x)/x^m$ lies in E^{*p}. If $\mathrm{Gal}(E/F)$ is a p-group, then m may be taken to be* 1.

Now let $N/K(\mu_p)$ be a solution to $(L(\mu_p)/K(\mu_p), \theta^*(\varepsilon))$, where $\varepsilon \neq 0$. Since $N/L(\mu_p)$ is a Kummer extension there exists x in $L(\mu_p)^* \setminus L(\mu_p)^{*p}$ such that $N = L(\mu_p, \sqrt[p]{x})$. Let $H = \mathrm{Gal}(K(\mu_p)/K)$, and let k be an integer such that $k|H| \equiv$

1 (mod p). For all $\rho \in H$ let $i(\rho)$ be an integer such that $\rho(\zeta) = \zeta^{i(\rho)}$ and consider $\gamma = k \sum_{\rho \in H} i(\rho)\rho^{-1} \in \mathbf{Z}[H]$. The group ring $\mathbf{Z}[H]$ acts on $K(\mu_p)^*$ in the obvious fashion, and if we let H act trivially on L we get an action on $L(\mu_p)^*$ too.

THEOREM 4. *Let* $N' = L(\mu_p, \sqrt[p]{\gamma(x)})$. *Then:*
(i) N' *is Galois over* $K(\mu_p)$ *with* $\mathrm{Gal}(N'/K(\mu_p)) \cong \mathrm{Gal}(N/K(\mu_p))$.
(ii) N' *is Galois over* K *with* $\mathrm{Gal}(N'/K) \cong H \times \mathrm{Gal}(N/K(\mu_p))$.

PROOF. (i) Let B be the multiplicative group generated by x and $L(\mu_p)^{*p}$. Then by Kummer theory each $y \in B \setminus L(\mu_p)^{*p}$ yields a unique generator ξ_y of $\mathrm{Gal}(N/(L(\mu_p))$ such that

$$\frac{\xi_y(\sqrt[p]{y}}{\sqrt[p]{y}} = \zeta$$

Sending ξ_x to $\bar{1} \in \mathbf{F}_p$ we obtain an identification $\mathrm{Gal}(N/(L(\mu_p)) \xrightarrow{\sim} \mathbf{F}_p$, enabling us to view the cohomology class ε corresponding to the group extension

$$1 \to \mathrm{Gal}(N/(L(\mu_p)) \to \mathrm{Gal}(N/K(\mu_p)) \to \mathrm{Gal}(L(\mu_p)/K(\mu_p)) \to 1$$

as an element of $H^2(G, \mathbf{F}_p)$, where $G = \mathrm{Gal}(L(\mu_p)/K(\mu_p))$. The field $N = L(\mu_p, \sqrt[p]{x})$ is Galois over $K(\mu_p)$, so from each $\sigma \in G$ we obtain an element $x_\sigma \in L(\mu_p)^*$ such that $\sigma(x)/x = x_\sigma^p$. Massy ([M], formula (3.2)) has an explicit expression in terms of x_σ for a cocycle $X(\sigma, \tau)$ representing ε:

$$\frac{x_\sigma \sigma(x_\tau)}{x_{\sigma\tau}} = \zeta^{X(\sigma,\tau)}, \quad \sigma, \tau \in G.$$

Let $y = \gamma(x)$. Then we have

$$\frac{\sigma(y)}{y} = \frac{\sigma(\gamma(x))}{\gamma(x)} = \gamma\left(\frac{\sigma(x)}{x}\right) = \gamma(x_\sigma)^p,$$

so letting $y_\sigma = \gamma(x_\sigma)$, we get

$$\frac{y_\sigma \sigma(y_\sigma)}{y_{\sigma\tau}} = \gamma\left(\frac{x_\tau \sigma(x_\tau)}{x_{\sigma\tau}}\right) = \gamma(\zeta)^{X(\sigma,\tau)}.$$

