CLASS GROUPS AND BRAUER GROUPS

BY
JACK SONN

ABSTRACT

Let F be a global field, n a positive integer not divisible by the characteristic of F. Then there exists a finite extension E of F whose class group has a cyclic direct summand of order n. This theorem, in a slightly stronger form, is applied to determine completely, on the basis of the work of Fein and Schacher, the structure of the Brauer group $\mathrm{Br}(F(t))$ of the rational function field $F(t)$. As a consequence of this, an additional theorem of the above authors, together with a note at the end of the paper, imply that $\mathrm{Br}(F(t)) \simeq \mathrm{Br}(F(t_1, \cdots, t_n))$, where $t_1, \cdots, t_n$ are algebraically independent over F.

In this paper we will prove the following theorem.

THEOREM 1. *Let F be a global field, n a positive integer not divisible by the characteristic of F. Then there exists a finite extension E of F whose class group has a cyclic direct summand of order n.*

The motivation for this theorem is a conjecture of Fein and Schacher [3] on the Brauer group $\mathrm{Br}(F(t))$ of $F(t)$, where $F(t)$ is the field of rational functions in one variable t over F. It is shown in [3] that if the characteristic of F is finite, then Theorem 1 (with n a prime power) is sufficient to determine completely the structure of $\mathrm{Br}(F(t))$ as an abelian group, and its truth is conjectured. Actually we will prove a sharper result than Theorem 1 which will suffice to determine $\mathrm{Br}(F(t))$ for number fields F as well, on the basis of [3].

We first summarize part of the discussion in [3]. If G is an additive abelian group, let G_p denote the p-primary part of G and $G^{(p)}$ the subgroup of elements of G of order p. Define recursively $p^0G = G$, $p^\lambda G = p(p^{\lambda-1}G)$ for a non-limit ordinal λ, and $p^\lambda G = \bigcap_{\mu<\lambda} p^\mu G$ for a limit ordinal λ. Then the Ulm invariants are defined by

$$U_p(\lambda, G) = \dim_{\mathbf{Z}/p\mathbf{Z}}((p^\lambda G)^{(p)}/(p^{\lambda+1}G)^{(p)}).$$

Received May 5, 1979

We have

$$U_p(\lambda, G_1 \oplus G_2) = U_p(\lambda, G_1) + U_p(\lambda, G_2)$$

for all p, λ.

$\mathrm{Br}(F(t))$ is a countable torsion abelian group, whose maximal divisible subgroup $\mathrm{DBr}(F(t))$ is a direct summand isomorphic to the direct sum of countably (and infinitely) many copies of $\mathbf{Q}/\mathbf{Z}$. $\mathrm{RBr}(F(t)) = \mathrm{Br}(F(t))/\mathrm{DBr}(F(t))$ is the direct sum of its p-primary components $\mathrm{RBr}(F(t))_p$, each of which is determined by its Ulm invariants $U_p(\lambda) = U_p(\lambda, \mathrm{RBr}(F(t))_p)$.

If $p = \mathrm{char}(F)$, then $\mathrm{RBr}(F(t))_p = 0$. If $p \neq \mathrm{char}(F)$, then the method of computing the Ulm invariants of $\mathrm{RBr}(F(t))_p$ is based on a split exact sequence due to Auslander and Brumer [2] (see [3, p. 42]):

$$0 \to \mathrm{Br}(F)_p \to \mathrm{Br}(F(t))_p \to \coprod_f (\hat{G}_{E(f)})_p \to 0$$

where f runs through all monic irreducible polynomials over F,

$$E(f) = F[t]/f(t)F[t],$$

G_E is the absolute Galois group $G(\tilde{E}/E)$, where $\tilde{E}$ is the separable closure of $E = E(f)$, and $\hat{G}_E$ is the character group $\mathrm{Hom}(G_E, \mathbf{Q}/\mathbf{Z})$.

