TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 326, Number 1, July 1991

CYCLIC GALOIS EXTENSIONS AND NORMAL BASES

C. GREITHER

ABSTRACT. A Kummer theory is presented which does not need roots of unity in the ground ring. For R commutative with $p^{-1} \in R$ we study the group of cyclic Galois extensions of fixed degree p^n in detail. Our theory is well suited for dealing with cyclic p^n-extensions of a number field K which are unramified outside p. We then consider the group $\mathrm{Gal}(\mathcal{O}_K[p^{-1}], C_{p^n})$ of all such extensions, and its subgroup $\mathrm{NB}(\mathcal{O}_K[p^{-1}], C_{p^n})$ of extensions with integral normal basis outside p. For the size of the latter we get a simple asymptotic formula $(n \to \infty)$, and the discrepancy between the two groups is in some way measured by the defect δ in Leopoldt's conjecture.

INTRODUCTION

This work begins with a general study of Galois extensions of a commutative ring R with finite abelian Galois group G (Part I). The results are applicable in a number-theoretical setting (Part II) and give theorems concerning the existence of p'-integral normal bases in C_{p^n}-extensions and $\mathbb{Z}_p$-extensions of an arbitrary number field K. (Here p is an odd prime, C_{p^n} is the cyclic group of order p^n, and "p'-integral" means "integral outside places over p".)

Let us start by describing the general situation. Let R be a commutative ring with 1 and G a finite abelian group. We study the finite abelian group $\mathrm{Gal}(R, G)$ which consists of the (isomorphism classes of) G-Galois ring extensions of R. (Such extensions were defined by Chase, Harrison, and Rosenberg [4]. The group structure on $\mathrm{Gal}(R, G)$ is due to Harrison [13] and goes back to Hasse [14] for the case $R = K$ a field. In that case, the basic idea is to admit some nonfields (Galois algebras) in order to form $\mathrm{Gal}(K, G)$.)

The principal link between general Galois theory of rings and number theory is the study of ramification. Let L be a G-Galois field extension of the number field K, Σ a set of finite places of K, and R the ring of Σ-integers in K. Then the integral closure S of R in L is a G-Galois extension of R if and only if L/K is unramified at all finite places outside Σ (see [4, Remark 1.5d]). In particular, $\mathcal{O}_L$ is Galois over $\mathcal{O}_K$ iff L/K is unramified except at infinity.

Received by the editors June 13, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R33, 11R27, 13B05.
Key words and phrases. Galois extensions of rings, descent, integral normal bases, Leopoldt's conjecture.

0002-9947/91 $1.00 + $.25 per page

It is well known [13] that the functor $\mathrm{Gal}(R, G)$ commutes with finite products in the second variable, so we will henceforth restrict our attention to cyclic groups G of prime power order, as is usual. There are several results in the literature on the structure of $\mathrm{Gal}(R, G)$ and the related group $\mathrm{NB}(R, G)$ which consists of those G-Galois extensions of R which have a normal basis over R. We refer to [10, 11, 12, 17], and in particular to [18] where it is shown that for $p^{-1} \in R$ and p odd, $\mathrm{NB}(R, C_{p^n})$ is isomorphic to a certain subquotient of $R[\widehat{C_{p^n}}]^*$.

Part I of this paper gives a structure theory of C_{p^n}-extensions of an arbitrary connected ring R in which the odd prime p is invertible. As before, let C_{p^n} be the cyclic group of order p^n with generator σ. The method is "Kummer theory plus Galois descent". First recall Kummer theory for commutative rings (Borevich [2]): If G is cyclic of order m and R contains both m^{-1} and a root ζ_m of the mth cyclotomic polynomial, then there is a short exact sequence (which depends on the choice of a generator σ for G):

$$1 \to R^*/R^{*m} \xrightarrow{i} \mathrm{Gal}(R, G) \xrightarrow{\pi} m\text{-torsion}(\mathrm{Pic}(R)) \to 1 .$$

Now we let $m = p^n$ and define S_n as "the" connected Galois extension of R which is obtained by adjoining the primitive p^nth root of unity ζ_{p^n} (this will be made precise). The Galois group G_n of S_n over R comes with an embedding $t\colon G_n \to (\mathbb{Z}/p^n\mathbb{Z})^*$ (where $t(\gamma) = g + p^n\mathbb{Z}$ if $\gamma(\zeta) = \zeta^g$). Starting from the obvious G_n-actions, one can define certain twisted actions of G_n on S_n^* modulo p^nth powers, and on the p^n-torsion of $\mathrm{Pic}(S_n)$. (In number theory, this is precisely the Tate twist $\cdots(-1)$.) We obtain in §2 (denoting fixed elements under the twisted action by an exponent $\cdots^{tG_n}$):

(1) a canonical homomorphism $j_0\colon \mathrm{NB}(R, C_{p^n}) \to (S_n^*/S_n^{*p^n})^{tG_n}$ with $\mathrm{Ker}(j_0)$ and $\mathrm{Coker}(j_0)$ finite cyclic of the same order $\gcd(p^n, |G_n|)$.

The existence of j_0 implies that $\mathrm{NB}(R, C_{p^n})$ has the same cardinality as the group $(S_n^*/S_n^{*p^n})^{tG_n}$, so one is led to ask whether these two groups are isomorphic. The answer is yes (see [8]), but we do not need this here since we will only deal with the cardinalities in Part II.

Second, we obtain

(2) a canonical isomorphism

$$\mathrm{Gal}(R, C_{p^n})/\mathrm{NB}(R, C_{p^n}) \to (p^n\text{-torsion}(\mathrm{Pic}(S_n)))^{tG_n} .$$

Two remarks about the proofs: (i) Property (1) is first proved with NB replaced by an auxiliary group Gal_0, and then we show $\mathrm{Gal}_0 = \mathrm{NB}$ in §3. (ii) Some of the new proofs in Part I would simplify if one were only interested in rings R which are Σ-integers in a number field K (see above).

In Part II we demonstrate that one can actually calculate the cardinality of $\mathrm{NB}(R, C_{p^n})$ for R an appropriate subring of a number field, using the results of the first part. The starting point is the following: If L/K is a G-Galois

extension of number fields, then $\mathcal{O}_L[p^{-1}]$ is G-Galois over $\mathcal{O}_K[p^{-1}]$ exactly if L/K is unramified at all finite places not dividing p (see above). This, combined with the fact that any $\mathbb{Z}_p$-extension of K is unramified outside p, suggests we choose $R = \mathcal{O}_K[p^{-1}]$ and study $\mathrm{Gal}(R, C_{p^n})$ for all n. We show in §1 that the order of $\mathrm{Gal}(R, C_{p^n})$ grows like a constant times $p^{n \cdot c(K)}$, where $c(K)$ is the number of independent $\mathbb{Z}_p$-extensions of K. One of our main results (§3) is: If $p \neq 2$, then the order of $\mathrm{NB}(R, C_{p^n})$ grows like a constant times $p^{n \cdot (r_2+1)}$, where r_2 is the number of complex places of K as usual. This sheds a new light on Leopoldt's conjecture which predicts that $c(K) = r_2 + 1$. To wit: Leopoldt's conjecture holds for K and $p \neq 2$ if and only if $|\mathrm{Gal}(R, C_{p^n})/\mathrm{NB}(R, C_{p^n})|$ is bounded. Next, we consider $\mathbb{Z}_p$-extensions of R and show (§4) that the group $\mathrm{NB}(R, \mathbb{Z}_p)$ is isomorphic to $\mathbb{Z}_p^{r_2+1}$. This has been previously proved by I. Kersten and J. Michaliček [19, 20] for K totally real or a CM field. At the end of §4, we make some remarks about the index of $\mathrm{NB}(R, \mathbb{Z}_p)$ in $\mathrm{Gal}(R, \mathbb{Z}_p)$.

The transition from C_{p^n}-extensions to $\mathbb{Z}_p$-extensions, natural as it is, presents technical problems. We need Iwasawa's results on the structure of p-class groups in (cyclotomic) $\mathbb{Z}_p$-extensions. In order to make the presentation in §4 tauter, we postpone some "complicated trivialities" about projective systems, and another calculation we need, to a final section, §5.

Acknowledgment. I am grateful to I. Kersten who showed me (among other improvements) a considerable simplification of the proof of Theorem II4.6. I also should like to thank the referee for his useful remarks on the presentation.

A word on *terminology*. All rings and algebras will be commutative, with unit element. $\mathrm{Gal}(R, G)$ denotes always the set of isomorphism classes of Galois extensions of the ring R with the finite group G in the sense of [4], which is our standard reference. $\mathrm{NB}(R, G)$ denotes the subset of isomorphism classes of extensions which possess a normal basis. The letter p denotes a prime number, and it will always be said whether $p = 2$ is excluded or not.

This paper is a slightly shortened version of the first two chapters of the author's Habilitationsschrift [8]. Most of the results were announced in [9].

PART I. General Theory of C_{p^n}-Extensions

1. Twisted actions

This section contains definitions and auxiliary results, used in the sequel.

Let p be an odd prime, $n \in \mathbb{N}$, and G a finite cyclic group with generator γ and a fixed embedding

$$t: G \to (\mathbb{Z}/p^n\mathbb{Z})^*.$$

For any G-module M with $p^n \cdot M = 0$ one can define a twisted action of G on M by

$$\delta * x = t(\delta)^{-1} \cdot \delta(x), \qquad x \in M,\ \delta \in G.$$

We call this the t-action. In [6] it is called *Stickelberger action.* (If G is a quotient group of the absolute Galois group of $\mathbb{Q}$ such that t is the cyclotomic character, $(M, *)$ is also denoted $M(-1)$ and called a *Tate twist.*)

Motivating example. G is the Galois group $G(K(\zeta_{p^n})/K)$, where K is a field, and t is defined by $\delta(\zeta_{p^n}) = (\zeta_{p^n})^{t(\delta)}$ for all $\delta \in G$. M is defined as $K(\zeta_{p^n})^*/K(\zeta_{p^n})^{*p^n}$. (The importance of this example will become clear in §2, when Kummer theory is introduced.)

Definition. The ith cohomology group of M with the t-action of G is denoted $H_t^i(G, M)$.

The group of fixed elements of M under the t-action of G is denoted M^{tG}.

Lemma 1.1. (a) *If $n \geq 2$ and $g \in \mathbb{Z}$ is such that $\bar{g} \in (\mathbb{Z}/p^n\mathbb{Z})^*$ has order m with $p|m$, then $\bar{g} \in ((\mathbb{Z}/p^{n+1}\mathbb{Z}))^*$ has order pm. (For $p = 2$, the same holds if $g \equiv 1 \bmod 4$.)*

(b) *If $n \geq 2$ and $g \in \mathbb{Z}$ is such that $\bar{g} \in (\mathbb{Z}/p^n\mathbb{Z})^*$ has order m with $p|m$, then p does not divide $(g^m - 1)/p^n$. (For $p = 2$, the same holds if $g \equiv 1 \bmod 4$.)*

Proof. (a) This is [6, Lemma 2.1]. For the reader's convenience, we indicate the argument: Let H be the subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^*$ generated by the residue class of g, and H' be the subgroup of $((\mathbb{Z}/p^{n+1}\mathbb{Z}))^*$ generated by the residue class of g. Then one has a group epimorphism $f: H' \to H$, and we have to show $\mathrm{Ker}(f)$ has p elements. We have $\mathrm{Ker}(f) = h' \cap W$, where W is the p-element subgroup of $((\mathbb{Z}/p^{n+1}\mathbb{Z}))^*$ generated by $\overline{1+p^n}$. Since $((\mathbb{Z}/p^{n+1}\mathbb{Z}))^*$ is cyclic and p divides $|H'|$, we must have $W \subset H'$, hence $\mathrm{Ker}(f) = w$. An obvious modification gives the statement for the case $p = 2$.

(b) We have $g^m = 1 + up^n$ with $u \in \mathbb{Z}$. By (a), the power g^m is incongruent to 1 modulo p^{n+1}, i.e., p does not divide u. □

We define for every abelian group M:

$$T_n(M) = \{x \in M | p^n x = 0\}, \qquad T^n(M) = M/p^n M.$$

Proposition 1.2. *Suppose $0 \to M_1 \to M \to M_2 \to 0$ is an exact sequence of G-modules and M_2 has no $\mathbb{Z}$-torsion. Then the sequence*

$$0 \to T^n(M_1)^{tG} \to T^n(M)^{tG} \to T^n(M_2)^{tG} \to 0$$

is again exact. (Note that in general the twisted action of G is defined only on $M/p^nM = T^n(M)$ and not on M itself.) (For $p = 2$, the proposition also holds if $tG \subset \{a + 2^n\mathbb{Z} | a \equiv 1 \bmod 4\}$.)

Proof. The sequence remains exact under application of T^n since

$$\mathrm{Tor}_{\mathbb{Z}}(\mathbb{Z}/p^n\mathbb{Z}, M_2)$$

is zero. We only have to show that the induced map

$$\pi: T^n(M)^{tG} \to T^n(M_2)^{tG}$$

is onto. Recall that γ is a generator of G. Let $x \in M_2$ and $t(\gamma) = g + p^n\mathbb{Z}$. Then $x + p^nM_2 \in T^n(M_2)^{tG}$ exactly if $gx \equiv \gamma(x) \bmod p^nM_2$, exactly if $(g-\gamma)\cdot x \in p^nM_2$. ($M_2$ is a module over the group ring $\mathbb{Z}G$ in the obvious way.) Now let $m = |G| =$ order of $g + p^n\mathbb{Z}$ in $(\mathbb{Z}/p^n\mathbb{Z})^*$, and let $u = (g^m - 1)/p^n$.

First Case: $p|m$. Then u is prime to p by 1.1(b). In $\mathbb{Z}G$ we have

$$u \cdot p^n = g^m - 1 = (g - \gamma) \cdot \left(\sum_{j=0}^{m-1} g^j \cdot \gamma^{m-1-j} \right).$$

Let $\rho = \sum_{j=0}^{m-1} g^j \cdot \gamma^{m-1-j} \in \mathbb{Z}G$. Then we may continue: $(g - \gamma) \cdot x \in p^nM_2$ implies $(g - \gamma) \cdot u \cdot x \in up^nM_2$. This in turn implies $(g - \gamma)ux = (g - \gamma) \cdot \rho \cdot y$ for some $y \in M_2$. Now multiplication with up^n is injective on M_2. Hence multiplication with $g - \gamma$ is also injective, and our last equation yields $u \cdot x \in \rho M_2$. Hence $u \cdot x$ can be lifted to $z \in \rho M$, and since $(g - \gamma) \cdot \rho \cdot M = u \cdot p^nM \subset p^nM$, the residue class of z is in $T^n(M)^{tG}$. So we have found a preimage of $u \cdot x + p^nM_2$, and we are done since multiplication with u is bijective on $T^n(M_2)$.

Second case: m is prime to p. Then the functor $(-)^{tG}$ is exact on p-primary G-modules, since $H_t^1(G, M_1)$ is zero for every p-primary G-module M_1. (Reason: $H_t^1(G, M_1)$ is simultaneously m-torsion and p-primary, hence zero.) Therefore 1.2 holds also in this case. □

2. Kummer theory and descent

In this section, p denotes an *odd* prime unless otherwise stated. Let C_{p^n} be the cyclic group of order p^n with generator σ.

We start by recalling the main result of Kummer theory [2]: If S is a ring which contains p^{-1} and a root ζ of the p^nth cyclotomic polynomial Φ_{p^n}, then there is an exact sequence (depending on the choice of ζ and of a generator σ of C_{p^n}):

$$\text{(K)} \qquad 1 \to T^n(S^*) \xrightarrow{i} \mathrm{Gal}(S, C_{p^n}) \xrightarrow{\pi} T_n(\mathrm{Pic}(S)) \to 0.$$

(Recall the notation of §1: $T^n(S^*) = S^*/S^{*p^n}$ and $T^n(\mathrm{Pic}(S))$ is the p^n-torsion in $\mathrm{Pic}(S)$.) We have (square brackets denote isomorphism classes)

$$i(x \cdot S^{*p^n}) = [(S[T]/(T^{p^n} - x), \sigma(\overline{T}) = \zeta \cdot \overline{T})],$$
$$\pi([A]) = [\{y \in A | \sigma(y) = \zeta \cdot y\}], \quad \text{for } A \text{ a } C_{p^n}\text{-extension of } S.$$

Now suppose that R is a connected ring with $p^{-1} \in R$. Since the discriminant of Φ_{p^n} is plus or minus a power of p, by [16, 1.1, 2.2] there exists for every $n \in \mathbb{N}$ a connected over-ring $S_n \supset R$ which is Galois over R and contains a root $\zeta = \zeta_{p^n}$ of Φ_{p^n}. By [16, 2.5, 2.6] we may choose S_n such that it is

generated by ζ. In this case, S_n is G_n-Galois over R where G_n is an abelian group, which comes with a natural embedding $t\colon G_n \to (\mathbb{Z}/p^n\mathbb{Z})^*$, $\delta(\zeta) = \zeta^{t(\delta)}$. Let γ_n ($= \gamma$ for short) be a fixed generator of G_n (such exists, since $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic as $p \neq 2$), and pick $g \in \mathbb{Z}$ such that

$$g + p^n\mathbb{Z} = t(\gamma).$$

Note that g is a primitive root modulo p^n if and only if $|G_n| = \varphi(p^n)$.

