if $\xi \neq (0, 0, \ldots, 0, 1)$ is a solution to $Q_0(\xi) = 1$, from (3.13) and (3.16) we find that

$$(4.3)\qquad N_2(s; \alpha, 1) = \begin{cases} q^{s-2}, & s \text{ odd}, \\ q^{s-2} + \tau q^{(s-2)/2} e(\alpha) = q^{s-2} - \tau q^{(s-2)/2}, & s \text{ even}, \end{cases}$$

where $e(\alpha) = -1$ ([3], p. 199). Therefore, from (3.3), we obtain

$$(4.4)\qquad N(s; 1, \alpha, 1) = \begin{cases} (q^{s-1} - 1) q^{s-2}, & s \text{ odd}, \\ (q^{s-1} - \tau q^{(s-2)/2})(q^{s-2} - \tau q^{(s-2)/2}), & s \text{ even}, \end{cases}$$

which is the number of solutions to (4.1).

References

[1] L. Carlitz, *Gauss sums over finite fields of order* 2^n, Acta Arith. 15 (1969), pp. 247–265.

[2] — *Reduction formulas for certain multiple exponential sums*, Czechoslovak Math. J. 20 (95) (1970), pp. 616–627.

[3] L. E. Dickson, *Linear groups with an exposition of the Galois theory*, New York 1958.

[4] J. D. Fulton, *Representations by quadratic forms in a finite field of characteristic two*, Math. Nachr. 77 (1977), pp. 237–243.

Received on 2. 9. 1976 (874)

ACTA ARITHMETICA
XXXV (1979)

Some results on p-extensions of local and global fields

by

ROBERT J. BOND (Chestnut Hill, Mass.)

1. Introduction. Let K be a local or a global field, p a prime, and $\tilde{K}$ the maximal p-extension of K; i.e., $\tilde{K}$ is the compositum of all Galois extensions of K of p-power degree. Let $G_K(p)$ be the Galois group of $\tilde{K}$ over K. The structure of $G_K(p)$ is well-known in the local case and is studied in some detail in the global case by Koch [3] and Höchsmann [2].

In this paper we consider the following question: what information about K is contained in $G_K(p)$ considered as an abstract pro-p-group? A similar question was answered by Neukirch in the case where K is a finite normal extension of the rationals. He shows in [4] that K is determined completely by the Galois group of the maximal solvable extensions of K over K. If K is a global field of non-zero characteristic, the effect of the Galois group of the separable closure of K over K is considered in [1].

Let K be a local field with residue class field k of characteristic $p_0 \neq p$. We prove that $G_K(p)$ determines $k^*(p)$, the p-primary part of the multiplicative group $k^* = k - \{0\}$. In the global case we show that $G_K(p)$ determines whether or not K has a primitive pth root of unity. We then restrict our attention to function fields with finite constant field k and show that $G_K(p)$ determines $k^*(p)$, $p \neq \operatorname{char} K$; more explicitly, if K and K' are two function fields of char $p_0 \neq p$ with constant fields k and k' respectively and if $G_K(p)$ and $G_{K'}(p)$ are isomorphic algebraically and topologically as pro-p-groups, then $k^*(p) \approx k'^*(p)$.

We then consider continuous automorphisms of $G_K(p)$ where K is a function field containing a primitive pth root of unity. We prove that if L is a constant field extensions of K of p-power degree, then $G_L(p)$ is a characteristic subgroup of $G_K(p)$.

First some notation. If K is a field, $\tilde{K}$ will denote the maximal p-extension of K and $G_K(p)$ or $G(\tilde{K}/K)$ the Galois group of $\tilde{K}$ over K. G_K will denote the Galois group of the separable closure of K over K. $H^n(G_K(p))$ will be the nth cohomology group $H^n(G_K(p), Z/pZ)$. If v is a valuation of K we let K_v be the completion of K with respect to v. We will write $\delta(K) = 1$ or 0 depending on whether or not K has a primitive pth root of unity.

Finally, if n is a positive integer, p a prime, we call $m \geqslant 0$ the *p-exponent of n* if p^m divides n but p^{m+1} does not.