But

$$\gamma(\zeta) = \left[\prod_{\rho \in H} \rho^{-1}(\zeta)^{i(\rho)}\right]^k = \left(\prod_{\rho \in H} \zeta\right)^k = \zeta^{k|H|} = \zeta,$$

so we get the same cocycle and hence in particular

$$\mathrm{Gal}(N'/K(\mu_p)) \cong \mathrm{Gal}(N/K(\mu_p)).$$

(ii) Let $\sigma \in \mathrm{Gal}(L(\mu_p)/K)$. Then σ may be written (uniquely) as a product $\sigma_0\sigma_1$, where σ_0 fixes L and σ_1 fixes $K(\mu_p)$. The field $N = L(\mu_p, \sqrt[p]{x})$ is Galois over $K(\mu_p)$, so $\sigma_1(x)/x$ lies in $L(\mu_p)^{*^p}$, a relation which we write

$$\sigma_1(x) \equiv x \bmod^\times L(\mu_p)^{*^p}.$$

Hence

$$\sigma(x) = \sigma_0(\sigma_1(x)) \equiv \sigma_0(x) \bmod^\times L(\mu_p)^{*^p},$$

so

$$\sigma(\gamma(x)) = \gamma(\sigma(x)) \equiv \gamma(\sigma_0(x)) = \sigma_0(\gamma(x)) \bmod^\times L(\mu_p)^{*^p}.$$

Viewing σ_0 as an element of $H = \mathrm{Gal}(K(\mu_p)/K)$, we have

$$\sigma_0\gamma = \sigma_0(k \sum_{\rho\in H} i(\rho)\rho^{-1}) = k \sum_{\rho\in H} i(\rho)\sigma_0\rho^{-1} \equiv k \sum_{\rho\in H} i(\sigma_0^{-1}\rho)^{-1} \equiv i(\sigma_0^{-1})\gamma (\bmod p\mathbf{Z}[H]).$$

Therefore

$$\sigma(\gamma(x)) \equiv \gamma(x)^{i(\sigma_0^{-1})} \bmod^\times L(\mu_p)^{*^p},$$

and we deduce from the lemma that the extension N'/K is Galois. Since $[N' : K(\mu_p)] = p^3$ is relatively prime to $[K(\mu_p) : K]$, the Galois group $\mathrm{Gal}(N'/K)$ will be the semidirect product of $H = \mathrm{Gal}(K(\mu_p)/K)$ and $\mathrm{Gal}(N'/K(\mu_p))$, with H acting on $\mathrm{Gal}(N'/K(\mu_p))$ by conjugation (see [Z], IV.7, Theorem 25). We shall show that this product is in fact direct, i.e. that the action of H on $\mathrm{Gal}(N'/K(\mu_p))$ is trivial. The field $L(\mu_p)$ is abelian over K, so we already know that the action on $\mathrm{Gal}(L(\mu_p)/K(\mu_p))$ is trivial. In other words, the group H acts via automorphisms of $E = \mathrm{Gal}(N'/K(\mu_p))$ which fix $E/\Phi(E)$ elementwise, $\Phi(E)$ being the Frattini subgroup of E. But by Theorem 12.2.2 in [H] the order of such an automorphism is a power of p, whereas $|H|$ is prime to p, so the action of H must be trivial.

COROLLARY. *Under the hypotheses of Theorem 4, there exists a D_i-extension N_0 of K such that $N' = N_0(\mu_p)$.*

PROOF. Let N_0 be the fixed field of the subgroup isomorphic to H.

3.

In this section we consider the case when either $\mathrm{char}(K) = p$ or $x^{p^2} - 1$ splits in K; so D_1 is realizable over K if and only if D_2 is. We will show that there exists, moreover, a fixed numerical relation between the number of D_1-extensions and the number of D_2-extensions of K provided one of these numbers is finite. For a field K and a finite group G, denote by $\nu(G, K)$ the number (possibly infinite) of G-extensions of K.

When $\mathrm{char}(K) \neq p$ we shall use cohomology to recognize the isomorphism classes of the Galois groups of the field extensions we have constructed. More precisely, consider $\varepsilon \in H^2(G, \mathsf{F}_p)$, with G of type (p, p) acting trivially on F_p. Up to isomorphism there are four possibilities for the middle group E in the short exact sequence: type (p, p, p), type (p^2, p), D_1 or D_2. Which one it is can be read off easily from the cohomology class ε. Following [F] (see also [M]) we define ε_*: $G \times G \to \mathsf{F}_p$ and ε^*: $G \to \mathsf{F}_p$ by