In [3] the $U_p(\lambda) = U_p(\lambda, \mathrm{RBr}(F(t))_p)$ are determined for all finite λ (they are zero for $\lambda <$ a cyclotomic constant $r_p(F)$ and $\aleph_0$ for $r_p(F) \leqq \lambda < \omega$ (ω = first infinite ordinal), except when $p = 2$ and $\sqrt{1} \notin F$, when $U_2(0) = \aleph_0$ and the rest are as above), and for all $\lambda \geqq 2\omega$ (all zero). It is also proved in [3] that $U_p(\lambda) \neq 0$ for infinitely many λ, $\omega \leqq \lambda < 2\omega$. Now by the Auslander–Brumer theorem [2], $U_p(\lambda) \neq 0$ if and only if there exists a finite extension E of F such that $U_p(\lambda, \hat{G}_E) \neq 0$. Let $\lambda = \omega + n$, n finite. Then $U_p(\lambda, \hat{G}_E) \neq 0$ if and only if there exists an element σ of order p in $\hat{G}_E$ and an element τ in $\hat{G}_E$ such that

(i) $p^n\tau = \sigma$,

(ii) $\tau = p^r x$ is solvable for x in $\hat{G}_E$

for every positive integer r, and

(iii) if $\tau \in \hat{G}_E$ with $p^{n+1}\tau' = \sigma$, then (ii) does not hold when τ is replaced by τ'.

Thus $U_p(\omega + n - 1, \hat{G}_E) \neq 0$ if and only if there exists a cyclic extension K/E of degree p, and a cyclic extension L/E of degree p^n with $L \supset K$, such that for every $r > 0$, L/E is contained in a cyclic extension L'/E of degree p^{n+r}, but for any cyclic extension M/E of degree p^{n+1} with $M \supset K$, there is an $r > 0$ such that M/E is not contained in a cyclic extension of degree p^{n+r}. Let us refer to L/E as above as *infinitely embeddable*.

THEOREM 2. *Let F be a global field, n a positive integer not divisible by the characteristic of F. Then there exists a finite (solvable) extension E of F, such that, for each prime p dividing n, there is a cyclic extension L/E of degree equal to the exact power of p dividing n, and unramified at all primes of E, but if M/E is any cyclic extension of p-power degree larger than that of L/E, such that $M \cap L \neq E$, then some finite prime of E not dividing p ramifies in M.*

COROLLARY. *Let F be a global field, p a rational prime different from the characteristic of F. Then theUlm invariants $U_p(\omega + m, \mathrm{RBr}(F(t))_p)$ are equal to $\aleph_0$ for all finite m.*

PROOF OF COROLLARY. By the preceding discussion, it suffices to prove that there are infinitely many finite extensions E of F such that $U_p(\omega + m, \hat{G}_E) \neq 0$. But then it suffices to prove the existence of one such E, since we can iterate (F is arbitrary). Let E and L be as in Theorem 2, with $n = p^m$. By [1, p. 106], L/E is infinitely embeddable (if L_Q/E_P is an unramified local extension, every unit of E_P is a norm from L_Q), but if M/E is cyclic of degree p^{m+1} with $M \cap L \neq E$ (so that M contains the subextension K/E of L/E of degree p), then M/E is not infinitely embeddable (if M_Q/E_P is ramified with $P \nmid p$, then not every unit of E_P is a norm from M_Q, hence not every p-power root of unity in E_P is a norm from M_Q). It follows that $U_p(\omega + m - 1, \hat{G}_E) \neq 0$, proving the corollary.

Before proving Theorem 2, we show Theorem 1 follows from it. Again let E be as in Theorem 2, p a prime dividing n, L/E the corresponding extension. Let K/E be the subextension of L/E of degree p, and let p_0 be the characteristic of F. If $p_0 = 0$, then L is contained in the Hilbert class of field H of E, the maximal abelian extension of E unramified at all finite primes. If $p_0 \neq 0$, then first of all, K/E cannot be a constant extension, since the constant extension M/E of degree $p[L:E]$ would violate Theorem 2. It follows that L has the same field of constants as E. If H is a maximal abelian unramified extension of E containing L and having the same field of constants as E, then $G(H/E) \simeq \mathrm{Cl}_E$, the class group of E [1, p. 79]. Of course $G(H/E) \simeq \mathrm{Cl}_E$ in the case $p_0 = 0$ as well [1, p. 74]. Let $[L:E] = p^m$, the p-part of n. Identifying Cl_E with $G(H/E)$, Theorem 2 implies that the character group of Cl_E (which is isomorphic to Cl_E) has an element of order p which is a p^{m-1}-th power but not a p^m-th power (stated multiplicatively). This implies that Cl_E has a cyclic direct summand of order p^m. Since this holds for every p dividing n, Cl_E has a cyclic direct summand of order n, proving Theorem 1.