In addition, we recall that the pth cohomological dimension $\mathrm{cd}_p(G_K(p)) \leqslant \mathrm{cd}_p(G_K)$ and that $H^n(G_K(p), A) \approx H^n(G_K, A)$ for all $n \geqslant 1$ if A is a torsion, p-primary $G_K(p)$-module. (See Serre, [7], II-4.)

2. Local results. Let K be a local field with residue class field k and let p be a prime, $p \neq \mathrm{char}\, k$. In this section, we will show that $G_K(p)$ determines $k^*(p)$.

The following result is well-known and can be found in [5] for the characteristic zero case. The proof for $\mathrm{char}\, K \neq 0$ is the same. See also [3].

PROPOSITION 1. *Let L be a separable extension of K.*

(1) *If $p^\infty \nmid [L:K]$ and $\delta(L) = 1$, then $G_L(p)$ is a Poincaré group of dimension 2 and rank 2.*

(2) *If $p^\infty \nmid [L:K]$ and $\delta(L) = 0$, then $G_L(p)$ is a free pro-p-group of rank $\leqslant 1$.*

(3) *If $p^\infty \mid [L:K]$, then $G_L(p)$ is a free pro-p-group of rank $\leqslant 1$.*

DEFINITION. Let G be a profinite group and p a prime. We define:

$$\chi_p(G) = \sup_{n\geqslant 0}\left\{\frac{1}{p^n}|H^1(G, Z/p^nZ)|\right\}.$$

PROPOSITION 2. $\chi_p(G_K(p)) = |k^*(p)|$.

Proof. $|H^1(G_K(p), Z/p^nZ)| = p^n|\mu_{p^n}|$ where μ_{p^n} is the group of p^nth roots of unity in K. It is easily shown that if n is the p-exponent of $|k^*|$, then $\mu_{p^n} \approx k^*(p)$.

COROLLARY. *Let K and K' be two local fields with residue class fields k and k' respectively. Assume that $p \neq \mathrm{char}\, k$ and $p \neq \mathrm{char}\, k'$. If $G_K(p) \approx G_{K'}(p)$, then $k^*(p) \approx k'^*(p)$.*

3. Some lemmas. Assume $\mathrm{char}\, K \neq p$ in this section.

LEMMA 1. *Let K be a field such that $\delta(K) = 1$. Let v be a valuation of K and w an extension of v to $\tilde{K}$. Then $\tilde{K}_w$ is the maximal p-extension of K_v.*

Proof. Suppose not. Then $\tilde{K}_w$ has a cyclic extension L of degree p. Then $L = \tilde{K}_w(a)$ where a is a root of $\chi^p - a$; $a \in \tilde{K}_w$. We can write $a = \lim a_i$ where each $a_i \in \tilde{K}$. By Krasner's lemma, if we choose i sufficiently large, $L = \tilde{K}_w(\beta)$ where β is a root of $X^p - a_i$. Then $\tilde{K}(\beta)$ is a Galois p-extension of $\tilde{K}$ and hence $\beta \in \tilde{K}$. Therefore, $L = \tilde{K}_w$, a contradiction.

LEMMA 2. *Let K be a Hensel field with respect to a valuation v. Suppose that $\delta(K_v) = 1$. Then $G_K(p) \approx G_{K_v}(p)$.*

Proof. By a theorem of Ostrowski, K is separably closed in K_v. Hence $\delta(K) = 1$. Let w be the extension of v to $\tilde{K}$. Then $G(\tilde{K}/K) \approx G(\tilde{K}_w/K_v)$ since v extends uniquely to $\tilde{K}$. But $G(\tilde{K}_w/K_v) = G_{K_v}(p)$ by Lemma 1.

LEMMA 3. *If $\delta(K) = 1$ and $K \neq \tilde{K}$, then K has at most one valuation which is undecomposed in $\tilde{K}$.*

Proof. Except for some obvious modifications, the proof is identical to the proof of Lemma 8 in [4].

LEMMA 4. *Let q be a positive integer relatively prime to p. Let m and n be positive integers such that $q^m - 1$ and $q^n - 1$ have the same positive p-exponent. Then m and n have the same p-exponent.*

Proof. Elementary.

4. Global results. In what follows, K_0 is a global field of characteristic $p_0 \geqslant 0$; $p_0 \neq p$. We let K be a separable, possibly infinite, p-extension of K_0 such that $K \subset \tilde{K}_0$.