We have certain *canonical operations*: The group G_n operates on $\mathrm{Gal}(S_n, C_{p^n})$ via the first argument, i.e.: For $\delta \in G_n$ and $[A] \in \mathrm{Gal}(S_n, C_{p^n})$, let $\delta[A] = [{}_\delta A]$, defining ${}_\delta A$ to be equal to A as a ring and C_{p^n}-set, but declaring that s times $a \in {}_\delta A$ is equal to $\delta^{-1}(s)\cdot a$ for $s \in S_n$. Similarly, G_n operates on $\mathrm{Pic}(S_n)$ by $\delta[P] = [{}_\delta P]$. Finally, G_n operates canonically (as a Galois group) on S_n^*, hence on $T^n(S_n^*)$.

Lemma 2.1. *With the canonical action of G_n on $\mathrm{Gal}(S_n, C_{p^n})$, and with the t-action on the outer terms $T^n(S_n^*)$ and $T_n(\mathrm{Pic}(S_n))$, the Kummer sequence* (K) *is G_n-equivariant. In number-theoretic terminology: We have an exact G_n-sequence*

$$1 \to T^n(S_n^*)(-1) \to \mathrm{Gal}(S_n, C_{p^n}) \to T_n(\mathrm{Pic}(S_n))(-1) \to 1.$$

Proof. Let $q = p^n$ and $x \in S_n^*$. Then $i(x \cdot S_n^{*p^n}) = [A_x]$, where A_x is defined as $(S_n[T]/(T^q - x), \sigma(\overline{T}) = \zeta \cdot \overline{T})$. By definition,

$${}_\gamma(A_x) = ({}_\gamma(S_n[T]/(T^q - x)),\ \sigma(\overline{T}) = \zeta \cdot \overline{T}).$$

Letting $\#$ denote the scalar multiplication of ${}_\gamma(A_x)$, we obtain

$$\begin{aligned}
{}_\gamma(A_x) &\cong ({}_\gamma(S_n[T]/(T^q - x)),\ \sigma(T) = \zeta^g \# T) && \text{since } \gamma^{-1}(\zeta^g) = \zeta \\
&\cong ({}_\gamma(S_n[Z]/(Z^q - x^r)),\ \sigma(Z) = \zeta \# Z) && \text{setting } Z = T^r \text{ with} \\
& && g \cdot r \equiv 1 \bmod p^n \\
&\cong ((S_n[Z']/(Z'^q - \gamma(x^r))),\ \sigma(Z') = \zeta \cdot Z') && \text{via } \gamma\colon S_n \to S_n \text{ and } Z \mapsto Z' \\
&\cong A_{\gamma(x^r)}.
\end{aligned}$$

Therefore $\gamma(i(x)) = i(\gamma * x)$, hence i is a G_n-homomorphism. The equivariance of π is proved similarly: We evaluate $\pi([{}_\gamma A]) = [\{y \in {}_\gamma A | \sigma(y) = \zeta \# y\}] = [\{y \in A | \sigma(y) = \zeta^r y\}]$. From Kummer theory one knows that

$$\{y \in A | \sigma(y) = \zeta^s \cdot y\} \cong \{y \in A | \sigma(y) = \zeta \cdot y\}^{\otimes^s} \quad \text{canonically for all } s \in \mathbb{N},$$

hence $\{y \in {}_\gamma A | \sigma(y) = \zeta \# y\} \cong \{y \in A | \sigma(y) = \zeta \cdot y\}^{\otimes^r}$. This is even an S_n-isomorphism if we let S_n operate via γ^{-1} on the right-hand side, too. We therefore obtain

$$\{y \in {}_\gamma A | \sigma(y) = \zeta \# y\} \cong {}_\gamma\{y \in A | \sigma(y) = \zeta \cdot y\}^{\otimes^r},$$

which shows that $\pi(\gamma[A]) = \pi([{}_\gamma A]) = \gamma_* \pi([A])$. □

Next, we consider the canonical map

$$j\colon \mathrm{Gal}(R, C_{p^n}) \to \mathrm{Gal}(S_n, C_{p^n}),$$
$$j([A]) = [S_n \otimes_R A].$$

From now on, we shall abuse notation and write A for $[A]$, etc.

Lemma 2.2. *The map j is a group homomorphism and* $\mathrm{Im}(j)$ *is contained in the subgroup* $\mathrm{Gal}(S_n, C_{p^n})^{G_n}$ *of fixed elements under* G_n.

Proof. The first statement is well known. Let $A \in \mathrm{Gal}(R, C_{p^n})$. Then the map $\delta \otimes \mathrm{id}_A\colon {}_\delta(S_n \otimes_R A) \to S_n \otimes_R A$ is an S_n-isomorphism for all $\delta \in G_n$. Hence $j(A)$ is fixed under G_n. □

The Kummer sequence (K) gives also a sequence whose middle term is $\mathrm{Gal}(R, C_{p^n})$. More precisely, let

$$\mathrm{Gal}_0(R, C_{p^n}) = j^{-1}(\mathrm{Im}(i)), \qquad j_0 = j|\mathrm{Gal}_0(R, C_{p^n}),$$
$$P(R, C_{p^n}) = \mathrm{Gal}(R, C_{p^n})/\mathrm{Gal}_0(R, C_{p^n}).$$

Then we have a diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & \mathrm{Ker}(j_0) & = & \mathrm{Ker}(j) & & & & \\
 & & \cap & & \cap & & & & \\
1 & \to & \mathrm{Gal}_0(R, C_{p^n}) & \to & \mathrm{Gal}(R, C_{p^n}) & \to & P(R, C_{p^n}) & \to & 1 \\
 & & {\scriptstyle j_0}\downarrow & & {\scriptstyle j}\downarrow & & \downarrow & & \\
1 & \to & T^n(S_n^*)^{tG_n} & \to & \mathrm{Gal}(S_n, C_{p^n})^{G_n} & \to & T_n(\mathrm{Pic}(S_n))^{tG_n} & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \mathrm{Coker}(j_0) & \subset & \mathrm{Coker}(j) & & & &
\end{array}$$

We shall determine kernel and cokernel of the homomorphisms j and j_0. The results are:

Theorem 2.3. *Let R and S_n be as above. In particular, let R be connected. Then* $\mathrm{Ker}(j)$ *and* $\mathrm{Coker}(j)$ *are both cyclic of order* $\gcd(p^n, |G_n|)$.

Theorem 2.4. *The same assertion as in Theorem* 2.3 *holds for j_0 instead of j. Hence* $\mathrm{Coker}(j_0) \cong \mathrm{Coker}(j)$ *canonically (see diagram). Moreover,* $\mathrm{Coker}(j_0)$ *is canonically isomorphic to a quotient of* $\mu_{p^n}(S_n) = \{s \in S_n | s^{p^n} = 1\}$.

Remarks. (a) For R a field, $p \neq \mathrm{char}(R)$, the assertion about $\mathrm{Coker}(j_0)$ was proved by Childs in [6].

(b) For $n = 1$ the theorems say that j and j_0 are isomorphisms (note $\gcd(p, p-1) = 1$).

Both Theorems 2.3 and 2.4 can be proved in two different ways: by a cohomological argument, and by explicit descent theory. Either method has advantages (and some drawbacks), and we decided to present both: the former for 2.3 and the latter for 2.4, since we need explicit descent anyway in §3, while the cohomological argument is elegant and straightforward (given the existence of separable closures which is, for general rings, a theorem of Janusz [16]).

Proof of Theorem 2.3. Let Ω be a separable closure of R, and Γ be the (profinite) Galois group of Ω over R. By [12, Theorem 4 and remark "This is true..." on p. 10], there is a natural isomorphism $\varphi = \varphi_{R,G}$: $\mathrm{Gal}(R, G) \cong \mathrm{Hom}(\Gamma, G)$ for every abelian group G (all homomorphisms and cochains on Γ are supposed to be continuous, of course). For the reader's convenience we recall the construction of φ, or rather of φ^{-1} since this is easier: For any $f: \Gamma \to G$, one lets $\varphi^{-1}(f) = \mathrm{Gal}(R, f)(\Omega)$. (Since Ω is a Γ-extension only in the profinite sense, one might replace Ω by $\Omega^{\mathrm{Ker}(f)}$ and let $\varphi^{-1}(f) = \mathrm{Gal}(R, f)(\Omega^{\mathrm{Ker}(f)})$.) In particular, if f is onto, $\varphi^{-1}(f)$ is just $\Omega^{\mathrm{Ker}(f)}$ with G operating via $\bar{f}^{-1}$.

Now let $\Gamma_n \subset \Gamma$ be the fixed group of S_n (see above; we may and shall suppose $S_n \subset \Omega$). Then Ω is also the separable closure of S_n, and j: $\mathrm{Gal}(R, G) \to \mathrm{Gal}(S_n, G)$ corresponds to the *restriction* res: $\mathrm{Hom}(\Gamma, G) \to \mathrm{Hom}(\Gamma_n, G)$. Moreover $\Gamma/\Gamma_n = G_n$, and the operation of G_n on $\mathrm{Gal}(S_n, G)$ is easily translated: For $S_n \subset S \subset \Omega$, S/S_n G-Galois, one has ${}_\gamma S \cong \gamma(S) \subset \Omega$ for all $\gamma \in \Gamma$, hence if $\varphi(S) = h: \Gamma_n \to G$, then $\varphi({}_\gamma S) = {}^\gamma h$, with ${}^\gamma h(\beta) = \gamma h(\gamma^{-1}\beta)$. Note that obviously ${}^\gamma h = h$ for $\gamma \in \Gamma_n$.

After these preparations, let us set $C = C_{p^n}$ and replace $\mathrm{Gal}(R, C)$ by $\mathrm{Hom}(\Gamma, C)$, and also $\mathrm{Gal}(S_n, C)$ by $\mathrm{Hom}(\Gamma_n, C)$. In doing so, we replace j by res: $\mathrm{Hom}(\Gamma, C) \to \mathrm{Hom}(\Gamma_n, C)$. We write all Hom groups as H^1, agreeing that Γ operates trivially on C. Moreover we embed "res" in an exact sequence:

$$1 \to H^1(\Gamma/\Gamma_n, C) \xrightarrow[\mathrm{inf}_1]{} H^1(\Gamma, C) \xrightarrow[\mathrm{res}]{} H^1(\Gamma_n, C)$$
$$\xrightarrow[t]{} H^2(\Gamma/\Gamma_n, C) \xrightarrow[\mathrm{inf}_2]{} H^2(\Gamma, C).$$

Here t is the *connection* or *transgression* (see [23, XI 10.6]). It is easy in our case to give the definition of t: Pick a left transversal $\{\beta_\tau | \tau \in \Gamma/\Gamma_n\}$ of Γ_n in Γ. Define for every $f \in H^1(\Gamma_n, C) = \mathrm{Hom}(\Gamma_n, C)$ and $\tau, \vartheta \in \Gamma/\Gamma_n$: $t(f)_{\tau,\vartheta} = \beta_\tau \beta_\vartheta \beta_{\tau\vartheta}^{-1}$. Then $t(f)$ defines a 2-cohomology class in $H^2(\Gamma/\Gamma_n, C)$ which is trivial if and only if f extends to Γ.

We finally show that inf_2 is trivial. It will clearly suffice if the map $\mathrm{inf}_{2,m}$: $H^2(\Gamma/\Gamma_n, C) \to H^2(\Gamma/\Gamma_m, C)$ is trivial for some $m \geq n$ (note $\Gamma_m \subset \Gamma_n$). By Lemma 2.7 below, there is an index m such that p^n divides $[\Gamma_n : \Gamma_m]$. By Lemma 2.3.1, $\mathrm{inf}_{2,m}$ will be trivial.

Lemma 2.3.1. *If* $p^n | [\Gamma_n : \Gamma_m]$, *then* $\mathrm{inf}_{2,m}$: $H^2(\Gamma/\Gamma_n, C) \to H^2(\Gamma/\Gamma_m, C)$ *is trivial.*

Proof. $H^2(G, C) \cong \mathrm{Ext}^1_{\mathbb{Z}}(G, C)$ canonically, whenever G is finite cyclic and acts trivially on C, and inf in our case corresponds to the natural map from $\mathrm{Ext}(\Gamma/\Gamma_n, C)$ to $\mathrm{Ext}(\Gamma/\Gamma_m, C)$ induced by pulling back. We take an extension $0 \to C \to E \to \Gamma/\Gamma_n \to 0$ and let $0 \to C \to E' \to \Gamma/\Gamma_m \to 0$ be the pulled-

back extension. Take a preimage $\gamma' \in E'$ of a generator of Γ/Γ_m and let $\gamma =$ image of γ' in Γ/Γ_n. We have that $\gamma^{|\Gamma/\Gamma_n|} = c \in C$. It follows that $\gamma'^{|\Gamma/\Gamma_m|} = c^{|\Gamma_n/\Gamma_m|} = 1$ since p^n divides $|\Gamma_n/\Gamma_m|$ and $C = C_{p^n}$, hence the pulled-back extension splits. □

This shows that $\mathrm{Ker}(j) \cong H^1(G_n, C)$ and

$$\mathrm{Coker}(j) \cong H^2(G_n, C) \cong H^0(G_n, C).$$

Since G_n is cyclic and C is finite, the Herbrand quotient $(h^0/h^1)(G_n, C)$ is 1, hence $\mathrm{Ker}(j)$ and $\mathrm{Coker}(j)$ have the same order $\gcd(p^n, |G_n|)$. Both are cyclic because C is cyclic. This proves Theorem 2.3. □

Remarks. (a) At the end of the paper [6] there is a short indication of a cohomological argument. Our procedure here is both simpler and more general.

(b) For the (hitherto excluded) case $p = 2$ one gets by the same method: If all G_m are cyclic, then Theorem 2.3 is still true for all n.

Proof of Theorem 2.4. Since S_n is connected by construction, [13, Theorem 6] can be applied and gives $\mathrm{Ker}(j_0) = \mathrm{Ker}(j) \cong \mathrm{Hom}(G_n, C_{p^n})$ which is indeed cyclic of order $\gcd(p^n, |G_n|)$. (Or else, see the argument for the kernel given in the previous proof.)

The essential point is the determination of $\mathrm{Coker}(j_0)$. By [16, 2.5] we know that $\mu_{p^n}(S_n)$ is generated by ζ because S_n is connected. Let $m = |G_n|$ and $e = e_n = p^n/\gcd(p^n, m)$. (One can show that the sequence (e_n) is eventually constant.)

Claim. There exists an exact sequence

$$\mathrm{Gal}_0(R, C_{p^n}) \xrightarrow{j_0} T^n(S_n^*)^{tG_n} \xrightarrow{\partial} \frac{\mu_{p^n}(S_n)}{\mu_{e_n}(S_n)} \longrightarrow 1.$$

Proof of the claim. We recall Galois descent theory (see, e.g., [21]). Let M be some algebraic structure (module, algebra, etc.) over S_n. Then $M \cong S_n \otimes_R N$ for some R-structure of the same kind if and only if:

> there exists a *descent datum* $(\varphi_\delta)_{\delta \in G_n}$ on M, i.e.: $\varphi_\delta \in \mathrm{Aut}_R(M)$, φ_δ is δ-linear (for all $x \in M$, $s \in S_n$: $\varphi_\delta(s \cdot x) = \delta(s) \cdot \varphi_\delta(x)$), and $\varphi_\delta \varphi_\varepsilon = \varphi_{\delta\varepsilon}$ for all $\delta, \varepsilon \in G_n$.

Since $G_n = \langle \gamma \rangle$, it is enough to consider only the single automorphism $\varphi = \varphi_\gamma$, where φ is γ-linear and satisfies $\varphi^m = \mathrm{id}_M$. For R a field, the following construction was found independently by Childs (see [6]). We talk now about the algebraic structure "algebra with C_{p^n}-action by algebra automorphisms". By faithfully flat descent, such a structure A over R is Galois over R if and only if $S_n \otimes_R A$ is Galois over S_n. (Note that S_n is Galois, hence faithfully flat over R.)

Let us take $[x] \in T^n S_n^*)^{tG_n} \subset S_n^*/S_n^{*p^n}$ (we denote residues mod $S_n^{*p^n}$ by [ ]), and let us try to find a descent datum $\varphi \in \mathrm{Aut}_R(A_x)$. There will be an

obstruction to the finding of φ, which we call $\partial([x])$. The fact that $[x]$ is fixed under the t-action of G_n means

(1) There is $u \in S_n^*$ with $\gamma(x) = x^g \cdot u^{p^n}$.

Now *suppose* φ is in $\mathrm{Aut}(A_x)$, is γ-linear, and commutes with the Galois action σ. From $\gamma(\zeta) = \zeta^g$ one easily infers that $\varphi(\overline{T})$ has the form $v \cdot \overline{T}^g$ for some $v \in S_n^*$. (Recall $A_x = S_n[T]/(T^{p^n} - x)$.) If we *define* φ by the assignment $\overline{T} \mapsto v \cdot \overline{T}^g$ and γ-linearity, then we obtain from (1):

(2) φ is an algebra automorphism $\Leftrightarrow v^{p^n} = u^{p^n} \Leftrightarrow v = \zeta^i u$ for some i.