PROOF OF THEOREM 2. Let $p^{m(p)}$ be the exact power of p dividing n for each $p \mid n$. We may without loss of generality assume that F contains the $p^{m(p)+1}$-th roots of unity, for each $p \mid n$. Let S be a finite set of primes of F containing the prime divisors of n, and sufficiently large so that the S-class number of F is one [7, p. 207]. (The S-class number of F is the order of the group of S-divisors modulo principal S-divisors.) The group of S-units of F (elements which are units outside S) is finitely generated [7, p. 207], so the extension F' of F generated by all n-th roots of S-units of F is a finite abelian extension of F of exponent n. By [6] there exist infinitely many primes of F which split completely in F'. Choose one of them, P, not dividing n. By the approximation theorem [7, p. 8], there exists an element $\pi \in F$ such that $\mathrm{ord}_P(\pi) = 1$ and π is close to 1 at all prime divisors of n in F, sufficiently close so that π is an n-th power in F_Q for every $Q \mid n$. Let $(\ ,\ )$ denote the n-th power norm residue symbol in F_P [1, p. 150].

Since $F_P(\pi^{1/n})/F_P$ is totally ramified, there exists a unit $u \in F_P$ such that (π, u) is a primitive n-th root of unity ζ. By the approximation theorem there exists $\rho \in F$ such that $\mathrm{ord}_P(\rho - u) > 0$, ρ is a unit at all primes where π is not, and ρ is close to 1 at the prime divisors of n, so that ρ is an n-th power in F_Q for every $Q \mid n$. Then since ρ/u is a 1-unit at P, $\rho/u = v^n$ for some $v \in F_P$ (recall $P \nmid n$). Hence

$$(\pi, \rho) = (\pi, uv^n) = (\pi, u) = \zeta.$$

Set $E = F((\pi\rho)^{1/n})$. Now fix $p \mid n$, and let p^m be the exact power of p dividing n. Set $L = E(\pi^{1/p^m})$. By choice of π and ρ, both $F(\pi^{1/n})$ and $F(\rho^{1/n})$ have degree n over F (over F_P in fact). Moreover, their intersection is F, for if not, their intersection would be of the form $F(\pi^{1/d}) = F(\rho^{1/d})$ for some $d \mid n$. By Kummer theory, $\rho = \pi^i a^d$ for some $a \in F$, i prime to d. Then

$$\zeta = (\pi, \rho) = (\pi, \pi^i a^d) = (\pi, \pi)^i (\pi, a^d) = 1 \cdot (\pi, a)^d,$$

a contradiction. Note that $(\pi, \pi) = 1$ since $(\pi, \pi) = (\pi, -\pi)(\pi, -1) = (\pi, -1) = 1$ since -1 is an n-th power in F by hypothesis (F contains the $2n$-th roots of 1). It follows that $[E : F] = n = [E(\pi^{1/n}) : E]$, hence $[L : E] = p^m$.

Now L/E is unramified at all primes not dividing p since $L = E(\pi^{1/p^m}) = E(\rho^{1/p^m})$ and ρ is a unit wherever π is not. The prime divisors of p in F split completely in L, so L/E is unramified at the prime divisors of p. The archimedean primes of F are all complex, so L/E is unramified there as well, hence at all primes.

Now suppose M/E is cyclic of degree p^{m+1} and $M \cap L \neq E$. Then $M = E(a^{1/p^{m+1}})$ for some $a \in E$. Suppose contrarily that every prime of E not dividing p is unramified in M. Let S' be the set of primes of E dividing primes in S. Then every prime of E outside S' is unramified in M. It follows that the principal S'-divisor (a) is a p^{m+1}-th power

$$(a) = A^{p^{m+1}}$$

A an S'-divisor. $M \cap L \neq E$ implies that $E(a^{1/p}) = E(\pi^{1/p})$, hence

$$a = \pi^i b^p$$

for some $b \in E$, i prime to p. Passing to S'-divisors,

$$A^{p^{m+1}} = (a) = (\pi^i b^p)$$

and taking norms into F,

$$N(A)^{p^{m+1}} = (\pi^{ni} N(b)^p),$$

an equation in S-divisors. By choice of S, $N(A)$ is a principal S-divisor (f), $f \in F$, so