PROPOSITION 3. *Let v run through all valuations of K_0. Then there is a monomorphism*

$$\varphi\colon H^2(G_{K_0}(p)) \to \bigoplus_v H^2(G_{K_{0v}}(p)).$$

If $\delta(K_0) = 0$, φ is an isomorphism. If $\delta(K_0) = 1$, coker φ has order p.

Proof. This result is due to Höchsmann [2].

If $[K : K_0] = \infty$, we can define

$$\varphi\colon H^2(G_K(p)) \to \prod_v H^2(G_{K_v}(p))$$

where v runs through all valuations of K. But note that here the image of φ is in the direct product.

PROPOSITION 4. $\varphi\colon H^2(G_K(p)) \to \prod_v H^2(G_{K_v}(p))$ *is a monomorphism.*

Proof. This proof is similar to Neukirch's proof of Satz II in [6]. We write $K = \bigcup_{i=0}^{\infty} K_i$ where each K_i is a finite separable p-extension of K_0. Let v be a valuation of K such that $\delta(K_v) = 1$. (We have only to consider such valuations for if $\delta(K_v) = 0$, $H^2(G_{K_v}(p)) = 0$ by Proposition 1.) Let $v_i = v|K_i$ and $\hat{K} = \bigcup_{i=0}^{\infty} K_{iv_i} \subset K_v$. Then $\hat{K}$ is a Hensel field whose completion at v is K_v. So by Lemma 2, $H^2(G_{\hat{K}}(p)) \approx H^2(G_{K_v}(p))$. Hence the following diagram is commutative:

$$\begin{array}{ccc} H^2(G_{K_i}(p)) & \xrightarrow{\mathrm{res}_i} & H^2(G_K(p)) \\ \Big\downarrow{\scriptstyle e_{v_i}} & & \Big\downarrow{\scriptstyle e_v} \\ H^2(G_{K_{iv_i}}(p)) & \xrightarrow{\mathrm{res}_{v_i}} & H^2(G_{\hat{K}}(p)) \end{array}$$

Let $x \in H^2(G_K(p))$ and assume $\varphi(x) = (x_v) = 0$. Then $\varrho_v(x) = 0$ for all v. Now $x = \operatorname{res}_i(x_i)$ for all $i \geqslant i_0$ for some i_0; $x_i \in H^2(G_{K_i}(p))$. Let $x_{v_i} = \varrho_{v_i}(x_i) \in H^2(G_{K_{iv_i}}(p))$. Then $0 = \varrho_v(x) = \operatorname{res}_{v_i}\varrho_{v_i}(x_i) = \operatorname{res}_{v_i}(x_{v_i})$.

Let V_i be the set of valuations v_i of K_i such that $x_{v_i} \neq 0$. Then each V_i is a finite set since in the finite global field case the image of φ is in the direct sum. The V_i's form an inverse system. Let $V = \varprojlim V_i$. Then V is the empty set since $\varrho_v(x) = 0$ for all v. Therefore V_i is empty for i sufficiently large. This implies that $x_{v_i} = 0$ for all valuations v_i of K_i and hence $x_i = 0$ since

$$H^2(G_{K_i}(p)) \to \bigoplus_{v_i} H^2(G_{K_{iv_i}}(p))$$

is one-to-one. Therefore $x = 0$.

PROPOSITION 5. *Suppose that $G_K(p) \approx G_F(p)$ where F is a local field of* $\operatorname{char} p_0$ *and $\delta(F) = 1$. Then K has a valuation v such that:*

(i) *v is discrete with finite residue class field,*

(ii) $\delta(K_v) = 1$,

(iii) *If v extends to $\tilde{v}$ on $\tilde{K}$, then $\tilde{K}_{\tilde{v}}$ is the maximal p-extension of K_v,*

(iv) *The decomposition field of $\tilde{v}$ over K is a finite extension of K.*

Proof. For each valuation v of K, let $\tilde{v}$ be an extension to $\tilde{K}$ and D_v the decomposition field of $\tilde{v}$ over K. Let $G_v = G_{K_v}(p)$ and $H_v = G(\tilde{K}_{\tilde{v}}/K_v)$. Then $H_v \approx G(\tilde{K}/D_v)$. The map φ of Proposition 4 can be factored as:

$$\varphi\colon H^2(G_K(p)) \xrightarrow{\alpha} \prod_v H^2(H_v) \xrightarrow{\beta} \prod_v H^2(G_v).$$

Since φ is one-to-one, so is α. Now $G_K(p) \approx G_F(p)$ and $\delta(F) = 1$, so $H^2(G_K(p)) \neq (0)$. Therefore, there exists a valuation v of K such that $H^2(H_v) \neq (0)$.