The map φ then is a descent datum precisely if $\varphi^m = \mathrm{id}$, i.e., $\varphi^m(\overline{T}) = \overline{T}$. We calculate:

$$\varphi^2(\overline{T}) = \varphi(v \cdot \overline{T}^g) = \gamma(v) \cdot v^g \cdot \overline{T}^{g^2},$$

$$\varphi^3(\overline{T}) = \gamma^2(v) \cdot \gamma(v^g) \cdot v^{g^2} \cdot \overline{T}^{g^3},$$

$$\cdots$$

$$\varphi^m(\overline{T}) = \gamma^{m-1}(v) \cdot \gamma^{m-2}(v^g) \cdot \cdots \cdot \gamma(v^{g^{m-2}}) \cdot v^{g^{m-1}} \cdot \overline{T}^{g^m},$$

or in symbolic exponential notation (exponents in $\mathbb{Z}G_n$)

$$= v^{c_m} \cdot \overline{T}^{g^m}, \quad \text{where } c_m = \sum_{j=0}^{m-1} g^j \cdot \gamma^{m-1-j}.$$

Let $z = \varphi^m(\overline{T})/\overline{T}$. Since $g^m \equiv 1 \bmod p^n$, z is a unit of S_n.

Lemma. $z^{p^n} = 1$.

Proof of the Lemma. Write $q = p^n$. Recall $\overline{T}^q = x$, and by definition $z = \overline{T}^{g^m - 1} \cdot v^{c_m}$. It follows that $z^{p^n} = x^{g^m - 1} \cdot v^{p^n \cdot c_m}$. Now use $v^{p^n} = u^{p^n} = x^{-g} \cdot \gamma(x) = x^{-g+\gamma}$, so we get $z^{p^n} = x^{g^m - 1} \cdot x^{(-g+\gamma) \cdot c_m} = 1$, since it follows from the definition of c_m that $(-g + \gamma) \cdot c_m = -g^m + \gamma^m = -g^m + 1$.

Remark. We have shown that φ is a descent datum if and only if z equals 1.

Definition. Let $\partial([x])$ be the class of z in $\mu_{p^n}(S_n)/\mu_{e_n}(S_n)$.

It has to be checked that ∂ is well defined. There are two choices involved in its definition: one may, first, replace x by $x \cdot w^q$ for $s \in S_n^*$. Second, one may keep x but change v by some power of ζ. Let us first examine the effect of the latter change. One sees that changing v to $v\zeta$ changes z by the factor $\zeta^{c_m} = (\zeta^{g^{m-1}})^m = (\zeta^{g^{-1}})^m$. Since g is prime to p^n, this is a primitive e_nth root of unity by definition of e_n, whence z does not change modulo $\mu_{e_n}(S_n)$. Now imagine that we changed x to $x' = x \cdot w^q$. Then u changes to $u' = u \cdot \gamma(w)/w^q$, and by the above argument we may choose v' as we like, as long as $v'^q = u'^q$. If we take $v' = v \cdot \gamma(w)/w^q$, then the resulting z' equals z (easy check).

Now we can prove the exactness of the sequence in our claim. Once ∂ is well defined, it is obviously a homomorphism. If $[x] \in \mathrm{Im}(j_0)$, then A_x

is descendable, i.e., some descent datum φ must exist and satisfy $\varphi^m = \mathrm{id}$. Hence z can be chosen 1, and $\partial([x])$ is trivial. On the other hand, if $\partial([x])$ is trivial, then z (as constructed above for some choice of v) is an e_nth root of unity. Hence it is a power of $\zeta^{g^{-1}m}$. We may change v by the same power of ζ^{-1}, and by the above verification that ∂ was well defined, z will change to 1. Therefore the new v gives a descent datum.

∂ is surjective: Take $x = \zeta$. We have $\gamma(x) = x^g$, which shows that $[x]$ is contained in $T^n(S_n^*)^{tG_n}$. We can take $u = v = 1$ and obtain directly that $z = \zeta^{(g^m-1)/p^n}$ (see the proof of the lemma above). If $n \geq 2$, Lemma 1.1(b) shows that z is a primitive p^nth root of unity, hence ∂ is onto. If $n = 1$, then m is prime to p since it divides $p - 1 = |(\mathbb{Z}/p^n\mathbb{Z})|$, hence we get $e = e_1 = p$, and the range $\mu_p(S_n)/\mu_e(S_n)$ of ∂ is trivial, so there is nothing to prove. This finishes the proof of the claim, and Theorem 2.4 follows. □

Corollary 2.5. *The groups* $\mathrm{Gal}_0(R, C_{p^n})$ *and* $T^n(S_n^*)^{tG_n}$ *have the same order (which may be infinite in general). Likewise* $|\mathrm{Gal}(R, C_{p^n})| = |\mathrm{Gal}(S_n, C_{p^n})^{G_n}|$. *In the case* $p = 2$, *this remains correct if all* G_n *are cyclic.*

Proof. This is clear from Theorems 2.3 and 2.4. □

As remarked in the Introduction, one can even prove that $\mathrm{Gal}_0(R, C_{p^n})$ and $T^n(S_n^*)^{tG_n}$ are isomorphic as groups. In the same vein, $\mathrm{Gal}(R, C_{p^n})$ and $\mathrm{Gal}(S_n, C_{p^n})^{tG_n}$ are also isomorphic. The isomorphisms are not canonical. For details, see [8].

Remark. All results in this section remain valid if one lets $p = 2$ and supposes that for all n, $t(G_n)$ is contained in the image of $1 + 4\mathbb{Z}$ in $\mathbb{Z}/2^n\mathbb{Z}$. This happens exactly if R contains i (a square root of -1).

We conclude this section with some remarks on the extension S_n/R and the groups G_n.

Definition. The *characteristic number* $\varepsilon = \varepsilon_R$ of R is the supremum of all $d \in \mathbb{N}$ such that S_1 contains a root of the cyclotomic polynomial Φ_{p^d}. ($\varepsilon = \infty$ may happen.)

Example. $\varepsilon = 1$ if R is $\mathbb{Z}[p^{-1}]$.

Lemma 2.6. *The extension* S_n/R *is unique in the following sense: If* T/R *is connected,* Γ*-Galois for some abelian group* Γ, *and contains a root* η *of* Φ_{p^n} *such that* $t\colon \Gamma \to (\mathbb{Z}/p^n\mathbb{Z})^*$ *with* $\gamma(\eta) = \eta^{t(\gamma)}$ *for all* $\gamma \in \Gamma$ *is injective, then* $\Gamma \cong G_n$ *canonically, and* S_n *is* G_n*-isomorphic to* T.

In particular, the definition of ε *does not depend on the choice of* S_1.

Proof. First we show T is generated by η. All powers of η with exponent prime to p are roots of Φ_{p^n}, and all roots of Φ_{p^n} are primitive p^nth roots of unity. By [16, 2.5], all roots of Φ_{p^n} in T are powers of η. Hence one may apply [16, 2.6] and obtain that $R[\eta]$ is Galois over R. Its Galois group is a

factor group of Γ, but by hypothesis all $\gamma \in \Gamma$ are determined by their effect on η, hence the Galois group of $R[\eta]$ over R is exactly Γ, i.e., $T = R[\eta]$. Exactly in the same way one shows $S_n = R[\zeta]$.

By [16, pp. 463–464] R has a separable closure Ω and both S_n and T are embeddable in Ω. Let D and E be isomorphic images of S_n, resp. T, in Ω. Then D and E are generated by the respective images of ζ and η. But there are only $(p-1)p^{n-1}$ primitive p^nth roots of unity in Ω [16, 2.5]. Hence $\eta = \zeta^i$ for some i prime to p, so $D = E$. From this everything follows. □

Lemma 2.7. *For $n > \varepsilon$, S_n has rank $p^{n-\varepsilon}$ over S_1. For $n \leq \varepsilon$, $S_n = S_1$.*

Proof. The second statement is clear. The rank of S_{n+1} over S_n is 1 or p, since S_{n+1} is obtained from S_n by adjoining a pth root, and all pth roots of unity are already in S_n. Therefore certainly $S_{\varepsilon+1}$ has rank p over S_ε. We must show that the following is impossible: $S_n \neq S_{n+1}$ but $S_{n+1} = S_{n+2}$. If this were the case, then $|G(S_{n+2}/S_n)| = p$, whence the group $t(G(S_{n+2}/S_n))$ would be the subgroup of $(\mathbb{Z}/p^{n+2}\mathbb{Z})^*$ which is generated by $\overline{(1+p^{n+1})}$. Hence the restriction $G(S_{n+2}/S_n) \to G(S_{n+1}/S_n)$ would be trivial. This restriction, however, is onto by the main theorem of Galois theory [5]. Hence $G(S_{n+1}/S_n) = 1$, a contradiction. □

3. Proof of $\mathrm{Gal}_0(R, C_{p^n}) = \mathrm{NB}(R, C_{p^n})$

As usual, R is supposed connected with $p^{-1} \in R$, p an odd prime. Let S_n be a connected G_n-Galois extension of R which contains a primitive p^nth root ζ_{p^n}, as in §2. Also in §2 (after 2.2), we constructed a short exact sequence

$$1 \to \mathrm{Gal}_0(R, C_{p^n}) \to \mathrm{Gal}(R, C_{p^n}) \to P(R, C_{p^n}) \to 1.$$

Note $P(R, C_{p^n})$ was defined by this sequence. In §4 we will be concerned with $P(R, C_{p^n})$. In this section, we will show that $\mathrm{Gal}_0(RC_{p^n})$ consists precisely of the C_{p^n}-extensions of R which have a normal basis.

Theorem 3.1. *With the notation of §2, we have*

$$\mathrm{Gal}_0(R, C_{p^n}) = \mathrm{NB}(R, C_{p^n}).$$

Proof. "$\supset$": By definition of Gal_0, we have to show that for arbitrary A in the group $\mathrm{NB}(R, C_{p^n})$, $j(A) = S_n \otimes A$ is in the image of i in the Kummer sequence (K) (beginning of §2). We show instead that it is in the kernel of π: $\mathrm{Gal}(R, C_{p^n}) \to T_n(\mathrm{Pic}(S_n))$. Recall $\pi(B)$ was defined to be the (class of the) invertible S_n-module $\{z \in B | \sigma(z) = \zeta_{p^n} \cdot z\}$. Now $B = S_n \otimes_R A$ has a normal basis by hypothesis, so B and $S_n[C_{p^n}]$ are isomorphic modules over the group ring $S_n[C_{p^n}]$. Therefore $\pi(B)$ is isomorphic to

$$\{x \in S_n[C_{p^n}] \| \sigma \cdot x = \zeta \cdot x\},$$

and one sees that the latter is free cyclic over S_n with generator $1 + \zeta \cdot \sigma^{-1} + \zeta^2 \cdot \sigma^{-2} + \cdots + \zeta^{q-1} \cdot \sigma^{1-q}$, $q = p^n$. Hence $\pi(B) = \pi(j(A))$ is trivial.

"$\subset$": This is more difficult. Let $A \in \mathrm{Gal}(R, C_{p^n})$ such that $B = S_n \otimes A$ is in $\mathrm{Im}(i)$, i.e., there exists $x \in S_n^*$ such that

$$B \cong (S_n[T]/(T^{p^n} - x), \sigma(T) = \zeta \cdot T) \quad (\text{with } \zeta = \zeta_{p^n}).$$

Recall that the right-hand side is denoted A_x. We also know that B carries a descent datum, i.e., a C_{p^n}-equivariant R-automorphism φ of B with order $m = |G_n|$ which is γ-linear ($\varphi(sz) = \gamma(s)\varphi(z)$ for all $s \in S_n$, $z \in B$). As earlier, γ is a fixed generator of G_n. A is exactly the algebra of fixed elements under φ. By descent theory, an element $z \in A$ gives a normal basis of A over R if and only if $1 \otimes z$ (written also z by abuse of notation) gives a normal basis of B over S_n.

The idea of proof is now: Via $B \cong A_x$, consider φ as a descent datum on A_x. Determine *all* normal bases of A_x, show that at least one of them is fixed by φ, i.e., descends and gives a normal basis over R.

Lemma 3.2. *Let $q = p^n$ and $z = \sum_{i=0}^{q-1} a_i \cdot \overline{T}^i \in A_x$, $a_i \in S_n$. Then z gives a normal basis (i.e., the elements $\alpha(z)$, $\alpha \in C_{p^n}$, are an S_n-basis of A_x) if and only if all a_i are units in S_n.*

Proof. $\{1, \overline{T}, \ldots, \overline{T}^{q-1}\}$ is an S_n-basis of A_x. Therefore z defines a normal basis if and only if the matrix

$$M = \begin{pmatrix} a_0 & a_1 & \cdots & a_{q-1} \\ a_0 & \zeta \cdot a_1 & \cdots & \zeta^{q-1} \cdot a_{q-1} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ a_0 & \zeta^{q-1} a_1 & \cdots & \zeta^{(q-1)^2} \cdot a_{q-1} \end{pmatrix},$$

which is the coefficient matrix of $(z, \sigma(z), \ldots, \sigma^{q-1}(z))^T$, is invertible. But we have $M = V \cdot \mathrm{diag}(a_0, \ldots, a_{q-1})$ with

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \zeta & \cdots & \zeta^{q-1} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 1 & \zeta^{q-1} & & \zeta^{(q-1)^2} \end{pmatrix}$$

a Vandermonde matrix. Therefore $\det(V) = \pm \prod_{0 \le i < j < q} (\zeta^i - \zeta^j)$, and this is already a unit in S_n because a power of $\zeta^i - \zeta^j$ is associated to p in $\mathbb{Z}[\zeta]$ for all $i < j < q$, and p is a unit in R. Hence M is invertible iff $\mathrm{diag}(a_0, \ldots, a_{q-1})$ is invertible. □

Now we give the proof of 3.1.

Definition. Let $U \subset I = \{0, 1, 2, \ldots, q^{-1}\}$ be a subset and let $y = \sum_{j=0}^{q-1} a_i \cdot \overline{T}^i \in A_x$ with $a_i \in S_n$. We say that y *covers* U if $a_i = 0$ for i not in U and a_i is a unit for i in U.

Lemma 3.3. (a) *If* $U_1 \cap U_2 = \emptyset$ *and* y_1 *covers* U_i $(i = 1, 2)$, *then* $y_1 + y_2$ *covers* $U_1 \cup U_2$.

(b) y *defines a normal basis of* A_x *over* S_n *if and only if* y *covers* I.

Proof. (a) is trivial. (b) follows from Lemma 3.2. □

Let G_n operate on I via $t : \delta(i) = \mathrm{res}(t(\delta) \cdot i)$ for $i \in I$, $\delta \in G_n$. By 3.3 it suffices to show: For every G_n-orbit $U \subset I \cong \mathbb{Z}/p^n\mathbb{Z}$, there exists $y = y_U$ which covers U and is invariant under φ. The case $U = \{0\}$ is trivial (take $y = 1$), so we suppose 0 is not in U. To construct y, we pick $i \in U$ and let $H = \mathrm{Stab}(i) = \{\delta \in G_n | t(\delta) \cdot i \equiv i \bmod p^n\}$. Then

$$t(H) = \{\bar{j} \in (\mathbb{Z}/p^n\mathbb{Z})^* | (\overline{(j-1)i} = \bar{0}\} \cap t(G_n),$$

and the group preceding $\cap$ in this equation is a cyclic group of order $\min(p^n, p^v)$ where v is the precise number of factors p dividing i. Therefore H and $t(H)$ are cyclic p-groups, and there exists $k \leq n$ such that

$$t(H) \equiv \{\bar{j} \in (\mathbb{Z}/p^n\mathbb{Z})^* | j \equiv 1 \bmod p^{n-k}\}.$$

Lemma 3.4. $\sum_{h \in t(H)} h = p^k + p^n\mathbb{Z}$.

Proof.

$$\begin{aligned} \sum_{h \in t(H)} h &= |H| \cdot 1 + \sum_{s \bmod p^k} s \cdot p^{n-k} + p^n\mathbb{Z} \\ &= p^k + p^{n-k} \cdot \tfrac{1}{2} p^k (p^k - 1) + p^n\mathbb{Z} \\ &= p^k + p^n\mathbb{Z}, \quad \text{since } p \neq 2. \quad \square \end{aligned}$$

We write $i = p^k i_1$, $i_1 \in \mathbb{N}$. (p^k divides i since $1 + p^{n-k} \in t(H)$.)