$$(f)^{p^{m+1}} = (\pi^{ni} N(b)^p) = (\pi^{ni/p} N(b))^p,$$

$$(f)^{p^m} = (\pi^{ni/p} N(b)).$$

It follows that

$$f^{p^m} \alpha = \pi^{ni/p} N(b)$$

for some S-unit α of F. But α is an n-th power β_1^n in F_P, hence a p^m-th power β^{p^m} in F_P. Then

$$(f\beta)^{p^m} = \pi^{ni/p} N(b)$$

in F_P, where N can be interpreted as the local norm of E/F at P, since the local degree of E/F at P is n. We then have

$$\begin{aligned}
(f\beta, \pi\rho)^{p^m} &= ((f\beta)^{p^m}, \pi\rho) \\
&= (\pi^{ni/p} N(b), \pi\rho) \\
&= (\pi^{ni/p}, \pi\rho)(N(b), \pi\rho) \\
&= (\pi^{ni/p}, \pi\rho) \\
&= (\pi, \pi)^{ni/p} (\pi, \rho)^{ni/p}
\end{aligned}$$

$$= (\pi, \rho)^{ni/p}$$

$$= \zeta^{ni/p}.$$

The first term in this chain of equations is a root of unity of order prime to p, while the last has order p, a contradiction. Thus some prime of E not dividing p ramifies in M. q.e.d.

REMARKS. (1) It follows from the proof of Theorem 2 that at the end of the statement of Theorem 2, the phrase "not dividing p" can be replaced by "not dividing any prime in S, where S is any finite set of primes of F given in advance."

(2) Yahagi [8] has proved that if p is a rational prime and F is a number field whose class number is prime to p, then for any finite abelian p-group G, there exists a cyclic extension E of F whose p-class group is isomorphic to G.

NOTE. Fein and Schacher [5] have recently proved that the Ulm length of $\mathrm{RBr}(F(t_1,\cdots,t_n))_p$ is 2ω (i.e. $U_p(\lambda, \mathrm{RBr}(F(t_1,\cdots,t_n))) = 0$ for $\lambda \geqq 2\omega$), where $p \neq \mathrm{char}(F)$, and $t_1,\cdots,t_n$ are algebraically independent over F. This result, together with [4] and the corollary to Theorem 2, determines the structure of $\mathrm{Br}(F(t_1,\cdots,t_n))_p$ completely, except for the case $n > 1$, $p = 2$, $\varepsilon(4) \notin F$, where $\varepsilon(m)$ denotes a primitive m-th root of unity, in which case the finite set of Ulm invariants

$$U_2(m) = U_2(m, \mathrm{RBr}(F(t_1,\cdots,t_n))), \qquad 1 \leqq m \leqq r-2,$$

with r maximal such that $\varepsilon(2^r) \in F(\varepsilon(4))$, is missing [4, theorem 3]. We take this opportunity to prove that these Ulm invariants are all zero.

THEOREM 3. *Let F be a global field of characteristic $\neq 2$, $\varepsilon(4) \notin F$, r maximal such that $\varepsilon(2^r) \in F(\varepsilon(4))$. Let $t_1,\cdots,t_n$ be algebraically independent over F. Then the Ulm invariants*

$$U_2(m, \mathrm{RBr}(F(t_1,\cdots,t_n))) = 0$$

for $1 \leqq m \leqq r-2$.

PROOF. By induction on n. If $n = 1$, this is already known [3]. Assume the theorem is true for n. By the Auslander–Brumer sequence above, it suffices to prove that for every finite extension E of $F(t_1,\cdots,t_n)$,

$$U_2(m, \hat{G}_E) = 0 \qquad \text{for } 1 \leqq m \leqq r-2.$$

Let E be such an extension. If $\varepsilon(4) \in E$, then $\varepsilon(2^r) \in E$, in which case

$U_2(m, \hat{G}_E) = 0$ for $0 \leqq m \leqq r-2$ [3, 4]. We therefore assume $\varepsilon(4) \notin E$. We assume also that $r \geqq 3$; otherwise there is nothing to prove.