Claim. $G_v = H_v$.

Let Ω_v be the maximal p-extension of K_v. Let $R_v = G(\Omega_v/\tilde{K}_{\tilde{v}})$ and $v_0 = v\,|\,K_0$. Then p^∞ divides $[\tilde{K}_{\tilde{v}}: K_{0v_0}]$. (Otherwise, $G(\tilde{K}/D_v) \approx H_v$ would be a finite closed subgroup of $G_K(p)$ contradicting the fact that $\operatorname{cd}_p(G_K(p)) = 2$.) So by Proposition 1, R_v is a free pro-p-group of rank $\leqslant 1$. If R_v has rank 1, then $\operatorname{cd}_p(G_v) = \operatorname{cd}_p(R_v) + \operatorname{cd}_p(H_v)$. (See Serre [7], I-32.) But $\operatorname{cd}_p(H_v) = 2$ and $\operatorname{cd}_p(G_v) \leqslant 2$. So $R_v = \{1\}$ and $G_v = H_v$.

Since $H^2(G_v) \neq (0)$, $\delta(K_v) = 1$ and K_v is a finite extension of K_{0v_0}. Hence v is discrete with finite residue class field.

Since $G_K(p) \approx G_F(p)$, $G(\tilde{K}/D_v) \approx G_{F_1}(p)$ where F_1 is a p-extension of F. Then $[F_1:F] < \infty$ since $G(\tilde{K}/D_v) \approx G_v$ and $\operatorname{cd}_p(G_v) = 2$. Therefore, $[D_v:K] < \infty$.

PROPOSITION 6. *Suppose $\delta(K) = 1$. Then the following are equivalent:*

(1) *K has a discrete valuation v with finite residue class field such that v is undecomposed in $\tilde{K}$.*

(2) *$G_K(p) \approx G_F(p)$ where F is a local field of* $\operatorname{char} p_0$ *and $\delta(F) = 1$.*

Proof. (1) $\Rightarrow$ (2) follows easily by taking $F = K_v$. Conversely, suppose (2) holds. Let v be the valuation of K satisfying the 4 properties of Proposition 5. It suffices to show that $D_v = K$. Let N be the normal closure of D_v over K. Then $[N:K] < \infty$ since $[D_v:K] < \infty$. Hence $N \neq \tilde{K}$. If $D_v \neq K$, then v extends to another valuation w on $\tilde{K}$. Let D_w be the decomposition field of w over K. Since D_w is conjugate to D_v, $D_w \subset N$ which implies that N has two valuations which are undecomposed in $\tilde{K}$. This contradicts Lemma 3. Therefore $D_v = K$.

THEOREM 1. *Let K_0 and K_0' be two global fields of* $\operatorname{char} p_0 \geqslant 0$; $p_0 \neq p$. *Suppose that $G_{K_0}(p) \approx G_{K_0'}(p)$. Then $\delta(K_0) = 1$ iff $\delta(K_0') = 1$.*

Proof. Assume $\delta(K_0) = 1$ and let $\lambda\colon G_{K_0}(p) \to G_{K_0'}(p)$ be the isomorphism. Let v be a valuation of K_0 extending to $\tilde{v}$ on $\tilde{K}_0$. Let K be the decomposition field of $\tilde{v}$ over K_0. Denote $\tilde{v}\,|\,K$ by v also. Then $K_v = K_{0v}$ so by Proposition 6, $G_K(p) \approx G_F(p)$ where F is a local field of $\operatorname{char} p_0$ and $\delta(F) = 1$. (Note: $F = K_{0v}$.)