For any subgroup $V \subset G_n$ and any multiplicative group M on which G_n operates, we define

$$N_V(a) = \prod_{\delta \in V} \delta(a) \quad \text{for } a \in M.$$

If M is a ring, we also have this norm map, plus an additive analog $\mathrm{tr}_V(a) = \sum_{\delta \in V} \delta(a)$. We let G_n operate on A_x via φ by setting $\gamma^j(z) = \varphi^j(z)$ for $z \in A_x$, $j \in \mathbb{N}$. Then N_H and tr_H are functions on A_x. On $I = \{0, 1, \ldots, p^n - 1\} \cong \mathbb{Z}/p^n\mathbb{Z}$, we have tr_H (we write this rather than N_H, since I is an additive group). Lemma 3.4 says that $\mathrm{tr}_H(i_1) = \sum_{t(H)} h \cdot i_1 = p^k \cdot i_1 = i$. We now consider the element $N_H(\overline{T}^{i_1})$. It will have the form $w \cdot \overline{T}^{\mathrm{tr}_H(i_1)} = w \cdot \overline{T}^i$ for some $w \in S_n^*$ and will be H-invariant. For any H-invariant $z \in A_x$ we let $\mathrm{tr}_{G_n/H}(z) = \sum \delta(z)$ with δ running over any transversal of H in G_n. Thus we can define

$$\begin{aligned} y &= \mathrm{tr}_{G_n/H}(N_H(\overline{T}^{i_1})) = \mathrm{tr}_{G_n/H}(w \cdot \overline{T}^i) \\ &= \sum_{\delta \in G_n \bmod H} \delta(w \cdot \overline{T}^i) = \sum_{\delta \in G_n \bmod H} w_\delta \cdot \overline{T}^{t(\delta)i} \quad \text{with some } w_\delta \in S_n^*. \end{aligned}$$

Here the $t(\delta)i$ are all distinct and exhaust the orbit U. Hence y covers U. By construction, y is G_n-invariant, hence φ-invariant. This proves Theorem 3.1. □

Remark 3.5. For $p = 2$ the main result of this section remains valid if one supposes that for all n, $t(G_n)$ is contained in $(1+4\mathbb{Z})/2^n\mathbb{Z}$. Then G_n is again cyclic. One needs a modification in the last part of the proof, since Lemma 3.4 is not exactly true for $p = 2$.

4. The main exact sequence (calculation of $P(R, C_{p^n})$)

Let R be, as always, a connected ring containing $1/p$, p an odd prime.

In §2 we constructed exact sequences (Theorems 2.3 and 2.4) which fit together in the following diagram:

$$\begin{array}{ccccccccc} & & \mathrm{Ker}(j_0) & = & \mathrm{Ker}(j) & & & & \\ & & \downarrow & & \downarrow & & & & \\ 1 & \to & \mathrm{Gal}_0(R, C_{p^n}) & \xrightarrow{i} & \mathrm{Gal}(R, C_{p^n}) & \xrightarrow{\pi} & P(R, C_{p^n}) & \to & 1 \\ & & {\scriptstyle j_0}\downarrow & & {\scriptstyle j}\downarrow & & {\scriptstyle j'}\downarrow & & \\ 1 & \to & T^n(S_n^*)^{tG_n} & \xrightarrow{i} & \mathrm{Gal}(S_n, C_{p^n})^{G_n} & \xrightarrow{\pi'} & T_n(\mathrm{Pic}(S_n))^{tG_n} & & \\ & & \downarrow & & \downarrow & & & & \\ & & \mathrm{Coker}(j_0) & = & \mathrm{Coker}(j) & & & & \end{array}$$

Recall from the claim in 2.4 and from 2.3 that $\mathrm{Coker}(j_0) = \mathrm{Coker}(j)$ was isomorphic to a certain factor group of $\mu_{p^n}(S_n)$, via ∂. It is immediate by the Snake Lemma that j' is injective, and it is easy to see that j' is surjective exactly if π' is. (Here i' and π' are induced by i and π in the Kummer sequence.) The objective of this section is to show that j' is an isomorphism, by showing π' is onto. This will give the announced determination of the group $P(R, C_{p^n})$.

Theorem 4.1. *The map* $\pi'\colon \mathrm{Gal}(S_n, C_{p^n})^{G_n} \to T_n(\mathrm{Pic}(S_n))^{tG_n}$ *is surjective.*

Proof. We first recall the description of $\mathrm{Gal}(S_n, C_{p^n})$ by *discriminant modules*: A discriminant module over S_n is a pair (P, ν), where ${}_{S_n}P$ is projective of rank one, and ν is an isomorphism $P^{\otimes q} \to S_n$ $(q = p^n)$. Two such pairs, (P, ν) and (Q, β), are called isomorphic if there is an isomorphism $f\colon P \to Q$ such that $\beta = \nu(f^{\otimes q})$. The set of isomorphism classes of discriminant modules carries a composition:

$$(P, \nu)\cdot(Q, \beta) = (P \otimes Q, (\nu \otimes \beta)\tau : (P \otimes Q)^{\otimes q} \xrightarrow[\cong]{\tau} P^{\otimes q} \otimes Q^{\otimes q} \xrightarrow{\nu\otimes\beta} S_n),$$

which makes it into an abelian group $\mathrm{Disk}(q, S_n)$. One has an isomorphism

$$\pi\colon \mathrm{Gal}(S_n, C_{p^n}) \to \mathrm{Disk}(q, S_n),$$
$$A \mapsto (\pi(A), \mathrm{mult}) \text{ (recall } \pi(A) = \{x \in A \mid \sigma(x) = \zeta \cdot x\}).$$

The inverse map is given by $(P, \nu) \mapsto A_{(P,\nu)}$, where

$$A_{(P,\nu)} = (S_n \oplus P \oplus P^{\otimes 2} \oplus \cdots)/(y - \nu(y)\cdot 1 \mid y \in P^{\otimes q}).$$

(See [2, pp. 524–526]. Borevich does not use the term "discriminant module".)

The group G_n operates canonically on $\mathrm{Disk}(q, S_n)$ by $\delta(P, \nu) = ({}_\delta P, \delta\nu)$. Note that this makes sense, because $\delta\nu\colon {}_\delta P^{\otimes q} \to {}_\delta S_n \to S_n$ is S_n-linear. As in Lemma 2.1, one shows: The isomorphism between $\mathrm{Gal}(S_n, C_{p^n})$ and $\mathrm{Disk}(p^n, S_n)$ is G_n-linear if we take the Stickelberger action on $\mathrm{Disk}(p^n, S_n)$. Therefore we get an exact sequence obtained from the middle row of the diagram preceding Theorem 2.3:

$$1 \to \mathrm{Ker}(j) \to \mathrm{Gal}(S_n, C_{p^n}) \xrightarrow{j} \mathrm{Disk}(p^n, S_n)^{tG_n}.$$

We introduce symbolic tensor powers (all tensor products are taken over S_n):

Definition. For P an invertible S_n-module and $z = \sum c_\delta \cdot \delta \in \mathbb{Z}[G_n]$, we define

$$P^z = \bigotimes_{\delta \in G_n} (\delta^P)^{\otimes c_\delta} \text{(a negative tensor power means the } S_n\text{-dual of the corresponding positive power)}.$$

Remarks. (a) $P^z \otimes P^u \cong P^{z+u}$, $(P^z)^u \cong P^{zu}$ canonically for $z, u \in \mathbb{Z}[G_n]$.

(b) $P^{-z} \cong (P^z)^*$ canonically for $z \in \mathbb{Z}[G_n]$.

(c) If S_n is a domain, then all invertible S_n-modules are isomorphic to fractional ideals. If one defines $P^z = \prod \delta(P)^{c_\delta} \subset \mathrm{Quot}(S_n)$ for $P \subset \mathrm{Quot}(S_n)$ a fractional ideal, then the canonical isomorphisms in (a) and (b) become equalities.

(d) The operation $(\ )^z$ is likewise defined for morphisms, and is an endofunctor of the category of invertible S_n-modules.

Lemma 4.2. *The operation* $(\ )^z$ *extends in a natural fashion to an operation on* $\mathrm{Disk}(p^n, S_n)$.

Proof. By Remark (a), second statement, there is a canonical isomorphism $\iota : (P^z)^q \to (P^q)^z$. Hence $(\nu)^z\iota$ is a map from $(P^z)^q$ to S_n^z. Now S_n^z is canonically S_n-isomorphic to S_n (for $z = \delta$, take $\delta : S_n^z = {}_\delta S_n \to S_n$. In general, tensor together). Let ν_z denote the composite: $(P^q)^z \to S_n^z \to S_n$ and define $(P, \nu)^z$ as $(P^z, \nu_z\iota)$. Remarks (a) and (b) still hold for this operation of $\mathbb{Z}[G_n]$ on $\mathrm{Disk}(p^n, S_n)$. □

Lemma 4.3. *Let* $P \in \mathrm{Pic}(S_n)$ *be a* p^n*-torsion element, and let* $(P, \nu) \in \mathrm{Disk}(p^n, S_n)$.

(a) *(The class of)* P *is in* $\mathrm{Pic}(S_n)^{tG_n}$ *if and only if* $P^{\gamma-g} \cong S_n$.

(b) *(The class of)* (P, ν) *is in* $\mathrm{Disk}(p^n, S_n)^{tG}$ *if and only if* $(P^{\gamma-g}, \nu_{\gamma-g}\iota) \cong (S_n, 1)$.

Proof. (a) Recall $t(\gamma) = g + p^n\mathbb{Z}$. Take $r \in \mathbb{Z}$ with $gr \equiv 1 \bmod p^n$. Then P is fixed under the Stickelberger action of $G_n \Leftrightarrow P \cong {}_\gamma P^{\otimes r} \Leftrightarrow P^{\otimes g} \cong {}_\gamma P^{\otimes rg} \Leftrightarrow P^{\otimes g} \cong {}_\gamma P \Leftrightarrow P^{\gamma-g} \cong S_n$. The second and third equivalence used that $P^{\otimes p^n} \cong S_n$.

(b) This is the same proof, with one extra point: Some steps in (a) used that $p^{\otimes q}$ is trivial. Thus one has to make sure that also $\mathrm{Disk}(q, S_n)$ is q-torsion as an abelian group. Although this is probably standard, we indicate the argument since it gives the idea of how to prove 4.1. Take (P, ν) in $\mathrm{Disk}(q, S_n)$. Then $P^{\otimes q}$ also has the structure of a discriminant module and, looking carefully at the definition of the product in $\mathrm{Disk}(q, S_n)$, one sees that the map $(P^{\otimes q})^{\otimes q} \to S_n$ is given by

$$(P^{\otimes q})^{\otimes q} \xrightarrow{\text{twist}} (P^{\otimes q})^{\otimes q} \xrightarrow{\nu^{\otimes q}} S_n$$

where twist $= \tau_{q,q}$ is a special case $(q = r)$ of the canonical isomorphism $\tau_{r,q}\colon (P^{\otimes r})^{\otimes q} \to (P^{\otimes q})^{\otimes r}$. But one checks easily (e.g., by localizing and picking generators) that twist is the identity. From this one deduces that $\nu\colon (P^{\otimes q}, \nu^{\otimes q}) \to (S_n, 1)$ is an isomorphism of discriminant modules. □

Now we continue the proof of 4.1. Take an element of $T_n(\mathrm{Pic}(S_n))^{tG_n}$, i.e., take $P \in T_n(\mathrm{Pic}(S_n))$ with $P^{\gamma-g} \cong S_n$ (Lemma 4.3(a)). Pick an isomorphism $h\colon P^{\gamma-g} \cong S_n$. In the proof of Proposition 1.2, we showed that there is an integer u prime to p such that $u \cdot p^n = \rho \cdot (\gamma - g)$ for some ρ in $\mathbb{Z}[G_n]$.

Define $Q = P^u$ $(= P^{\otimes u})$, and define $\nu\colon Q^{\otimes q} \to S_n$ as the composition

$$Q^{\otimes q} = (P^u)^{\otimes q} \xrightarrow{\cong} (P^{\gamma-g})^{\rho} \xrightarrow{h_\rho} S_n.$$

(Here h_ρ is h^ρ followed by $(S_n)^\rho \cong S_n$, as in the proof of 4.2.)

If we can show that (Q, ν) is in $\mathrm{Disk}(q, S_n)^{tG_n}$, we will be done. For then (Q, ν) will define a C_{p^n}-extension $A \in \mathrm{Gal}(S_n, C_{p^n})^{tG_n}$ with $\pi(A) = Q$, hence we will have a preimage of $Q = P^u$, and since u is prime to p and P is $p^n = q$-torsion, we also will have a preimage of P.

It is obvious from the definition that (Q, ν) is a discriminant module. The point is to show that it is fixed under the Stickelberger action of G_n.

We have to prove that the two discriminant modules $(S_n, 1)$ and $(Q, \nu)^{\gamma-g} = (Q^{\gamma-g}, \nu_{\gamma-g}\iota)$ are isomorphic (ι the canonical isomorphism $(Q^{\gamma-g})^q \xrightarrow{\sim} (Q^q)^{\gamma-g}$). Let F be the composition

$$f\colon Q^{\gamma-g} \to (P^{\gamma-g})^u \xrightarrow{h_u} S_n.$$

We claim that f is an isomorphism of discriminant modules from $(Q^{\gamma-g}, \nu_{\gamma-g}\iota)$ to $(S_n, 1)$. For this to be the case, we need that

$$\begin{array}{ccc} (Q^{\gamma-g})^q & \xrightarrow{\iota} & (Q^q)^{\gamma-g} \\ {\scriptstyle f_q}\downarrow & & \downarrow{\scriptstyle \nu_{(\gamma-g)}} \\ S_n & = & S_n \end{array}$$

commutes. This is intuitively clear, since up to canonical isomorphisms we have $f_q = (h_u)_q = h_{uq} = h_{\rho(\gamma-g)} = (h_\rho)_{\gamma-g} = \nu_{\gamma-g}$. If S_n is a domain or, more generally, if it admits an artinian quotient ring, then we may assume that P is a fractional ideal, and as explained in Remark (c) above, all canonical isomorphisms are just identities. Hence we are done in that case. Since this absolutely suffices for all applications, we leave the general case to the reader (or see [8, p. 24]). □

Remarks. What we have achieved in §§2–4 is the following. We have a description of the abelian group $\mathrm{NB}(R, C_{p^n})$ by a canonical exact sequence linking it to a "more elementary" group $T^n(S_n^*)^{tG_n}$ such that these two groups have the same order, and we mentioned that $\mathrm{NB}(R, C_{p^n})$ can even be shown to be isomorphic to $T^n(S_n^*)^{tG_n}$. What is more, we also have a description of the factor group $P = \mathrm{Gal}(R, C_{p^n})/\mathrm{NB}(R, C_{p^n})$: it is canonically isomorphic to $T_n(\mathrm{Pic}(S_n))^{tG_n}$.

I. Kersten and J. Michaliček also gave a description of $\mathrm{NB}(R, C_{p^n})$ by showing that it is isomorphic to a certain subquotient of $R[\Gamma_n]^*$, where Γ_n is the dual group of C_{p^n}. They obtained lifting theorems for C_{p^n}-extensions by this method (see [18]).

While it takes a little more to deduce the lifting theorems from our results, our description has the advantage that the groups $T^n(S_n^*)^{tG_n}$ are often quite tractable, as we will see in Part II. In contrast, the calculation of $T_n(\mathrm{Pic}(S_n))^{tG_n}$ is much harder.

It is also possible to describe $\mathrm{NB}(R, C_{p^n})$ by a *factor* group of $T^n(S_n^*)$. To this end, one defines a *corestriction* for the functors Gal and NB and one proves similarly as Merkurjev [24] that cor: $\mathrm{NB}(S_n, C_{p^n}) \to \mathrm{NB}(R, C_{p^n})$ is surjective, and that its kernel is $(1-\gamma)\cdot\mathrm{NB}(S_n, C_{p^n})$. Using this result [8, p. 27], one may reprove lifting theorems of Saltman [25, Theorem 2.1, Corollary 5.3] and Kersten and Michaliček [18, Corollary 3.11]. It is remarkable that these lifting theorems do not remain exactly true for $p = 2$ (Wang's famous counterexample [26]).

PART II. Applications in Number Theory

1. C_{p^n}-extensions and $\mathbb{Z}_p$-extensions

Let p be a prime. From §2 onward, we will also need $p \neq 2$. In the first part, we repeatedly indicated how to deal with $p = 2$ by means of extra hypotheses. In order to rid this part of these interruptions, we indicate here once and for all that all results remain valid if K (see below) contains i (a square root of -1). The reason is that then G_n is cyclic and $t(G_n) \subset \{1 + 4r | r \in \mathbb{Z}\} \subset (\mathbb{Z}/2^n\mathbb{Z})^*$, so the theory of Part I is applicable. This said, we *henceforth assume p odd.*

We recall some definitions and facts from algebraic number theory. Suppose K is an algebraic number field with r real and $2s$ nonreal embeddings $K \to \mathbb{C}$.

(In standard notation, r is r_1 and s is r_2, but we want to save subscripts.) A $\mathbb{Z}_p$-extension L/K is a normal algebraic field extension such that $G(L/K)$, the automorphism group of L over K, is isomorphic to $\mathbb{Z}_p$ as a topological group. Equivalently, a $\mathbb{Z}_p$-extension is a sequence

$$K = L_0 \subset L_1 \subset L_2 \subset \cdots, \quad \text{with } L_n \text{ a } C_{p^n}\text{-Galois extension of } K.$$

Here L is the union of all the L_n. By [27, 13.2] only primes of K above p can ramify in L/K. If L'/K is the compositum of all $\mathbb{Z}_p$-extensions, then [27, Theorem 13.4]

$$G(L'/K) \cong \mathbb{Z}_p^{c(K)},$$

where $c(K)$ is a number between $s+1$ and $[K : \mathbb{Q}] = r + 2s$. Leopoldt's conjecture states that $c(K) = s + 1$. Often one denotes $c(K) - s - 1$ by δ and calls it the *defect*. (The conjecture originates from [22]. More details can also be found in [27, §5].)