In order to prove the theorem, it suffices to prove that if $x \in \hat{G}_E$ with $2x \neq 0$ and $4x = 0$, then $2x = 2^{r-1}y$ for some $y \in \hat{G}_E$, or equivalently, if K/E is a quadratic extension which is contained in a cyclic extension L/E of degree 4, then K/E is contained in a cyclic extension M/E of degree 2^r.

Case 1. $K = E(\varepsilon(4))$

$\hat{G}_E$ can be identified with the first cohomology group $H^1(G_E, \mathbf{Q}/\mathbf{Z})$ with G_E acting trivially on $\mathbf{Q}/\mathbf{Z}$. We have the cohomology maps:

res: $H^1(G_E, \mathbf{Q}/\mathbf{Z}) \to H^1(G_K, \mathbf{Q}/\mathbf{Z})$ and cor: $H^1(G_K, \mathbf{Q}/\mathbf{Z}) \to H^1(G_E, \mathbf{Q}/\mathbf{Z})$,

satisfying the equation

$$\text{cor.\,res.} = [K : E] = 2.$$

The assumption $K = E(\varepsilon(4))$ means that $\operatorname{res} 2x = 0$. Then $2 \operatorname{res} x = 0$, $\operatorname{res} x \neq 0$ implies that $\operatorname{res} x = 2^{r-1}y$, $y \in \hat{G}_K$, since $\varepsilon(2^r) \in K$. Then $2x = \operatorname{cor}.\operatorname{res} x = 2^{r-1} \operatorname{cor} y$. q.e.d.

Case 2. $K \neq E(\varepsilon(4))$

Let $E' = E(\varepsilon(4))$. Let $E'(2^r)$ be the maximal abelian extension of E' of exponent 2^r. By Kummer theory, $G(E'(2^r)/E')$ is $G(E'/E)$—isomorphic to $\operatorname{Hom}(E'^*/E'^{*2^r}, \mu(2^r))$, where $\mu(2^r)$ denotes the group of 2^r-th roots of unity in E'. Here $G(E'/E)$ acts on $G(E'(2^r)/E')$ by conjugation in $G(E'(2^r)/E)$ and on $\operatorname{Hom}(E'^*/E'^{*2^r}, \mu(2^r))$ by the rule

$$f^\sigma(x) = f(x^{\sigma^{-1}})^\sigma, \qquad x \in E'^*/E'^{*2^r}, \qquad f \in \operatorname{Hom}(E'^*/E'^{*2^r}, \mu(2^r)).$$

Let $G(E'/E) = \{1, \sigma\}$, and suppose $\varepsilon(2^r)^\sigma = \varepsilon(2^r)^j$. Let x be a nonsquare in E'. Then $E'(x^{2^{-r}})$ is cyclic of degree 2^r over E'. By the preceding remark, $E'(x^{2^{-r}})$ is abelian over E if and only if $x^{\sigma-j} \in E'^{*2^r}$.

Let $a \in E$, $\sqrt{a} \notin E'$. If $E(\sqrt{a})$ is embeddable into a cyclic extension M/E of degree 2^r, then $E'(\sqrt{a})$ is embeddable into the cyclic extension ME'/E' of degree 2^r, and necessarily, $ME' = E'((a\alpha^2)^{1/2^r})$ for some $\alpha \in E'$. Furthermore, ME'/E is abelian, hence by the preceding remark (with $x = a\alpha^2$), we have

$$(a\alpha^2)^{\sigma-j} \in E'^{*2^r}.$$

Conversely, if the latter condition is satisfied for some $\alpha \in E'^*$, then as we have seen, $E'((a\alpha^2)^{1/2^r})/E$ is abelian, contains K, and in fact contains a cyclic extension M/E of degree 2^r, since its Galois group is the direct product of a cyclic group of order 2 and a cyclic group of order 2^r.

Let $K = E(\sqrt{a})$, $a \in E$. The assumption that K/E is embeddable into a cyclic extension L/E of degree 4 implies that

$$(a\alpha^2)^{\sigma-j} \in E'^{*4}$$

for some $\alpha \in E'^*$. We show first that

$$(a\beta^2)^{\sigma-j} \in E'^{*2^r}$$

for some $\beta \in E'^*$, which implies that $M' = E'((a\beta^2)^{1/2^r})$ is abelian over E and contains a subfield M which is cyclic of degree 2^r over E.