Then $\lambda(G_K(p)) = G_{K'}(p)$ for some p-extension K' of K_0'; $K' \subset \tilde{K}_0'$. By Proposition 5, there exists a valuation v' of K' such that

(i) v' is discrete with finite residue class field,

(ii) $\delta(K'_{v'}) = 1$,

(iii) If v' extends to $\tilde{v}'$ on $\tilde{K}_0'$, then $\tilde{K}'_{0\tilde{v}'}$ is the maximal p-extension of $K'_{v'}$,

(iv) The decomposition field $D_{v'}$ of $\tilde{v}'$ over K' is a finite extension of K'.

Now let E' be the decomposition field of $\tilde{v}'$ over K_0' and denote $\tilde{v}\,|\,K_0'$ by v' also. Clearly $E' \subset D_{v'}$.

Claim. $E' = D_{v'}$.

Let $H_{v'} = G_{E'}(p) \approx G_{K'_{0v'}}(p)$ and let

$$H_v = \lambda^{-1}(H_{v'}) = G(\tilde{K}/E) \quad \text{for some subfield } E \text{ of } \tilde{K}_0.$$

Since $H_v \approx G_{K'_{0v'}}(p)$ and $\delta(K'_{0v'}) = 1$, by Proposition 6, E has a discrete valuation w which is undecomposed in $\tilde{K}_0$. Let $\lambda^{-1}(G(K_0'/D_{v'})) = G(\tilde{K}_0/D)$. Then $E \subset D$. Extend w to w_1 on D. Then by Lemma 3, $w = \tilde{v}\,|\,E$. This implies that $K \subset E$ and hence $K' \subset E'$. Therefore, $D_{v'} \subset E'$ and hence $D_{v'} = E'$.

Let $G_v = G_K(p)$ and $G_{v'} = G_{K'}(p)$. Then, to summarize the above steps, $G_v \approx G_{K_{0v}}(p)$, $\lambda(G_v) = G_{v'}$ and G_v has a closed subgroup H_v of finite index in G_v such that $\lambda(H_v) = H_{v'} \approx G_{K'_{0v'}}(p)$. We can do this for each valuation v of K_0.

Let S' be the set of valuations v' of K' obtained in this way. Now consider the following commutative diagram:

$$\begin{tikzcd}
H^2(G_{K_0}(p)) \arrow[r, "\varphi"] \arrow[d, "\lambda_1"] & \bigoplus_v H^2(G_v) \arrow[r, "\alpha"] \arrow[d, "\lambda_2"] & \bigoplus_v H^2(H_v) \arrow[d, "\lambda_3"] \\
H^2(G_{K'_0}(p)) \arrow[r, "\beta"] & \bigoplus_{v' \in S'} H^2(G_{v'}) \arrow[r, "\gamma"] & \bigoplus_{v' \in S'} H^2(H_{v'})
\end{tikzcd}$$

The maps $\lambda_1, \lambda_2, \lambda_3$ are isomorphisms induced by λ as described above. α and γ are induced by the restriction maps. By Proposition 3, φ is one-to-one but not onto, since $\delta(K_0) = 1$.

Assume $\delta(K'_0) = 0$. Then, again by Proposition 3, $\gamma\beta$ is onto.

Claim. If $G_v \neq H_v$, then res: $H^2(G_v) \to H^2(H_v)$ is the zero map.

We know that $[G_v : H_v] = p^m$ for some $m \geqslant 0$. We have isomorphisms inv_1: $H^2(G_v) \to Z/pZ$ and inv_2: $H^2(H_v) \to Z/pZ$ induced by the invariant maps of the corresponding Brauer groups. Furthermore, $\mathrm{inv}_2 \circ \mathrm{res} = [G_v : H_v]\,\mathrm{inv}_1$ which implies that res is the zero map if $m > 0$.

Case 1. Suppose there is a valuation v_1 of K such that $G_{v_1} \neq H_{v_1}$. We have a commutative diagram:

$$\begin{tikzcd}
H^2(G_{K_0}(p)) \arrow[r, "\varphi_1"] \arrow[d, "\approx"] & H^2(G_{v_1}) \arrow[r, "\alpha_1"] \arrow[d, "\approx"] & H^2(H_{v_1}) \arrow[d, "\approx"] \\
H^2(G_{K'_0}(p)) \arrow[r, "\beta_1"] & H^2(G_{v'_1}) \arrow[r, "\gamma_1"] & H^2(H_{v'_1})
\end{tikzcd}$$

The maps are obtained from the previous diagram by projecting onto the v_1-factor.