In this section, we explain the connection between $\mathbb{Z}_p$-extensions and C_{p^n}-extensions, as studied in the first part. Let for the moment G be any finite abelian group. Then the G-Galois field extensions L/K correspond by class field theory to closed subgroups $U_L \subset C_K$ (the idele class group of K) with $C_K/U_L \cong G$. On the other hand, the set of all G-Galois extensions of K in the sense of Part I and of [4] form an abelian group called $\mathrm{Gal}(K, G)$, and there is a canonical isomorphism $\mathrm{Gal}(K, G) \cong \mathrm{Hom}_{\mathrm{cont}}(\Omega, G)$ with Ω the absolute Galois group of K (see [13, Theorem 4]). Note that $\mathrm{Gal}(K, G)$ consists of the field extensions of K with Galois group G, plus some extensions which are not fields. Actually, $L \in \mathrm{Gal}(K, G)$ is a field if and only if the corresponding $f\colon \Omega \to G$ is surjective. Since Ω^{ab} is isomorphic to C_K modulo the connected component of its neutral element by class field theory, we obtain an isomorphism

$$\begin{aligned} \mathrm{Gal}(K, G) &\cong \mathrm{Hom}_{\mathrm{cont}}(C_K, G) \\ L &\mapsto f_L \end{aligned}$$

(Hasse [14, p. 39]). Again, $L \in \mathrm{Gal}(K, G)$ is a field iff the corresponding f_L is surjective. For example, $f_L = 1$ if L is the trivial G-extension. ($L \cong K \times \cdots \times K$ as K-algebra.)

Now we consider ramification. Let Σ be a finite set of finite places of K, and let $R = \mathcal{O}_K^{\Sigma}$ be the ring of Σ-integers in K. Then $\mathrm{Gal}(R, G)$ is a subset of $\mathrm{Gal}(K, G)$ and consists precisely of the G-extensions L/K which are unramified outside Σ and infinity (see, e.g., [4, Remark 1.5d)]). If $\Sigma = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, then L/K is unramified outside Σ if and only if $f_L(U_{\mathfrak{p}_i}) = 1$ for $i = \{1, \ldots, n\}$ [27, Appendix, Theorem 14]. (Here $U_{\mathfrak{p}_i}$ is the unit group of the valuation ring of the completed field $K_{\mathfrak{p}_i}$.)

Our aim is to obtain information about $c(K)$ by looking at the groups $\mathrm{Gal}(R, C_{p^n})$ with $R = \mathcal{O}_K[p^{-1}]$ (i.e., take $\Sigma = \{\text{places dividing } p\}$). For

this, two lemmas are needed. The first is quite easy, and the second is presumably well known. Let the Landau symbol $O(1)$ stand for a function $f: \mathbb{N} \to \mathbb{R}^+$ with values in an interval $[c, C]$, $0 < c < C < \infty$.

Lemma 1.1. *Let M be a finitely generated $\mathbb{Z}_p$-module of rank $r(M)$. Then*

$$|\mathrm{Hom}(M, \mathbb{Z}/p^n\mathbb{Z})| = p^{n \cdot r(M)} \cdot O(1) \quad \text{for } n \to \infty.$$

Proof. Both sides are multiplicative with respect to direct sums. If M is torsion, then $|\mathrm{Hom}(M, \mathbb{Z}/p^n\mathbb{Z})|$ stays bounded for $n \to \infty$. By the structure theory for finitely generated $\mathbb{Z}_p$-modules, we are thus reduced to the case $M = \mathbb{Z}_p$, which is obvious. □

Lemma 1.2. $|\mathrm{Gal}(R, C_{p^n})| = p^{n \cdot c(K)} \cdot O(1)$ *for* $n \to \infty$.

Proof. Let L/K be the maximal abelian extension unramified outside p. We use the notation from the appendix of [27] for class field theory.

Let $H = G(L/k)$. Then

$$H \cong C_K \Big/ \left(\prod_{\mathfrak{p} \nmid p} U_{\mathfrak{p}} \cdot D_k \right), \qquad C_K = \text{idele class group of } K,$$

$$D_K = \text{connected component of } 1 \in C_K.$$

In other words, we have $H = (C_K / \prod_{\mathfrak{p} \nmid p} U_{\mathfrak{p}}) / \overline{D}_K \cong (J_K / K^* \cdot \prod_{\mathfrak{p} \nmid p} U_{\mathfrak{p}}) / \overline{D}_K$, where J_K stands for the idele group of K, and it is shown in [27, p. 267, bottom] that the latter group (called J' there) has a subgroup H'' of finite index such that H'' is isomorphic to $\mathbb{Z}_p^{c(K)}$. It is also shown in loc.cit. (pp. 267–268) that if L' is the compositum of all $\mathbb{Z}_p$-extensions of K, then $H' = G(L'/K)$ has finite index in H.

As discussed above,

$$\begin{aligned} \mathrm{Gal}(R, C_{p^n}) &= \{E \in \mathrm{Gal}(K, C_{p^n}) | E \text{ unramified outside } S\} \\ &\cong \{f \in \mathrm{Hom}_{\mathrm{cont}}(C_K, C_{p^n}) | f(U_{\mathfrak{p}}) = 1 \ \forall \mathfrak{p} \nmid p\} \\ &= \mathrm{Hom}_{\mathrm{cont}}(H, C_{p^n}) = \mathrm{Hom}_{\mathrm{cont}}(H_p, C_{p^n}), \end{aligned}$$

where H_p is the pro-p-part of the profinite group H. Note H_p is a finitely generated $\mathbb{Z}_p$-module, since H' has finite index in it. Now H_p has rank $c(K)$ over $\mathbb{Z}_p$ since $H' \cong \mathbb{Z}_p^{c(K)}$ by definition of $c(K)$, hence we may apply Lemma 1.1 to get our conclusion. □

2. Module-theoretic lemmas

In this section we prove some results which will be needed later, when we calculate certain fixed groups under twisted actions. Let p be an odd prime, n a natural number, and $G = G_n = \langle \gamma \rangle$ a cyclic group with an embedding $t: G \to (\mathbb{Z}/p^n\mathbb{Z})^*$, $t(\gamma) = g + p^n\mathbb{Z}$. Let P be the group ring $\mathbb{Z}_p[G]$. We resume

and extend the notation of I, §1: For every P-module M, we let

$$T^n(M) = M/p^nM,$$
$$A(M) = (T^n(M))^{tG} = \{x \in M/p^nM | g^{-1} \cdot \gamma x = x\} \quad (^{-1} \text{ taken mod } p^n)$$
$$= \{x \in M/p^nM | (\gamma - g)x = 0\},$$
$$\alpha(M) = |A(M)|.$$

Theorem 2.1. *Suppose M and N are finitely generated P-modules without $\mathbb{Z}$-torsion. If $\mathbb{Q}_p \otimes M \cong \mathbb{Q}_p \otimes N$ over $\mathbb{Q}_p[G]$ ($\otimes$ taken over $\mathbb{Z}_p$), then $\alpha(M) = \alpha(N)$.*

Proof. Consider the category $\mathscr{C}$ of finitely generated P-modules without $\mathbb{Z}$-torsion, and form a Grothendieck group $G_0^{\mathbb{Z}}(\mathscr{C})$ by taking the free abelian group on (a skeleton of) $\mathscr{C}$ and factoring out relations $[M] - [M_1] - [M_2]$ for $M, M_1, M_2 \in \mathscr{C}$ and $0 \to M_1 \to M \to M_2 \to 0$ exact. Clearly $G_0^{\mathbb{Z}}(\mathscr{C})$ is generated by the classes of P-modules M which do not possess a nontrivial $\mathbb{Z}$-pure P-submodule M' (for any such M' gives an exact sequence $0 \to M' \to M \to M/M' \to 0$ with also M/M' $\mathbb{Z}$-torsion-free of smaller $\mathbb{Z}$-rank). Let us call modules M without nontrivial $\mathbb{Z}$-pure P-submodules presimple.

Lemma 2.2. *M is presimple if and only if $\mathbb{Q}_p \otimes M$ is simple over $\mathbb{Q}_p[G]$.*

Proof. "$\Rightarrow$": Let U be a nontrivial direct summand of $\mathbb{Q}_p \otimes M$. (Observe that $M \subset \mathbb{Q}_p \otimes M$.) Then $0 \neq U \cap M \neq M$, and $M/U \cap M$ is torsion-free, a contradiction.

"$\Leftarrow$": Every $\mathbb{Z}$-pure nontrivial submodule $U \subset M$ gives a nonzero submodule $U' = \mathbb{Q}_p \otimes U \subset \mathbb{Q}_p \otimes M$. But $U' \neq \mathbb{Q}_p \otimes M$, since U is pure in M and $U \neq M$. □

Lemma 2.3. *Every simple $\mathbb{Q}_p[G]$-module T is of the form $\mathbb{Q}_p \otimes M$ for a finitely generated P-module without $\mathbb{Z}$-torsion, and M is uniquely determined up to isomorphism by these conditions.*

Proof. Since T is finitely generated over $\mathbb{Q}_p$, the existence of M is clear. Suppose M is given with $\mathbb{Q}_p \otimes M = T$. The annihilator of T is a maximal ideal I in $\mathbb{Q}_p[G]$, and $\mathbb{Q}_p[G]/I$ is a local field K. Let $\mathfrak{p} = P \cap I$. Then $\mathfrak{p} \cap \mathbb{Z}_p = 0$, $P/\mathfrak{p}$ embeds in K, and $\mathbb{Q}_p \otimes (P/\mathfrak{p}) \cong K$. The generator γ of G maps to a p^nth root of unity $\zeta \in K$, hence $P/\mathfrak{p} \cong \mathbb{Z}_p[\zeta]$ is integrally closed, one-dimensional, and local. M is a $P/\mathfrak{p}$-module, and finitely generated without $\mathbb{Z}$-torsion. Hence M has no $\mathbb{Z}_p[\zeta]$-torsion, i.e., M is free over $\mathbb{Z}_p[\zeta] \cong P/\mathfrak{p}$. Since $K \cong (\mathbb{Q}_p[G])/I \cong T \cong \mathbb{Q}_p \otimes M$, M necessarily has rank 1, i.e., $M \cong P/\mathfrak{p}$. □

Corollary 2.4. *The canonical map $b\colon G_0^{\mathbb{Z}}(\mathscr{C}) \to K_0(\mathbb{Q}_p[G])$, $b([M]) = [\mathbb{Q}_p \otimes M]$, is an isomorphism.*

Proof. The homomorphism b takes a system of generators of $G_0^{\mathbb{Z}}(\mathscr{C})$, namely the classes of presimple P-modules, by 2.3 injectively to a basis of $K_0(\mathbb{Q}_p[G])$,

namely the classes of simple $\mathbb{Q}_p[G]$-modules. In particular, the system of generators was already a basis. □

Now we can finish the proof of Theorem 2.1. We claim that α induces a homomorphism from $G_0^{\mathbb{Z}}(\mathscr{E})$ to the multiplicative group $\mathbb{Q}^*$. For this one only has to check that α is multiplicative on short exact sequences

$$0 \to M_1 \to M \to M_2 \to 0,$$

M, M_1, M_2 $\mathbb{Z}$-torsion-free P-modules. By Proposition I1.2,

$$0 \to A(M_1) \to A(M) \to A(M_2) \to 0$$

is again exact. Hence $\alpha(M) = \alpha(M_1) \cdot \alpha(M_2)$.

Finally, suppose we have finitely generated P-modules M and N without $\mathbb{Z}$-torsion, $\mathbb{Q}_p \otimes M \cong \mathbb{Q}_p \otimes N$. Since b is injective, the classes of M and N in $G_0^{\mathbb{Z}}(\mathscr{E})$ are the same. As α is defined on that Grothendieck group, the conclusion $\alpha(M) = \alpha(N)$ follows. □

One can define $\alpha(M)$ exactly in the same way if M is a module over $\mathbb{Z}[G]$ (not over $\mathbb{Z}_p[G] = P$ as above). Then we have:

Corollary 2.5. *If M and N are $\mathbb{Z}$-torsion-free finitely generated $\mathbb{Z}[G]$-modules with $\mathbb{R} \otimes_{\mathbb{Z}} M \cong \mathbb{R} \otimes_{\mathbb{Z}} N$ over $\mathbb{R}[G]$, then $\alpha(M) = \alpha(N)$.*

Proof. Since the canonical map $K_0(\mathbb{Q}[G]) \to K(\mathbb{R}[G])$ is injective, we obtain that $\mathbb{Q} \otimes M \cong \mathbb{Q} \otimes N$. Let $M' = \mathbb{Z}_p \otimes_{\mathbb{Z}} M$ and $N' = \mathbb{Z}_p \otimes_{\mathbb{Z}} N$. Then $\mathbb{Q}_p \otimes M' \cong \mathbb{Q}_p \otimes N'$ ($\otimes$ over $\mathbb{Z}_p$), so by 2.1 we get $\alpha(M') = \alpha(N')$. It is obvious from the definition that $\alpha(M') = \alpha(M)$ and $\alpha(N') = \alpha(N)$. □

3. Calculations with units in number fields

In this section, R will always be the ring of p-integers $\mathscr{O}_K[p^{-1}]$ of the arbitrarily given algebraic number field K. As above, we assume $p \neq 2$.

Let $k = [K : \mathbb{Q}]$, r be the number of real embeddings $K \to \mathbb{C}$, and $2s = k - r$ be the number of nonreal embeddings $K \to \mathbb{C}$. Let $K_n = K(\zeta_{p^n})$ and $G_n = \mathrm{Aut}(K_n/K)$. As usual, let $t: G_n \to (\mathbb{Z}/p^n\mathbb{Z})^*$ be given by $\delta(\zeta_{p^n}) = (\zeta_{p^n})^{t(\delta)}$ for all $\delta \in G_n$. Then the ring $S_n =$ ring of p-integers in $K_n = R[\zeta_{p^n}]$ is connected and G_n-Galois over R. (The reason is that K_n/K is unramified outside p. See the general remarks at the beginning of §1.) This shows S_n coincides with the extension S_n of R which we studied in Part I (see §2 in particular), i.e., Corollary I2.5 may be applied. This is the reason why we are interested in the cardinality of $|T^n(S_n^*)|^{tG_n}$. Recall that we abbreviated this to $\alpha(S_n^*)$ in §2. The goal of this section is

Theorem 3.1. *For $n \to \infty$ we have $\alpha(S_n^*) = p^{n\cdot(s+1)} \cdot O(1)$.*

More precisely, if ε is maximal with $\zeta_{p^\varepsilon} \in K_1$, then

$$\alpha(S_n^*) = p^{n\cdot(s+1)+d}, \quad \text{with } -\varepsilon \leq d \leq 2k.$$

As a preparation for the proof of this theorem, we first need a result about the relative Galois module structure of the group of units $E(K_n)$ of K_n. This is essentially the theorem of Herbrand and Artin. We only consider the case $n \neq 0$. K has $r+s$ places (= nonequivalent valuations) β_i, $i = 1, \ldots, r+s$. For every i, one chooses an extension of β_i to K_n and denotes it again by β_i. The extension β_i is always a complex place, since K_n is totally complex ($\zeta_p \in K_n$). Suppose now that β_i is real on K, and take an embedding $\varphi_i: K_n \to \mathbb{C}$ which induces the extension β_i. Let conj: $\mathbb{C} \to \mathbb{C}$ be the complex conjugation. Then φ_i and conj φ_i agree on K and have the same image, hence there exists a unique $\sigma_i \in G_n$ such that $\varphi_i \sigma_i = \text{conj}\, \varphi_i$. By evaluating this equation in ζ_{p^n} and noting that $\varphi_i(\zeta_{p^n})$ is a p^nth root of unity in $\mathbb{C}$, one finds that $\sigma_i(\zeta_{p^n}) = (\zeta_{p^n})^{-1}$, i.e., σ_i does not depend on i and is characterized by $t(\sigma_i) = -1$. To indicate this in our notation, we write τ for σ_i. Note that τ need not exist if K is already totally complex.

Now we quote the following theorem of Artin [1, GW, p. 197] (note his r is our $r+s-1$):

There are $r+s$ units $x_1, x_2, \ldots, x_{r+s} \in E(K_n)$ such that the conjugates $\sigma(x_i)$ with $1 \leq i \leq r+s$ and $\sigma \in G_n$ contain a maximal set of independent units, and the only relations are: $\tau(x_i) = x_i$ for $\beta_i | K$ real, and $\Pi\sigma(x_i)$ (Π over all i, all σ) is 1. (Ignore τ if K is already totally complex.)