Now since $\varepsilon(4)^\sigma = \varepsilon(4)^{-1}$, we have

$$(a\alpha^2)^{\sigma-j} = (a\alpha^2)^{\sigma+1} = N(a\alpha^2) = a^2N(\alpha)^2 \in E'^{*4}$$

where $N = N_{E'/E}$. Thus

$$\pm aN(\alpha) \in E'^{*2}$$

and since $-1 \in E'^{*2}$, we have

$$aN(\alpha) \in E'^{*2}.$$

But $aN(\alpha) \in E$, hence

$$E((aN(\alpha))^{1/2}) \subseteq E',$$

so

$$aN(\alpha) = \pm b^2$$

for some $b \in E$, hence

$$aN(\alpha b^{-1}) = \pm 1.$$

Setting $\beta = \alpha b^{-1}$, we have

$$aN(\beta) = \pm 1,$$

$$1 = a^2N(\beta^2) = a^2\beta^{2(\sigma+1)}$$

$$= (a\beta^2)^{\sigma+1} = (a\beta^2)^{\sigma-j+j+1} \in E'^{*2^r}.$$

Since σ has order 2, $j \equiv -1$ or $-1+2^{r-1} \bmod 2^r$. If $j \equiv -1$, then $(a\beta^2)^{j+1} \in E'^{*2^r}$ and we are finished. If $j \equiv -1+2^{r-1}$, let $\gamma = a^{2^{r-3}}\beta$. Then

$$\begin{aligned}(a\gamma^2)^{\sigma-j} &= (a\gamma^2)^{(\sigma+1)-(j+1)}\\ &= (a^{1+2^{r-2}}\beta^2)^{\sigma+1}(a\gamma^2)^{-(j+1)}\\ &= a^{2^{r-1}-(j+1)}\gamma^{-2(j+1)} \in E'^{*2^r},\end{aligned}$$

as required.

We show now that K/E is embeddable into a cyclic extension M_1/E of degree 2^r. We observe first that the cyclic subextension M/E of degree 2^r of M'/E, whose existence we have just established, does not contain E', since M'/E' is cyclic of degree 2^r. Hence M contains either $E(\sqrt{a}) = K$ or $E(\sqrt{-a})$. We must consider two cases.

Case 2.1. E'/E is embeddable into a cyclic extension of E of degree 4. By Case 1 above, E'/E is then embeddable into a cyclic extension M_2/E of degree 2^r. Then $M \cap M_2 = E$, and in this case both $E(\sqrt{a})$ and $E(\sqrt{-a})$ are embeddable into cyclic extensions of E of degree 2^r, contained in MM_2.

Case 2.2. E'/E is not embeddable into a cyclic extension of E of degree 4. Then the same is true for $E(\sqrt{-a})/E$, for otherwise both $E(\sqrt{a})$ and $E(\sqrt{-a})$ would be embeddable into cyclic extensions of degree 4 of E, hence so would E', contrary to hypothesis. It follows that m does not contain $E(\sqrt{-a})$, hence M contains $K = E(\sqrt{a})$. q.e.d.

References

1. E. Artin and J. Tate, *Class Field Theory*, W. A. Benjamin, Inc., New York–Amsterdam, 1968.
2. M. Auslander and A. Brumer, *Brauer groups of discrete valuation rings*, Indag. Math. **30** (1968), 286–296.
3. B. Fein and M. Schacher, *Ulm invariants of the Brauer group of a field*, Math. Z. **154** (1977), 41–50.
4. B. Fein and M. Schacher, *Ulm invariants of the Brauer group of a field, II*, Math. Z. **163** (1978), 1–3.
5. B. Fein and M. Schacher, *Brauer groups and character groups of function fields*, to appear.
6. M. Nagata, T. Nakayama and T. Tuzuku, *On an existence lemma in valuation theory*, Nagoya Math. J. **6** (1953), 59–62.
7. E. Weiss, *Algebraic Number Theory*, McGraw-Hill, 1963.
8. O. Yahagi, *Construction of number fields with prescribed l-class groups*, Tokyo J. Math. **1** (1978), 275–283.

Department of Mathematics
Technion — Israel Institute of Technology
Haifa, Israel