By the above claim, $\alpha_1 = 0$; hence $\gamma_1 = 0$. But $\gamma_1\beta_1$ is onto since $\gamma\beta$ is onto. This implies that $H^2(H_{v'_1}) = 0$, a contradiction.

Case 2. Suppose $G_v = H_v$ for all v.

In this case, α and γ are the identity maps. Hence β is onto which implies that φ is also onto, again a contradiction.

Therefore, $\delta(K'_0) = 1$. ∎

We will now restrict our attention to the function field case; i.e., we will assume $p_0 > 0$.

Theorem 2. *Let K_0, K'_0 be two function fields of* $\mathrm{char}\, p_0 > 0$, $p_0 \neq p$, *with finite fields of constants k_0 and k'_0 respectively. Assume $\delta(K_0) = 1$. If $G_{K_0}(p) \approx G_{K'_0}(p)$, then $k_0^*(p) \approx k_0'^*(p)$.*

Proof. By Theorem 1, we know that $\delta(K'_0) = 1$. Also, by the steps described in the proof of Theorem 1, given a valuation v of K_0, there is a valuation v' of K'_0 such that if K is the decomposition field of $\tilde{v}$ over K_0, then $\lambda(G_K(p)) = G_{K'}(p)$ where K' is the decomposition field of $\tilde{v}'$ over K'_0.

Let P and P' be the prime divisors associated to v and v' respectively and let d, d' be their degrees. Let k and k' be the corresponding residue class fields. Assuming that $|k_0| = p_0^f = q$ and $|k'_0| = p_0^{f'} = q'$, we have $|k| = q^d$ and $|k'| = q'^{d'}$.

Now $G_{K_{0v}}(p) \approx G_K(p) \approx G_{K'}(p) \approx G_{K'_{0v'}}(p)$, so by the corollary to Proposition 2, $k^*(p) \approx k'^*(p)$; i.e., $q^d - 1$ and $q'^{d'} - 1$ have the same p-exponent.

Let $D = P_1^{n_1} P_2^{n_2} \ldots P_r^{n_r}$ be a divisor of K_0 of degree 1. Then $\sum n_i d_i = 1$ where $d_i = \deg P_i$. For each i, let P'_i be the corresponding prime of K'_0, $d'_i = \deg P'_i$, and let k_i, k'_i be the respective residue class fields. So $q^{d_i} - 1$ and $q'^{d'_i} - 1$ have the same p-exponent. Call it m_i. Let m and m' be the p-exponents of $q - 1$ and $q' - 1$ respectively. Clearly $m \leqslant m_i$ and $m' \leqslant m_i$ for all i.

$$q^{d_i} - 1 = (q-1)(1 + q + q^2 + \ldots + q^{d_i - 1})$$

and $q \equiv 1 \pmod{p}$ since $\delta(K_0) = 1$. Hence if $m_i < m$, $d_i \equiv 0 \pmod{p}$. But this cannot happen for all i since the d_i's are relatively prime. So there is at least one i such that $m_i = m$. Therefore, $m' \leqslant m$ and by symmetry $m' = m$. Hence $k_0^*(p) \approx k_0'^*(p)$.

Corollary 1. *Suppose $\delta(K_0) = 1$, $|k_0| = p_0^f$ and $|k'_0| = p_0^{f'}$. If $G_{K_0}(p) \approx G_{K'_0}(p)$, then f and f' have the same p-exponent.*

Proof. This follows immediately from Theorem 2 and Lemma 4.

Corollary 2. *Suppose $\delta(K_0) = 1$ and λ: $G_{K_0}(p) \to G_{K'_0}(p)$ is an isomorphism. Let L be a finite Galois p-extension of K_0 and L' the fixed field of $\lambda(G_L(p))$. Let E and E' be the constant fields of L and L' respectively. Then $[E : k_0] = [E' : k'_0]$.*

Proof. Let $[E : k_0] = p^n$ and $[E' : k'_0] = p^m$. Then by Theorem 2, $p_0^{fp^n} - 1$ and $p_0^{f'p^m} - 1$ have the same p-exponent. Applying Lemma 4 and Corollary 1 we get that $m = n$.