We have to reformulate this slightly for our purpose. For this, we let $E'(K_n) = E(K_n) \times \xi^{\mathbb{Z}}$, where ξ is just a formal symbol and G_n acts trivially on ξ. Let $x_i' = (x_i, \xi) \in E'(K_n)$. Then one sees directly that the conjugates $\sigma(x_i')$ with $1 \leq i \leq r+s$ contain a maximal $\mathbb{Z}$-independent set in $E'(K_n)$ and the only relations are $\tau(x_i') = x_i'$ for $\beta_i | K$ real. Tensoring with $\mathbb{Q}$, we can say this differently:

Theorem 3.2. *Let* $L_n = L_n(K) = \mathbb{Q} \otimes_{\mathbb{Z}} E'(K_n)$.

(a) *If* K *is totally complex, then* L_n *is* $\mathbb{Q}[G_n]$*-free of rank* $r+s = s$.

(b) *If* K *is not totally complex, then* $L_n = A \oplus B$, A *is* $\mathbb{Q}[G_n]$*-free of rank* s, *and* B *is* $(Q[G_n])/(1-\tau)$*-free of rank* r. (*Recall* $\tau \in G_n$ *is characterized by* $t(\tau) = -1$.) □

For the next corollary, we introduce the notation $LE'(K_n) = E'(K_n)/\text{torsion}$. Note that the torsion in $E'(K_n)$ is given by the roots of unity, and note also that $L_n \cong \mathbb{Q} \otimes_{\mathbb{Z}} LE'(K_n)$. Then Theorem 3.2 gives

Corollary 3.3. $Q \otimes_{\mathbb{Z}} LE'(K_n) \cong \mathbb{Q} \otimes_{\mathbb{Z}} ((\mathbb{Z}[G_n]/(1-\tau))^r \times \mathbb{Z}[G_n]^s)$. (*For* $r = 0$, *ignore the term containing* τ.)

The major step in the proof of 3.1 is the evaluation of $\alpha(E(K_n))$. Recall the definition of $A(-)$ and α from §2. The technical core of the argument is the following:

Lemma 3.4. (a) $\alpha(\mathbb{Z}[G_n]) = p^n$.

(b) $\alpha(\mathbb{Z}[G_n]/(1-\tau)) = 1$.

(*Loosely speaking: Factoring out a quite small ideal makes all the difference for* α!)

Proof. (a) $A(\mathbb{Z}[G_n]) = \{y \in (\mathbb{Z}/p^n\mathbb{Z})[G_n] | \gamma y = gy\} = (\mathbb{Z}/p^n\mathbb{Z}) \cdot (\sum_{i=0}^{m-1} g^i \cdot \gamma^{-i})$ (recall $|G_n| = m$), and this group has p^n elements.

(b) We have $\mathbb{Z}[G_n]/(1-\tau) \cong \mathbb{Z}[H_n]$ with $H_n = G_n/\langle\tau\rangle$. Since τ has order 2, necessarily $\tau = \gamma^{m/2}$. Let γ_1 be the image of γ in H_n, and take

$$y = \sum_{i=0}^{m/2-1} a_i \cdot \gamma_1^{-1} \in (\mathbb{Z}/p^n\mathbb{Z})[H_n], \qquad a_i \in \mathbb{Z}/p^n\mathbb{Z},$$

and assume that $(g-\gamma) \cdot y = 0$. It follows that $a_{i+1} = g \cdot a_i$ for $i = 0, 1, \ldots, m/2-2$, and $a_0 = g \cdot a_{m/2-1}$. Hence $a_i = g^i \cdot a_0$ and $g^{m/2} \cdot a_0 = a_0$. But we know that $g^{m/2} = t(\gamma^{m/2}) = t(\tau) = -1$, so we have $a_0 = -a_0$. Since p is different from two, this implies $a_0 = 0$ and $y = 0$. □

Corollary 3.5. $\alpha(LE'(K_n)) = p^{n \cdot s}$.

Proof. By definition $LE'(K_n)$ is torsion-free, and by Dirichlet's Unit Theorem it is finitely generated. By Corollaries 3.3 and 2.5 we deduce that

$$\alpha(LE'(K_n)) = \alpha((\mathbb{Z}[G_n]/(1-\tau))^r \times \mathbb{Z}[G_n]^s).$$

The right-hand side is obviously equal to $\alpha(\mathbb{Z}[G_n]/(1-\tau))^r \cdot \alpha(\mathbb{Z}[G_n])^s$, and this quantity equals p^{ns} by Lemma 3.4. □

The rest of the proof is a detailed analysis of how $\alpha(LE'(K_n))$ relates to our target number $\alpha(S_n^*)$. Matters are as follows: $LE'(K_n)$ is obtained from the group of units $E(K_n)$ by two modifications: throw away torsion and adjoin $\xi^{\mathbb{Z}}$. On the other hand, S_n^* is obtained from $E(K_n)$, very roughly speaking, by adjoining inverses of divisors of p. We show basically that the effect on α of the first modification is a factor p^n, and that the effect of the second modification and the step from $E(K_n)$ to S_n^* is "bounded". Now for the details.

Proposition 3.6. $\alpha(E'(K_n)) = p^n \cdot \alpha(LE'(K_n))$.

Proof. Let $\mu(K_n)$ denote the roots of unity in K_n, and $\mu'(K_n)$ the subgroup of roots of unity of p-power order. We use the exact sequence of G_n-modules

$$1 \to \mu(K_n) \to E'(K_n) \to LE'(K_n) \to 1.$$

By Proposition I1.2 we obtain $\alpha(E'(K)) = \alpha(\mu(K_n)) \cdot \alpha(LE'(K_n))$. Obviously, $\alpha(\mu(K_n))$ equals $\alpha(\mu'(K_n))$, and we are done if we have shown that the latter is p^n. Let ε be maximal with $\zeta_{p^\varepsilon} \in K(\zeta_p)$, i.e., ε is the characteristic number of K in the sense of I, §2. It is well known that ε is finite for $n \geq \varepsilon$, $\mu'(K_n) = \mu_{p^n}(K_n)$. The t-action of G_n on μ_{p^n} is trivial, hence for $n \geq \varepsilon$, $\alpha(\mu'(K_n)) = \alpha(\mu_{p^n}(K_n)) = |\mu_{p^n}(K_n)| = p^n$. Now we show that the proposition also holds for $n < \varepsilon$. In this case, $\mu'(K_n) = \mu_{p^\varepsilon}(K_n)$, and $\gamma(\zeta_{p^\varepsilon}) = \zeta_{p^\varepsilon}^h$ with $h \equiv g \bmod p^n$.

Therefore the action of γ on $T^n(\mu_{p^\varepsilon}(K_n))$ is again raising to the gth power, and again the t-action is trivial on $T^n(\mu_{p^\varepsilon}(K_n))$. One sees also that $T^n(\mu_{p^\varepsilon}(K_n))$ has p^n elements. □

Proposition 3.7. $\alpha(S_n^*) = \alpha(E(K_n)) \cdot p^d$ *with* $d \in \{0, \ldots, 2k\}$ $(k = [K : \mathbb{Q}])$.

Proof. We begin with the exact sequence

$$1 \to E(K_n) \to S_n^* \xrightarrow{v} \mathbb{Z}^{I_n}.$$

Here I_n is the set of prime divisors of p in K_n, and $v = (v_i)_{i \in I_n}$ is the vector of corresponding valuations. G_n operates naturally on I_n such that the sequence is G_n-equivariant. Since $\mathrm{Im}(v)$ is torsion-free, Proposition I1.2 gives us a new exact sequence

$$1 \to A(E(K_n)) \to A(S_n^*) \to A(\mathrm{Im}(v)) \to 0.$$

We have to show that $A(\mathrm{Im}(v))$ has order at most p^{2k}. The trouble is that we do not know $\mathrm{Im}(v)$ precisely. But $\mathrm{Coker}(v)$ is finite (since it embeds into the class group of K_n). By Corollary 2.5, $\alpha(\mathrm{Im}(v)) = \alpha(\mathbb{Z}^{I_n})$, and we can deal with the latter. For this proof, we need to write g_n for g and γ_n for γ. (Thus, we have $G_n = \langle \gamma_n \rangle$, $\gamma_n(\zeta_{p^n}) = (\zeta_{p^n})^{g_n}$.) Let ε be as in the last proof. Then $[K_n : K]$ is a multiple of $p^{n-\varepsilon}$ for $n \geq \varepsilon$. ($[K_n : K_1]$ is exactly $p^{n-\varepsilon}$; see I2.7. That lemma is of course well known in the number-theoretic setting.) Hence g_n cannot be congruent to $1 \bmod p^{\varepsilon+1}$ for $n \geq \varepsilon$. It is an easy exercise to deduce from this that

$$g_n^s \not\equiv 1 \mod p^{\varepsilon+1+[\log_p(s)]} \quad \text{for } s \in \mathbb{N},\ n \geq \varepsilon + 1 + \log_p(s).$$

We need two auxiliary lemmas.

Lemma 3.7.1. $|I_n| \leq k/p^{\varepsilon-1}$, *where* $k = [K : \mathbb{Q}]$.

Proof. We may assume $n \geq \varepsilon$. In the prime factorization of p in K_n, every factor has exponent at least $p^{n-1}(p-1)$ (since $\mathbb{Q}(\zeta_{p^n}) \subset K_n$). Since $[K_n : \mathbb{Q}] = [K_n : K_1][K_1 : \mathbb{Q}] \leq p^{n-\varepsilon} \cdot (p-1) \cdot k$, there can be at most $k/p^{\varepsilon-1}$ distinct factors of p in K_n. □

Lemma 3.7.2. *Let* H *be a factor group of* G_n *with* s *elements. Then* $\alpha(\mathbb{Z}^H) \leq p^{\varepsilon+\log_p(s)}$.

Proof. This is very similar to the proof of Lemma 3.4(b). One has

$$A(\mathbb{Z}^H) \cong A(\mathbb{Z}[H]) \cong \{y \in (\mathbb{Z}/p^n\mathbb{Z})[H] \mid \gamma_n y = g_n y\}$$
$$= \left\{ a_0 \cdot \sum_{i=0}^{s-1} g_n^i \cdot \bar{\gamma}_n^{-i} \mid a_0 \in \mathbb{Z}/p^n\mathbb{Z},\ g_n^s \cdot a_0 = a_0 \right\}.$$

(Note that $\bar{\gamma}_n$ (the image of γ_n in H) is a generator of H.) Since $g_n^s \not\equiv 1 \bmod p^{\varepsilon+1+[\log_p(s)]}$, a_0 can take at most $p^{\varepsilon+[\log_p(s)]}$ different values. □

With these two lemmas, we can finish the proof of 3.7: Decompose I_n into G_n-orbits $J_1, \dots, J_r$. Then J_i is G_n-isomorphic to a factor group H_i of G_n with order $s_i = |J_i|$. Using 3.7.2, we get

$$\alpha(\mathbb{Z}^{I_n}) = \prod_{i=1}^{r} \alpha(\mathbb{Z}^{H_i}) \leq \prod_{i=1}^{r} p^{\varepsilon + \log_p(s_i)} \leq p^{r\cdot\varepsilon} \cdot \prod_{i=1}^{r} s_i .$$

By Lemma 3.7.1, $r\cdot\varepsilon \leq |I_n|\cdot\varepsilon \leq k\cdot p^{1-\varepsilon}\cdot\varepsilon \leq k$. The term Πs_i can be estimated from above by $2^{|I_n|}$ since the sum of the s_i is $|I_n|$. Hence we obtain altogether

$$\alpha(\mathbb{Z}^{I_n}) \leq p^k \cdot 2^{|I_n|} \leq p^k \cdot 2^k \leq p^{2k} . \quad \square$$

Now we can prove Theorem 3.1. From the definition it is clear that $\alpha(E'(K_n)) = \alpha(E(K_n)) \cdot \alpha(\xi^{\mathbb{Z}})$. The G_n-module $\xi^{\mathbb{Z}} \cong \mathbb{Z}$ fits the hypotheses of 3.7.2: Take $H = 1$. Then $\mathbb{Z} \cong \mathbb{Z}^H$ as G_n-module, and we get $1 \leq \alpha(\xi^{\mathbb{Z}}) \leq p^{\varepsilon}$. Hence

$$p^{-\varepsilon} \cdot \alpha(E'(K_n)) \leq \alpha(E(K_n)) \leq \alpha(E'(K_n)) .$$

Inserting Proposition 3.7 in this formula gives

$$p^{-\varepsilon} \cdot \alpha(E'(K_n)) \leq \alpha(S_n^*) \leq p^{2k} \cdot \alpha(E'(K_n)) .$$

By Corollary 3.5 and Proposition 3.6 we have

$$\alpha(E'(K_n)) = p^{n(s+1)} .$$

Putting the last two formulas together gives Theorem 3.1. $\square$

Corollary 3.8. $|\mathrm{NB}(R, C_{p^n})| = |\mathrm{Gal}_0(R, C_{p^n})| = p^{n(s+1)} \cdot O(1)$ *for* $n \to \infty$.

Proof. Combine Theorem 3.1 with Corollary I2.5 (the first $=$ sign is Theorem I3.1). $\square$

Remark 3.9. For $K = \mathbb{Q}$, one finds that $\alpha(\mathbb{Z}^{I_n}) = \alpha(\mathbb{Z}) = 1$, hence we may replace p^{2k} by 1 in the proof of 3.7, i.e., we obtain a sharpened version of the explicit formula in 3.1: $|\mathrm{NB}(R, C_{p^n})| = |\mathrm{Gal}_0(R, C_{p^n})| \leq p^n$. For p a regular prime number, $\mathrm{Pic}(S_n)$ has no p-torsion since the class number h of the p^nth cyclotomic field over $\mathbb{Q}$ is not divisible by p. For these p, we therefore have $P(R, C_{p^n})$ trivial, thus we have as a corollary that $|\mathrm{Gal}(R, C_{p^n})| \leq p^n$. But this is one key step in the proof of the theorem of Kronecker-Weber since it implies that every p-ramified C_{p^n}-extension of $\mathbb{Q}$ is cyclotomic.

4. Normal bases, Leopoldt's conjecture, and $\mathbb{Z}_p$-extensions

In this section we put together some results of the previous sections of this part. Let K, as always, be a number field, and let r and s be as in §1. Let p be an odd prime and $R = \mathcal{O}_K[p^{-1}]$. Let δ be the defect in Leopoldt's conjecture as in §1.

Theorem 4.1. *Leopoldt's conjecture holds for K and p (in short, $\mathrm{LC}(p)$ is valid) if and only if the order of the factor group $\mathrm{Gal}(R, C_{p^n})/\mathrm{NB}(R, C_{p^n})$ remains bounded for $n \to \infty$. This, in turn, happens if and only if for $n \to \infty$, the orders of the groups $T_n(\mathrm{Pic}(S_n))^{tG_n}$ remain bounded.*

Proof. The second statement follows from Theorem I4.1 and the comments preceding it (j': $\mathrm{Gal}(R, C_{p^n})/\mathrm{Gal}_0(R, C_{p^n}) \to T_n(\mathrm{Pic}(S_n))^{tG_n}$ is an isomorphism, and $\mathrm{Gal}_0(R, C_{p^n}) = \mathrm{NB}(R, C_{p^n})$ by Theorem I3.1).

By Corollary 3.8, $|\mathrm{NB}(R, C_{p^n})| = p^{n\cdot(s+1)} \cdot O(1)$. On the other hand, Lemma 1.2 shows that $|\mathrm{Gal}(R, C_{p^n})| = p^{n\cdot(s+1+\delta)} \cdot O(1)$. Thus by dividing the second by the first equation, we obtain

$$|\mathrm{Gal}(R, C_{p^n})/\mathrm{NB}(R, C_{p^n})| = p^{n\cdot\delta} \cdot O(1).$$

(Recall our agreement that $O(1)$ denotes a quantity, dependent on n, contained in an interval $[c, C]$, $0 < c < C < \infty$.) Hence the left-hand side is bounded for $n \to \infty$ if and only if δ is zero. □

The aim of the rest of the section is to reformulate these asymptotic formulas in terms of $\mathbb{Z}_p$-extensions. The following definition would make sense for every commutative ring R, but we always assume $R = \mathcal{O}_K[p^{-1}]$. Choose generators σ_n of C_{p^n} once and for all. Then there are canonical maps $C_{p^m} \to C_{p^n}$, $\sigma_m \mapsto \sigma_n$ for $m \geq n$.

Definition. (a) Let A be an R-algebra on which $\mathbb{Z}_p$ acts by algebra automorphisms. Let $\pi_n: \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z} \cong C_{p^n}$, $1 \mapsto \sigma_n$ be the canonical surjections. Then A is called a *$\mathbb{Z}_p$-extension* if $A_n = A^{\mathrm{Ker}(\pi_n)}$ is a C_{p^n}-extension for all n, and $A = \bigcup A_n$.

(b) A has *normal basis* if all A_n have a normal basis as C_{p^n}-extensions.

Remarks 4.2. (a) There is an obvious notion of isomorphism of $\mathbb{Z}_p$-extensions, and the Harrison product on C_{p^n}-extensions gives us a product on the set of isomorphism classes of $\mathbb{Z}_p$-extensions of R, hence we get an *abelian group* $\mathrm{Gal}(R, \mathbb{Z}_p)$.