$$\varepsilon_*(\sigma, \tau) = X(\sigma, \tau) - X(\tau, \sigma);$$

$$\varepsilon^*(\sigma) = \sum_{r \,(\mathrm{mod}\, p)} X(\sigma^r, \sigma),$$

where X is a cocycle representing ε; it can be seen that ε_* and ε^* are independent of the choice of X. One can show (see [M]) that ε_* is an alternating bilinear form, that ε^* is a linear form (thinking of G as a 2-dimensional F_p-vector space), and that $\varepsilon = 0$ if and only if $\varepsilon_* = 0$ and $\varepsilon^* = 0$. (Only the first of these three statements remains true when $p = 2$, however.) It follows from the formulae (1.7) and (1.9) in [M] that the isomorphism class of E depends only on whether ε_* and ε^* are identically zero or not, as shown in the following table:

	$\varepsilon^* = 0$	$\varepsilon^* \neq 0$
$\varepsilon_* = 0$	(p, p, p)	(p^2, p)
$\varepsilon_* \neq 0$	D_1	D_2

THEOREM 5. *Let K be a field which either has characteristic p or contains μ_{p^2}. Then if one of $\nu(D_1, K)$ and $\nu(D_2, K)$ is finite, so is the other, and we have*

$$\nu(D_2, K) = (p^2 - 1)\, \nu(D_1, K).$$

PROOF. First we deal with the case of characteristic p. Then by [Wi], p. 237 the finiteness of $\nu(G, K)$ for a p-group G depends only on K and not on G. Moreover, applying the theorem on the same page to D_1 and D_2, we find that if $\nu(D_1, K)$ and $\nu(D_2, K)$ are finite then

$$\nu(D_2, K) = \frac{|\mathrm{Aut}\,(D_1)|}{|\mathrm{Aut}\,(D_2)|}\, \nu(D_1, K).$$

Let u, v and w be as in section 1. Then any automorphism α of D_1 is of the form $\alpha(u) = u^i v^k w^m$, $\alpha(v) = u^j v^l w^n$, where (i, k) and (j, l) constitute a basis for $\mathsf{F}_p \times \mathsf{F}_p$ (thus $(p^2 - 1)(p^2 - p)$ possibilities) and m, $n \in \mathsf{F}_p$ (thus p^2 possibilities). So $|\mathrm{Aut}\,(D_1)| = p^2(p^2 - 1)(p^2 - p)$. The automorphisms of D_2 are given by $\alpha(u) = u^i v^k$, $\alpha(v) = u^{pj} v$, where i is a generator of $\mathbf{Z}/p^2\mathbf{Z}$ (thus $(p^2 - p)$ possibilities), and k, $j \in \mathsf{F}_p$ (thus p^2 possibilities). So $|\mathrm{Aut}\,(D_2)| = p^2(p^2 - p)$, and our theorem is proved for fields of characteristic p.

Now let K be a field of characteristic different from p in which $x^{p^2} - 1$ splits. By a previous remark any realization of D_i over K contains a unique (p,p)-extension of K, so it suffices to prove the formula

$$\nu(D_2, L/K) = (p^2 - 1)\,\nu(D_1, L/K),$$

where $\nu(D_i, L/K)$ is the number of D_i-extensions of K which contain a fixed (p,p)-extension L. Define an equivalence relation $\sim$ on the set of non-abelian Galois extensions N/K of degree p^3 and containing L, by setting $N \sim N'$ if and only if there exist $x \in L^*$ and $a \in K^*$ such that $N = L(\sqrt[p]{x})$ and $N' = L(\sqrt[p]{ax})$. (If $N = L(\sqrt[p]{x})$, $N' = L(\sqrt[p]{ax}) = L(\sqrt[p]{y})$ and $N'' = L(\sqrt[p]{by})$, then there must exist an integer i, not divisible by p, such that $y \equiv (ax)^i \bmod^\times L^{*p}$. Thus $by \equiv ba^i x^i \bmod^\times L^{*p}$, and we have $N = L(\sqrt[p]{x^i})$ and $N'' = L\sqrt[p]{ba^i x^i})$, proving the transivity of $\sim$.) Since $\sigma(ax)/ax = \sigma(x)/x$ for all $\sigma \in \mathrm{Gal}\,(L/K)$, the two extensions N/K and N'/K together with ξ_x and ξ_{ax} respectively (defined as in the proof of Theorem 4) give rise to the same cohomology class $\varepsilon \in H^2(G, \mathsf{F}_p)$. In particular $\mathrm{Gal}\,(N/K)$ and $\mathrm{Gal}\,(N'/K)$ are isomorphic. Next we note that $L(\sqrt[p]{x}) = L(\sqrt[p]{ax})$ only if either $x \in L^{*p}K^*$, i.e. $\mathrm{Gal}\,(L(\sqrt[p]{x})/K)$ is abelian of exponent p, a case we are excluding – or $a \in L^{*p}$; conversely $a \in L^{*p}$ clearly implies that $L(\sqrt[p]{x}) = L(\sqrt[p]{ax})$. Hence each equivalence class has the same number of elements, viz. $(K^*\colon L^{*p} \cap K^*)$. What this means is that it suffices to prove the formula with the number of equivalence classes of D_1- and D_2-extensions in place of the number of actual extensions. We shall do this by constructing a map λ from the set of all equivalence classes of D_2-extensions of K containing L to the set of all equivalence classes of D_1-extensions of K containing L, and then showing that the inverse image of any class of D_1-extensions has exactly $p^2 - 1$ elements.