Theorem 3. *If $\delta(K_0) = 1$ and L is a constant field extension of K_0 of p-power degree, then $G_L(p)$ is a characteristic subgroup of $G_K(p)$.*

References

[1] R. Bond, *Function fields with isomorphic Galois groups*, to appear, Trans. Amer. Math. Soc.

[2] K. Höchsmann, *Über die Gruppe der maximalen l-Erweiterung eines globalen Körpers*, J. Reine Angew. Math. 222 (1966), pp. 142–147.

[3] H. Koch, *Galoissche Theorie der p-Erweiterungen*, VEB Deutscher Verlag der Wissenschaften, Berlin 1970.

[4] J. Neukirch, *Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galois gruppe der maximal auflösbaren Erweiterungen*, J. Reine Angew. Math. 238 (1969), pp. 135–147.

[5] J. Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*, Invent. Math. 6 (1969), pp. 296–314.
[6] — *Über eine algebraische Kennzeichnung der Henselkörper*, J. Reine Angew. Math. 231 (1968), pp. 75–81.
[7] J. P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math, no. 5, Springer-Verlag, Berlin and New York 1965.

DEPARTMENT OF MATHEMATICS
BOSTON COLLEGE
Chestnut Hill, Massachusetts, USA

Received on 22. 9. 1976 (878)

ACTA ARITHMETICA
XXXV (1979)

Brauer's class number relation

by

C. D. Walter (Dublin)

The main part of this paper proves R. Brauer's class number relation [1] in a shorter and more natural way. Consequently it is possible to obtain Stark's generalization [8] with no extra effort and to observe that the theorem may be applied using only the units of the occurring fields. Nehrkorn's conjecture [6] that there exists a corresponding class group isomorphism is also shown to be correct.

I should like to thank Professors Cassels and Fröhlich for many helpful suggestions, and Trinity College, Cambridge, for financial support.

1. Relation theorems. In this first section are derived some general results to describe relations in torsion modules and in torsion-free modules. All the modules concerned will be finitely generated.

Let $\mathfrak{D}$ be a Dedekind domain contained in a field K of characteristic zero and write $\mathfrak{D}_\mathfrak{p} = \{\alpha/\beta \in K \mid \alpha \in \mathfrak{D},\ \beta \in \mathfrak{D}-\mathfrak{p}\}$ for its localisation at the prime ideal $\mathfrak{p}$. Then a $\mathfrak{D}$-lattice M is a finitely generated torsion-free $\mathfrak{D}$-module. M will be identified with its natural embedding in $KM = K\otimes_\mathfrak{D} M$ and $M_\mathfrak{p}$ will be written for $\mathfrak{D}_\mathfrak{p}\otimes_\mathfrak{D} M$.

If M and N are two $\mathfrak{D}$-lattices of $KM = KN$ then the index $[M:N]$ may be defined through the local indices $[M_\mathfrak{p}:N_\mathfrak{p}]$ for the free $\mathfrak{D}_\mathfrak{p}$-modules $M_\mathfrak{p}$ and $N_\mathfrak{p}$. Let $\delta_\mathfrak{p}$ be the determinant of a matrix which describes a basis of $N_\mathfrak{p}$ in terms of one for $M_\mathfrak{p}$. Then $[M_\mathfrak{p}:N_\mathfrak{p}] = \mathfrak{D}_\mathfrak{p}\delta_\mathfrak{p}$ is well-defined and non-zero. By taking free $\mathfrak{D}$-submodules of M and N with the same rank as M and N it is clear that the $\delta_\mathfrak{p}$ can be chosen equal for almost all $\mathfrak{p}$ and that the ratio of two $\delta_\mathfrak{p}$ is always in the field of fractions k of $\mathfrak{D}$. Hence the intersection over all primes $\mathfrak{p}$ which defines the index, viz.

$$[M:N] = \bigcap_\mathfrak{p} [M_\mathfrak{p}:N_\mathfrak{p}]$$

is the product of an ideal in $\mathfrak{D}$ and an element of K. If M and N are isomorphic then $[M:N] = \mathfrak{D}\delta$ for the determinant $\delta \in K$ of the corresponding automorphism of KM. Thus for $\mathfrak{D} = \boldsymbol{Z}$ and $K = \boldsymbol{C}$ this coincides with the usual definition of the index viewed as an ideal, and when $K = k$ the definition coincides with that of Fröhlich [2]. If K/k is a number