(b) The groups $\mathrm{Gal}(R, C_{p^n})$ form a projective system with maps f_n: $\mathrm{Gal}(R, C_{p^{n+1}}) \to \mathrm{Gal}(R, C_{p^n})$, $A \mapsto$ algebra of fixed elements in A under $p^n \cdot C_{p^{n+1}}$. One checks easily that the assignment $A \mapsto (A_n)_{n\in\mathbb{N}}$ defines an isomorphism

$$\alpha: \mathrm{Gal}(R, \mathbb{Z}_p) \to \varprojlim_n (\mathrm{Gal}(R, C_{p^n})).$$

(c) This isomorphism gives another:

$$\mathrm{Gal}(R, \mathbb{Z}_p) \to \varprojlim_n \mathrm{Hom}_{\mathrm{cont}}(\Gamma, C_{p^n}) = \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mathbb{Z}_p).$$

(Γ denotes the absolute Galois group of R in the sense of [16].)

Definition. The group $\mathrm{NB}(R, \mathbb{Z}_p)$ is defined as

$$\mathrm{NB}(R, \mathbb{Z}_p) = \varprojlim_n \mathrm{NB}(R, C_{p^n}).$$

Note that this is a subgroup of $\mathrm{Gal}(R, \mathbb{Z}_p)$ up to isomorphism: Via α, the group $\mathrm{NB}(R, \mathbb{Z}_p)$ is isomorphic to the subgroup of all $A \in \mathrm{Gal}(R, \mathbb{Z}_p)$ which have a normal basis (see part (b) of the definition of $\mathbb{Z}_p$-extension above). Note moreover that $\mathrm{Gal}(R, \mathbb{Z}_p)$ is torsion-free by 4.2(c), hence its subgroup $\mathrm{NB}(R, \mathbb{Z}_p)$ is also torsion-free. Let L' be the composite of all $\mathbb{Z}_p$-extensions of K and $H' = G(L'/K)$. Then

$$\mathrm{Gal}(R, \mathbb{Z}_p) \cong \mathrm{Hom}_{\mathrm{cont}}(\Omega, \mathbb{Z}_p) \cong \mathrm{Hom}_{\mathrm{cont}}(H', \mathbb{Z}_p),$$

and we saw in the proof of Lemma 1.2 that H' is a finitely generated $\mathbb{Z}_p$-module of rank $c(K)$. Hence we have:

Lemma 4.3. $\mathrm{Gal}(R, \mathbb{Z}_p) \cong \mathbb{Z}_p^{c(K)}$ *and* $\mathrm{NB}(R, \mathbb{Z}_p)$ *is finitely generated and free over* $\mathbb{Z}_p$. □

The rest of this section is devoted to a proof of $\mathrm{NB}(R, \mathbb{Z}_p) \cong \mathbb{Z}_p^{s+1}$. For K totally real or a CM field, this result has previously been proved by I. Kersten and J. Michaličeк (see [19, 20]). (The result gives another reformulation of Leopoldt's conjecture: $\mathrm{LC}(K, p)$ holds if and only if $\mathrm{NB}(R, \mathbb{Z}_p)$ has finite index in $\mathrm{Gal}(R, \mathbb{Z}_p)$.) Since the proof is fairly long and difficult, we first give a direct argument for the case $s = 0$. (Recall $s = r_2$ is half the number of complex embeddings of K.)

Theorem 4.4 (Kersten and Michaličeк [20]). *If* K *is totally real, then* $\mathrm{NB}(R, \mathbb{Z}_p) \cong \mathbb{Z}_p$.

Proof. It is well known that the cyclotomic $\mathbb{Z}_p$-extension Z of $\mathbb{Z}[p^{-1}]$ has a normal basis. Z will not become trivial when tensored up to R, hence $M = \mathrm{NB}(R, \mathbb{Z}_p)$ is not zero. Suppose $M \cong \mathbb{Z}_p^d$, $d > 1$. Abbreviate $\mathrm{Gal}(R, \mathbb{Z}_p)$ to X. From 4.2(c) one sees that X/p^nX injects into

$$\mathrm{Hom}_{\mathrm{cont}}(\Omega, \mathbb{Z}/p^n\mathbb{Z}) \cong \mathrm{Gal}(R, C_{p^n}).$$

Hence $M/p^nX \cap M$ injects into $\mathrm{NB}(R, C_{p^n})$. It is elementary module theory over a PID to see that the index of p^nM in $p^nX \cap M$ is bounded uniformly for all n. Hence the size of the kernel of the canonical map $M/p^nM \to \mathrm{NB}(R, C_{p^n})$ is also bounded, i.e., $|\mathrm{NB}(R, C_{p^n})|$ grows (up to a nonzero multiplicative constant) at least as fast as $|M/p^nM| = p^{nd}$. But this contradicts Corollary 3.8 (note $s = 0$). □

Now we prepare for the general case. As in the last proof, let us abbreviate $X = \mathrm{Gal}(R, \mathbb{Z}_p)$, and $M = \mathrm{NB}(R, \mathbb{Z}_p)$. When we say that a quantity which evidently depends on n is *bounded*, we mean that there are positive constants

independent of n which bound it above and below. Let φ_n denote the canonical map from M to $\mathrm{NB}(R, C_{p^n})$. We now formulate two theorems. The second will be the announced result, and the first will be seen to imply the second. The rest of the section is taken up by the proof of the first.

Theorem 4.5. *The orders of the cokernel groups* $\mathrm{Coker}(\varphi_n : M \to \mathrm{NB}(R, C_{p^n}))$ *are bounded.*

Theorem 4.6. M $(= \mathrm{NB}(R, \mathbb{Z}_p))$ *is isomorphic to* $\mathbb{Z}_p^{s+1}$ $(s = r_2$ *in standard notation*).

Proof of the implication 4.5 $\Rightarrow$ 4.6. We have $M \cong \mathbb{Z}_p^t$ for some t. As already used in the proof of 4.4, $\mathrm{Ker}(\varphi_n)$ equals $p^n X \cap M$, and this module can be trapped between $p^n M$ and $p^{n-c} M$ for some constant c independent of n (elementary module theory, or Lemma of Artin-Rees). Hence we have, using 4.5:

$$|\mathrm{NB}(R, C_{p^n})| = |M/\mathrm{Ker}(\varphi_n)| \cdot O(1) = |M/p^n M| \cdot O(1) = p^{n \cdot t} \cdot O(1).$$

Corollary 3.8 immediately gives $t = s + 1$. □

Let us now begin the proof of 4.5. We first consider the following special case:

Assumption. $K = K_1$.

Then $\zeta_p \in K$, and by Lemma I2.7 we may choose the generators γ_n of G_n such that $t(\gamma_n) = (1 + p^\varepsilon) + p^n \mathbb{Z}$, hence also $\gamma_{n+1} \mapsto \gamma_n$ for all n. Here $\varepsilon = \varepsilon_K$ is the characteristic number of K (see I, §2).

Write M_n for $\mathrm{NB}(R, C_{p^n})$. By definition $M = \varprojlim M_n$, and $\pi_n : M \to M_n$ is the nth projection. $M_n' = \bigcap_{m \geq n} \mathrm{Im}(M_m \to M_n)$. Then, as is well known, $\varprojlim M_n = \varprojlim M_n'$. In our case all M_n are finite and every M_n' is of the form $\mathrm{Im}(M_{m(n)} \to M_n)$ for $m(n)$ big enough, and the transition maps of the projective system (M_n') are *surjective*. Hence the projections $M \to M_n'$ are surjective, and it suffices to show the boundedness of the orders $|M_n/M_n'|$, or equivalently of $|\mathrm{Coker}(M_m \to M_n)|$ for all m, n with $m \geq n$.

Lemma 4.7. *Given a short exact sequence of projective systems*

$$0 \to B_n \xrightarrow{i_n} A_n \xrightarrow{\pi_n'} C_n \to 0$$

such that $|\mathrm{Coker}(A_m \to A_n)|$ *is bounded, one has the formula*

$$|\mathrm{Coker}(B_m \to B_n)| = |\mathrm{Ker}(C_m \to C_n)/\pi_m'(\mathrm{Ker}(A_m \to A_n))| \cdot O(1).$$

Proof. This is an immediate consequence of the Snake Lemma. □

We want to apply this to $B_n = M_n$, $A_n = \mathrm{Gal}(R, C_{p^n})$, $C_n = A_n/B_n = P(R, C_{p^n})$. The hypothesis of 4.7 is satisfied since

$$\mathrm{Gal}(R, C_{p^n}) = \mathrm{Hom}_{\mathrm{cont}}(H, C_{p^n}),$$

H as in 1.2, and there we saw that $H \cong$ free $\mathbb{Z}_p$-module $\times$ finite group. Our objective, Theorem 4.5, states: $|\mathrm{Coker}(B_m \to B_n)|$ is bounded. Since $p^n \cdot A_m \subset \mathrm{Ker}(A_m \to A_n)$ and $A_m \to C_m$ is onto, 4.5 will follow with the help of 4.7 once we have shown

Principal Claim. $|\mathrm{Ker}(C_m \to C_n)/p^n C_m|$ is bounded, with $C_n = P(R, C_{p^n})$. (The map $C_m \to C_n$ is induced by the map $\mathrm{Gal}(R, C_{p^m}) \to \mathrm{Gal}(R, C_{p^n})$.)

In the proof of this claim we shall proceed as follows:

(a) We recall that $C_n \cong T_n(\mathrm{Pic}(S_n))^{tG_n}$ by Part I, §4. The isomorphism (called π there) will be denoted π_n for clarity. It depended on the choice of a primitive p^nth root ζ_{p^n}, so let us henceforth assume we have chosen for each n such a root ζ_{p^n}, such that $(\zeta_{p^{n+1}})^p = \zeta_{p^n}$. We figure out what the canonical maps $c_{nm}: C_n \to C_m$ give on the right-hand side $(n \geq m)$. It turns out that $\pi_{n+1} c_{n+1,n} \pi_n^{-1}$ is induced by the usual norm N_{K_{n+1}/K_n} on p-ideal class groups (see Lemma 5.5 below for the details). Therefore we may replace the projective system $(C_\cdot)$ by the projective system $T_\cdot(\mathrm{Pic}(S_\cdot))^{tG_\cdot}$, with the indicated transition maps.

(b) Next, we have to replace the system $T_\cdot(\mathrm{Pic}(S_\cdot))^{tG_\cdot}$ by other ones which are only "almost" isomorphic to it, but simpler to handle. We define a map between projective systems $f_\cdot: X_\cdot \to Y_\cdot$ to be a quasi-isomorphism if the orders of the kernels and cokernels of the f_n are bounded. For a complete definition see §5, where we also give some (basically trivial) lemmas on the behavior of such QI's (= quasi-isomorphisms).

The main result that we will have to use is Lemma 5.4: If $f_\cdot: X_\cdot \to Y_\cdot$ is a QI and $p^n X_n = 0$, $p^n Y_n = 0$ for all $n \in \mathbb{N}$, then the kernels and cokernels of the induced maps

$$f_{nm}: \mathrm{Ker}(X_m \to X_n)/p^n X_m \to \mathrm{Ker}(Y_m \to Y_n)/p^n Y_m$$

are also uniformly bounded for all $m \geq n$. This means in down-to-earth terms: In proving the Principal Claim, we are free to replace $T_\cdot(\mathrm{Pic}(S_\cdot))^{tG_\cdot}$ by any system $D_\cdot$ quasi-isomorphic to it.

(c) By Iwasawa theory, one finds a "good" such system $D_\cdot$.

(d) Proof of the Principal Claim with $D_\cdot$ in the place of $C_\cdot$.

After outlining the program, we only have to supply the details of (c) and (d), since (a) and (b) are covered by the technical results of §5.

Step (c) (*Iwasawa theory*). Let $K_n = \mathrm{Quot}(R_n) = K(\zeta_{p^n})$. We first make an

Assumption. $\zeta_p \in K$ (hence $\in R$), i.e., $K_1 = K$.

Iwasawa theory speaks (among other things) about the structure of the groups $\mathrm{Cl}'(F_n)_{(p)}$, where $F_\infty = \bigcup F_n$ is a $\mathbb{Z}_p$-extension of a number field $F = F_0$, $\mathrm{Cl}'(F_n)$ is the p-class group of F_n (= class group of F_n modulo classes of divisors of p), and the index (p) means: take p-Sylow subgroup. In our case, $K_\infty = \bigcup K_n$ does form a $\mathbb{Z}_p$-extension of $K = K_1$, but the numbering is not

the conventional one (i.e., $[K_n : K] = p^n$ fails to hold). To repair this, recall the following:

In I, §2 we defined $\varepsilon_K = \varepsilon$ (called characteristic number of K) to be the biggest $\varepsilon \in \mathbb{N}$ such that $\zeta_{p^\varepsilon} \in K(\zeta_p)$. By Lemma I2.7, if we let $F_n = K_{n+\varepsilon}$, then the F_n form a $\mathbb{Z}_p$-extension of K with conventional numbering.

Now let $\Lambda = \mathbb{Z}_p[[T]]$, and γ_n be the generator of G_n with $t(\gamma_n) = \overline{(1+p^\varepsilon)}$, i.e., $t(\zeta_{p^n}) = (\zeta_{p^n})^{1+p^\varepsilon}$. Hence $\gamma = \lim(\gamma_n)$ is a topological generator of $\varprojlim G_n \cong \mathbb{Z}_p$. We define a Λ-module structure on $T_n(\mathrm{Pic}(S_n))$ by letting T operate as $\gamma_n - 1$. Then $T_{n+\varepsilon}(\mathrm{Pic}(S_{n+\varepsilon}))^{tG_{n+\varepsilon}}$ is a projective system of Λ-modules of Lemma 5.5.

By [15, Theorem 8] there exists a noetherian torsion Λ-module X' with a submodule of finite index Y' (notation from [15]) such that there is an isomorphism of systems

$$X'/\nu_{n,e}Y' \xrightarrow{\sim} \mathrm{Pic}(S_{n+\varepsilon})_{(p)}.$$

Here e is some auxiliary number depending only on K (actually one could take $e = \varepsilon$), and the $\nu_{n,e}$ are certain explicit elements of Λ (see loc.cit.). It is not explicitly stated in [15] but it is obvious from the definition that $[X' : Y'] < \infty$ (see also [27, p. 280]). The isomorphism respects the transition maps since the transition maps on the right-hand side are induced by the appropriate norms (see Lemma 5.5).

Hence one immediately obtains a quasi-isomorphism (actually injective):

$$(*) \qquad X'/\nu_{n,e}Y' \to \mathrm{Pic}(S_{n+\varepsilon})_{(p)}.$$

By [27, p. 271] or [15] there exists a Λ-module E which is a finite direct sum of modules $\Lambda/(p^{k_i})$ and/or modules $\Lambda/(F_i^{s_i})$ (with $F_i \in \mathbb{Z}_p[T] \subset \Lambda$ irreducible, leading coefficient equalling 1 and all others being in $p\mathbb{Z}_p$), and a Λ-homomorphism $f: E \to Y'$ with finite kernel and cokernel (a so-called Λ-quasi-isomorphism). By Lemma 5.4 and $(*)$, the systems $E/\nu_{n,e}E$ and $\mathrm{Pic}(S_{n+\varepsilon})_{(p)}$ are quasi-isomorphic.

Now we do not want $\mathrm{Pic}(S_{n+\varepsilon})_{(p)}$ itself but rather $T_n(\mathrm{Pic}(S_n))^{tG_n}$ which equals:

$$(**) \qquad \begin{array}{c}\text{annihilator of } \gamma_n - t(\gamma_n) \text{ in} \\ \text{annihilator of } p^{n+\varepsilon} \text{ in } \mathrm{Pic}(S_{n+\varepsilon})_{(p)}.\end{array}$$

Let us abbreviate "annihilator of a in B" by $B[a]$. Using this new notation, and recalling that $\gamma_n - t(\gamma_n)$ operates as $T + 1 - (1+p^\varepsilon)$, we can rewrite the term $(**)$ as

$$\mathrm{Pic}(S_{n+\varepsilon})_{(p)}[p^{n+\varepsilon}][T - p^\varepsilon].$$

By Lemma 5.2 (applied twice), this system is quasi-isomorphic to

$$D_{n+\varepsilon} \stackrel{\mathrm{def}}{=} (E/\nu_{n,e}E)[p^{n+\varepsilon}][T - p^\varepsilon].$$

As was explained under step (b) above, it now suffices to prove the Principal Claim with $D_\cdot$ in the place of $C_\cdot \cong T_\cdot(\mathrm{Pic}(S_\cdot))^{tG_\cdot}$ (step (d) of the program).

Step (d). We can of course assume that E is either $\Lambda/(p^k)$ or $\Lambda/(F^s)$ ($k, s \in \mathbb{N}$, $F \in \mathbb{Z}_p[T]$ as described already). The rest of the proof is a brute force calculation, and not hard.