Let Γ_2 be an equivalence class of D_2-extensions of K containing L, and let $N_2 = L(\sqrt[p]{x})$ be a representative. Let ε_2 be the cohomology class corresponding to N_2/K and ξ_x. Then ε_2^* is a homomorphism from G to F_p, and by Kummer theory there is a unique element $\tilde{c} \in (L^{*p} \cap K^*)/K^{*p}$ such that for any of its representatives c in $L^{*p} \cap K^*$ we have $\zeta^{\varepsilon_2^*(\sigma)} = \sigma(\sqrt[p]{c})/\sqrt[p]{c}$ for all $\sigma \in G$. Let $y = x\sqrt[p]{c^{-1}}$. Now put $\lambda(\Gamma_2) = \Gamma_1$, where Γ_1 is the equivalence class of $N_1 = L(\sqrt[p]{y})$. Since two representatives of $\tilde{c}$ differ by an element of K^{*p}, the class Γ_1 is independent of which c we pick. The class Γ_1 is also independent of x (as long as $N_2 = L(\sqrt[p]{x})$), since replacing x by x^i replaces ε_2^* by $i\varepsilon_2^*$, and hence c by c^i, producing the extension $L(\sqrt[p]{y^i}) = L(\sqrt[p]{y}) = N_1$. Finally, replacing N_2 by an equivalent extension $L(\sqrt[p]{ax})$ gives $L(\sqrt[p]{ay})$, which is equivalent to N_1. So λ is well-defined. Let ε_1 be the cohomology class corresponding to N_1 and ξ_y. Choose $\zeta_\sigma \in \mu_{p^2} \subseteq K$ for each σ such that $\sigma(\sqrt[p]{c})/\sqrt[p]{c} = \zeta_\sigma^{-p}$; then $\sigma(y)/y = (\zeta_\sigma x_\sigma)^p$. Thus we have

$$\zeta^{\varepsilon_1^*(\sigma)} = \prod_{r(\bmod p)} \frac{\zeta_{\sigma^r} x_{\sigma^r} \sigma^r(\zeta_\sigma x_\sigma)}{\zeta_{\sigma^{r+1}} x_{\sigma^{r+1}}} = \zeta^{\varepsilon_2^*(\sigma)} \prod_{r(\bmod p)} \frac{\zeta_{\sigma^r}\zeta_\sigma}{\zeta_{\sigma^{r+1}}}.$$

Choosing $\zeta_{\sigma^r} = \zeta_\sigma^r$ for $r = 0, 1, \ldots, p-1$, we see that

$$\prod_{r(\bmod p)} \frac{\zeta_{\sigma^r}\zeta_\sigma}{\zeta_{\sigma^{r+1}}} = \frac{\zeta_\sigma^{p-1}\zeta_\sigma}{\zeta_\sigma^0} \prod_{r=0}^{p=2} \frac{\zeta_{\sigma^r}\zeta_\sigma}{\zeta_{\sigma^{r+1}}} = \zeta_\sigma^p = \frac{\sqrt[p]{c}}{\sigma(\sqrt[p]{c})} = \zeta^{-\varepsilon_2^*(\sigma)},$$

so ε_1^* is identically zero. Since ζ_σ is left fixed by G, it follows from formula (3.2) in [M] (quoted in section 2 above) that $\varepsilon_{1,*} = \varepsilon_{2,*}$, so N_1 is indeed a D_1-extension.

Now fix a class Γ_1 of D_1-extensions, and let $N_1 = L(\sqrt[p]{y})$ belong to Γ_1. Suppose that Γ_2 is such that $\lambda(\Gamma_2) = \Gamma_1$. Using the definition of $\sim$ and λ, we see that Γ_2 must have a member of the form $L(\sqrt[p]{c})$, where $x = y\sqrt[p]{c}$, for some $c \in L^{*^p} \cap K^*$. Thus we have to determine the number of inequivalent such extensions, for fixed y. So let us suppose

$$L(\sqrt[p]{y\sqrt[p]{c}}) \sim L(\sqrt[p]{y\sqrt[p]{d}}),$$

where $c, d \in L^{*^p} \cap K^*$. Hence for some integer j not divisible by p and some $a \in K^*$,

$$ay\sqrt[p]{c} \equiv y^j \sqrt[p]{d^j} \bmod^\times L^{*^p}.$$

We claim that $j \equiv 1 \pmod p$. For if not then we get $y \equiv b\sqrt[p]{e} \bmod^\times L^{*^p}$ for some $b \in K^*$ and some $e \in L^{*^p} \cap K^*$; but then $N_1 = L(\sqrt[p]{b\sqrt[p]{e}}) \sim L(\sqrt[p^2]{e})$, which is an abelian extension of K, contrary to assumption. Hence $j \equiv 1 (\bmod p)$, and we get $c^{-1}da^p \in L^{*^{p^2}}$. Thus $K(\sqrt[p^2]{c^{-1}da^p})$ is contained in L and therefore has degree at most p (or else it would be cyclic of degree p^2 and would not fit inside L). This means that $c^{-1}da^p$, hence $c^{-1}d$ belongs to K^{*^p}. Conversely, it is clear that if $c \equiv d \bmod^\times K^{*^p}$ then

$$L(\sqrt[p]{y\sqrt[p]{c}}) \sim L(\sqrt[p]{y\sqrt[p]{d}}).$$

Using calculations similar to the ones above it is easy to see that $x = y\sqrt[p]{c}$ gives a D_2-extension $L(\sqrt[p]{x})$ if and only if c is not a pth power in K.

Thus we conclude that the elements of the inverse image of Γ_1 are in one-to-one correspondence with the non-zero elements of $(L^{*^p} \cap K^*)/K^{*^p}$. As there are $p^2 - 1$ of these, the theorem is proved.

REFERENCES

[F] A. Fröhlich, *The rational characterization of certain sets of relatively abelian extensions*, Philos. Trans. Roy. Soc. London Ser.A 251 (1959), 385–425.

[G] R. Gillard, *Plongement d'une extension d'ordre p ou p^2 dans une surextension non abelienne d'ordre p^3*, J. Reine Angew. Math. 268–269 (1974), 418–426.
[H] M. Hall, *The Theory of Groups*, Macmillan, 1959.
[Ho] K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. 229 (1968), 81–106.
[J] C. U. Jensen, *On the representations of a group as a Galois group over an arbitrary field*, Copenhagen University Preprint Series No. 14, 1987.
[J-Y] C. U. Jensen and N. Yui, *Quaternion extensions*, Copenhagen University Preprint Series No. 10, 1987.
[K-L] W. Kuyk and H. W. Lenstra, *Abelian extensions of arbitrary fields*, Math. Ann. 216 (1975), 99–104.
[M] R. Massy, *Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p*, J. of Alg. 109 (1987), 508–535.
[S] J.-P. Serre, *Groupes de Galois sur Q*, Sém. Bourbaki 1987-88, exposé no. 689.
[W] G. Whaples, *Algebraic extensions of arbitrary fields*, Duke Math. J. 24 (1957), 201–204.
[Wi] E. Witt, *Konstruktion von galoisschen Körpern der Characteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. Reine Angew. Math. 174 (1936), 237–245.
[Z] H. Zassenhaus, *The Theory of Groups*, Chelsea Publishing Company, 1949.

MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
BOX 6701
11385 STOCKHOLM
SWEDEN