First case: $E = \Lambda/(p^k)$. We claim that the groups D_n themselves already have bounded order (which of course is much more than we want). We have $E/\nu_{n,e}E = \mathbb{Z}/(p^k)[[T]]/(\nu_{n,e})$, and by [27, p. 280 bottom], $\nu_{n,e}$ is a polynomial with leading coefficient 1, all others in $p\mathbb{Z}$. Hence it is enough to adjoin $[T]$ in the place of $[[T]]$ in the last formula. Moreover, for $k = 1$, the annihilator of $T - p^\varepsilon$ in $\mathbb{Z}/(p)[T]/(\text{any polynomial})$ is at most one-dimensional over $\mathbb{Z}/(p)$. An easy induction over k gives then $|(E/\nu_{n,e}E)[T - p^\varepsilon]| \leq p^k$, which suffices.

Second case: $E = \Lambda/(F^s)$, $F \in \mathbb{Z}_p[T]$ *with leading coefficient* 1, *all others in* $p\mathbb{Z}_p$.

Subcase A: $F \neq T - p^\varepsilon$. As in the first case, we show $|D_n|$ bounded. By working in $\mathbb{Q}_p[T]$, one sees that there exists $g \in \Lambda$ and $c \in \mathbb{N}$ such that $g \cdot (T - p^\varepsilon) \equiv p^c \bmod F^s$. Hence $D_{n+\varepsilon} \subset (E/\nu_{n,e}E)[T - p^\varepsilon] \subset (E/\nu_{n,e}E)[p^c]$, and this has uniformly bounded order since the p-ranks of the $E/\nu_{n,e}E$ remain bounded [27, 13.20].

Subcase B: $F = T - p^\varepsilon$. This is slightly more subtle. By [27, p. 281, formula preceding the second "Therefore"], we have

$$\nu_{n,e}E = p^{n-k} \cdot \nu_{k,e}E \quad \text{for all } n \text{ not less than some fixed } k .$$

This implies that the system of canonical surjections $E/\nu_{n,e}E \to E/p^{n-k}E$ has kernels of order $\leq |E/\nu_{k,e}E|$ (and trivial cokernels, of course). By applying Lemmas 5.2 and 5.4 for a last time, we may replace the projective system $D_{n+\varepsilon}$ by the system $D'_{n+\varepsilon} = (E/p^{n-k}E)[p^{n+\varepsilon}][T - p^\varepsilon]$ (forget about $n < k$). Note that one may delete "$[p^{n+\varepsilon}]$" without effect in the last formula. The point is now that $D'_{n+\varepsilon}$ is *calculable*. It is isomorphic to $((\mathbb{Z}/p^{n-k}\mathbb{Z})[T]/(T - p^\varepsilon)^s)[T - p^\varepsilon]$. Since $T - p^\varepsilon$ is a nonzero divisor in $(\mathbb{Z}/p^{n-k}\mathbb{Z})[T]$, the last expression is the same as $(T - p^\varepsilon)^{s-1}((\mathbb{Z}/p^{n-k}\mathbb{Z})[T]/(T - p^\varepsilon)^s)$, hence a $\mathbb{Z}/p^{n-k}\mathbb{Z}$-direct summand of $(\mathbb{Z}/p^{n-k}\mathbb{Z})[T]/(T - p^\varepsilon)^s$. From this one obtains that $\mathrm{Ker}(D'_{m+\varepsilon} \to D'_{n+\varepsilon})$ is identical with $p^{n-k} \cdot D'_{m+\varepsilon}$. Since $|p^{n-k} \cdot D'_{m+\varepsilon}/p^n \cdot D'_{m+\varepsilon}|$ is bounded (again, the p-rank of $E/\nu_{m,e}$ remains bounded), we have proved the Principal Claim.

This finishes the proof of 4.5 under the Assumption $K = K_1$.

To prove 4.5 without that assumption, a small additional argument is needed. In general, the tower $K \subset K_1 \subset K_2 \subset \cdots$ is not a $\mathbb{Z}_p$-extension, not even after renumbering. But if we let $\widetilde{G}_n = G(K_n/K_1) \subset G_n$, then $\widetilde{G}_n$ is the p-primary part of G_n, and has a unique complement H_n in G_n. Moreover, H_n

is canonically isomorphic to $G(K_1/K) = G_1$. We have

$$\mathrm{Pic}(S_n)[p^n]^{tG_n} = (\mathrm{Pic}(S_n)[p^n]^{t\widetilde{G}_n})^{tH_n}.$$

Now we already know 4.5 holds with K_1 in the place of K (the Assumption holds trivially). Hence the assertion 4.5 holds for the projective system $(\widetilde{C}_n) = (\mathrm{Pic}(S_n)[p^n]^{t\widetilde{G}_n})$, and we have to deduce the same assertion for the projective system $(C_n) = (\widetilde{C}_n^{tH_n})$. Let η_n be a generator of H_n and $h_n = t(\eta_n)$. Then $C_n^{tH_n}$ is exactly the annihilator of $\eta_n - h_n$ in C_n.

Claim. The elements $\eta_n - h_n$ are associated to idempotents e_n in $(\mathbb{Z}/p^n\mathbb{Z})[H_n]$.

Remark. Once they exist, the e_n are obviously unique.

Proof. Let $m = |G_1| = |H_n|$. Then m divides $p-1$, and we have an isomorphism:

$$f_n\colon (\mathbb{Z}/p^n\mathbb{Z})[H_n] \to (\mathbb{Z}/p^n\mathbb{Z})^m$$
$$\eta_n \mapsto (1, h_n, h_n^2, \ldots, h_n^{m-1}).$$

Then $f_n(\eta_n - h_n)$ has 0 in the second position and units in all other positions, because the m first powers of h_n are distinct mod p.

The claim now implies that the projective system (annihilator of $\eta_n - h_n$ in $\widetilde{C}_n$) is a direct summand of the projective system $(\widetilde{C}_n)$ itself. Hence the property 4.5 carries over from $(\widetilde{C}_n)$ to (C_n), and we are done. □

Concluding Remark. The question arises: If one knows that Leopoldt's conjecture is true for K, then what is the index of $\mathrm{NB}(R, \mathbb{Z}_p)$ in $\mathrm{Gal}(R, \mathbb{Z}_p)$? Although $\mathrm{Gal}(R, \mathbb{Z}_p)$ contains many nonfields, it is at least generated (over $\mathbb{Z}_p$) by the $\mathbb{Z}_p$-extensions in the usual sense (i.e., fields). Thus the index is 1 exactly if all field $\mathbb{Z}_p$-extensions of K have a p'-integral normal basis. Suppose now K is imaginary quadratic over $\mathbb{Q}$. Then Leopoldt's conjecture holds for all p, and $\mathrm{Gal}(R, \mathbb{Z}_p)$ is generated by L^+ and L^-, the cyclotomic and anticyclotomic $\mathbb{Z}_p$-extensions of K, for $p = 3$. It was shown by Kersten and Michaličeк [20] and the author [8] that the cyclotomic $\mathbb{Z}_p$-extension always has a p'-integral normal basis (actually, for $[K : \mathbb{Q}] = 2$, $p \neq 2$ this is trivial). Hence the point is what happens to L^-, and based on results of Greenberg [7] and Kersten and Michaličeк (oral communication), one can show that for some K, L^- has no p'-integral normal basis. Moreover, for $K = \mathbb{Q}(\sqrt{-3 \cdot 257})$ the index of $\mathrm{NB}(R, \mathbb{Z}_3)$ in $\mathrm{Gal}(R, \mathbb{Z}_3)$ is precisely $p^1 = 3$.

5. Some auxiliary results

Here we collect some results on quasi-isomorphism of projective systems, as well as an important lemma that was used in §4.

Definition. A (*projective*) *system* is a family $(X_n)_{n\in\mathbb{N}}$ of $\mathbb{Z}$-modules together with mappings $X_{n+1} \to X_n$. There is an obvious notion of *map of projective systems.*

Furthermore, we define:

Definition. (a) If $f_\cdot = (f_n)$ is a map between the systems $X_\cdot$ and $Y_\cdot$, then $f_\cdot$ is a *quasi-isomorphism* (QI for short) if $|\mathrm{Ker}(f_n)|$ and $|\mathrm{Coker}(f_n)|$ are uniformly bounded for all n.

(b) A *double system* $X_{\cdot\cdot}$ is a family of $\mathbb{Z}$-modules X_{nm}, $n \le m$; $n, m \in \mathbb{N}$. (No transition maps between the X_{nm} are requested.) Quasi-isomorphisms of double systems are defined as for systems: $f_{\cdot\cdot}: X_{\cdot\cdot} \to Y_{\cdot\cdot}$ is a QI if $|\mathrm{Ker}(f_{nm})|$ and $|\mathrm{Coker}(f_{nm})|$ are uniformly bounded for all n and m.

We need some basically trivial lemmas on systems and double systems.

Basic Lemma 5.1. (a) *If A and B are $\mathbb{Z}$-modules, $f \in \mathrm{Hom}(A, B)$, $\alpha \in \mathrm{End}(A)$, and $\beta \in \mathrm{End}(B)$ with $f\alpha = \beta f$, then one has for the maps $f': \alpha(A) \to \beta(B)$ and $f'': \mathrm{Coker}(\alpha) \to \mathrm{Coker}(\beta)$, induced by f, the inequalities*

$$|\mathrm{Ker}(f')| \le |\mathrm{Ker}(f)|, \qquad |\mathrm{Coker}(f')| \le |\mathrm{Coker}(f)|,$$
$$|\mathrm{Ker}(f'')| \le |\mathrm{Ker}(f)| \cdot |\mathrm{Coker}(f)|, \qquad |\mathrm{Coker}(f'')| \le |\mathrm{Coker}(f)|.$$

(b) *Under the same hypotheses on A, B, α, β as in* (a), *one has for the map $f^*: \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\beta)$ the inequalities*

$$|\mathrm{Ker}(f^*)|, |\mathrm{Coker}(f^*)| \le |\mathrm{Ker}(f)| \cdot |\mathrm{Coker}(f)|.$$

Proof. (a) is well known (see [15, §3, Lemma 2] or [27, p. 283]). Part (b) is a consequence of (a) using the Snake Lemma. □

Lemma 5.2. *If $f_\cdot: X_\cdot \to Y_\cdot$ is a quasi-isomorphism of systems, and if $\alpha_\cdot: X_\cdot \to X_\cdot$ and $\beta_\cdot: Y_\cdot \to Y_\cdot$ are endomorphisms of systems of $f_\cdot\alpha_\cdot = \beta_\cdot f_\cdot$, then the induced map of systems $f_\cdot^*: \mathrm{Ker}(\alpha_\cdot) \to \mathrm{Ker}(\beta_\cdot)$ is also a QI.*

Proof. The proof follows from 5.1(b). □

Lemma 5.3. *If $f_\cdot: X_\cdot \to Y_\cdot$ is a quasi-isomorphism of projective systems with $p^n X_n = 0$, $p^n Y_n = 0$ for all n, then the induced maps*

$$f_{nm}: \mathrm{Ker}(X_m \to X_n)/p^n X_m \to \mathrm{Ker}(Y_m \to Y_n)/p^n Y_m \qquad (m \ge n)$$

form a quasi-isomorphism of double systems.

Proof. Routine, using 5.1 and again the Snake Lemma. □

Lemma 5.4. *Let $f: D \to E$ be a quasi-isomorphism of Λ-modules such that $D/\nu_{n,e}D$ and $E/\nu_{n,e}E$ are finite for all $n \ge e$. (The meaning of Λ, $\nu_{n,e}$, and "quasi-isomorphism of Λ-modules" was explained in §4.) Then the induced maps $f_n: D/\nu_{n,e}D \to E/\nu_{n,e}E$ are a quasi-isomorphism of systems.*

Proof. Apply 5.1(a) with $A = D$, $B = E$, and α, β given by multiplication with $\nu_{n,e}$. □

We used twice in §4 a property of the system $T_\cdot(\mathrm{Pic}(S_\cdot))^{tG_\cdot}$ which we now prove. Recall from algebraic number theory: For any, say Galois, extension L/K of algebraic number fields, there is (besides the norm $N_{L/K}\colon L^* \to K^*$) also a norm from the ideal group of L to that of K, which also induces a norm map of ideal class groups and p-ideal class groups. All these norm will be written $N_{L/K}$. In our situation, $\mathrm{Pic}(S_n)$ is just the p-class group of K_n $(= \mathrm{Quot}(S_n))$, hence we have norm maps $\mathrm{Pic}(S_m) \to \mathrm{Pic}(S_n)$ for $m \geq n$. On the other hand, since $\mathrm{Gal}(-,-)$ is a bifunctor, the canonical surjection $c\colon C_{p^m} \to C_{p^n}$ $(m \geq n)$ induces a homomorphism $\mathrm{Gal}(c)\colon \mathrm{Gal}(R, C_{p^m}) \to \mathrm{Gal}(R, C_{p^n})$.

Lemma 5.5. *Let K be a number field and $R = \mathscr{O}_K[p^{-1}]$ as always. Let π_n be the map from Kummer theory* (I, §2): $\mathrm{Gal}(R, C_{p^n}) \to \mathrm{Pic}(S_n)$. *Then the following diagram commutes if $[K_{n+1} : K_n] = p$, i.e., for $n \geq \varepsilon_K$:*

$$\begin{array}{ccc} \mathrm{Gal}(R, C_{p^{n+1}}) & \xrightarrow{\pi_{n+1}} & \mathrm{Pic}(S_{n+1}) \\ {\scriptstyle c}\downarrow & & \downarrow{\scriptstyle N_{K_{n+1}/K_n}} \\ \mathrm{Gal}(R, C_{p^n}) & \xrightarrow{\pi_n} & \mathrm{Pic}(S_n) \end{array}$$

Remark. For $0 < n < \varepsilon$ the lemma does not hold, for $n = 0$ it holds.

Proof. First recall that originally π_n depended on a choice of generator σ_n of C_{p^n} and a choice of primitive p^nth rot of 1, ζ_{p^n}; but in §4 these choices have been made once and for all, and consistently, i.e., $\sigma_{n+1} \mapsto \sigma_n$ and $(\zeta_{p^{n+1}})^p = \zeta_{p^n}$.

Let Δ be the kernel of $G_{n+1} \to G_n$.

For A a $C_{p^{n+1}}$-extension of R, let $A' = S_{n+1} \otimes_R A$. Let $\tau = \sigma_{n+1}^{p^n}$, so τ generates $\mathrm{Ker}(C_{p^{n+1}} \to C_{p^n})$. Then A_τ, the fixed subring of τ, represents $\mathrm{Gal}(c)(A)$, the image of $[A]$ in $\mathrm{Gal}(R, C_{p^n})$. Similarly, $\mathrm{Gal}(c)(A') = A'_\tau$. We also need $A''_\tau = S_n \otimes_R A_\tau$. Altogether we have the following algebras and Galois groups:

$$\begin{array}{ccccc} A & & & & A' \\ {\scriptstyle\langle\tau\rangle}\cup & & & & \cup \\ A_\tau & \subset & A''_\tau & \subset & A'_\tau \\ {\scriptstyle C_{p^n}}\cup & & \cup & & \cup \\ R & \underset{G_n}{\subset} & S_n & \underset{\Delta}{\subset} & S_{n+1} \end{array}$$

By definition, abbreviating ζ_{p^n} to ζ and $\zeta_{p^{n+1}}$ to η, we have

$$\pi_{n+1}(A) = \text{class of } (P = A'^{(\sigma_{n+1}-\eta)}) \text{ in } \mathrm{Pic}(S_{n+1}),$$
$$\pi_n(A_\tau) = \text{class of } (P_0 = A''^{(\sigma_n-\zeta)}_\tau) \text{ in } \mathrm{Pic}(S_n).$$

By flatness of S_{n+1} over S_n we get that

$$S_{n+1} \otimes_{S_n} P_0 = A_\tau'^{(\sigma_{n+1}-\zeta)} = A'^{(\sigma_{n+1}-\zeta)},$$

since anything fixed by $\sigma_{n+1} - \zeta$ is already fixed by $\sigma_{n+1}^{p^n} = \tau$. Let $\Delta = \mathrm{Aut}(K_{n+1}/K_n)$ operate on $A' = S_{n+1}A$ via S_{n+1}. For $\delta \in \Delta$, one easily checks

$$\delta(P) = A'^{(\sigma_{n+1} - \delta(\eta))}.$$

Hence with $\nu = \sum_{\delta\in\Delta} \delta$:

$$\begin{aligned} P^\nu &= \prod_{\delta\in\Delta} A'^{(\sigma_{n+1}-\delta(\eta))} \\ &= A'^{(\sigma_{n+1}-z)}, \qquad z = \prod_{\delta\in\Delta} \delta(\eta) = \eta^\nu \text{ (by Kummer theory)} \\ &= A'^{(\sigma_{n+1}-\eta^p)} \quad \left(\text{since } \sum_{\delta\in\Delta} t(\delta) = 1 + (1+p^n) + \cdots + (1+(p-1)p^n)\right. \\ &\qquad \left. = p \bmod p^{n+1} \ (p \text{ is not } 2!)\right) \\ &= S_{n+1}P_0 \quad \text{by the above calculation.} \end{aligned}$$

On the other hand, if we write $P = xI$, $x \in P$, I a fractional ideal of S_{n+1}, we get

$$\begin{aligned} P^\nu &= x^\nu \cdot \prod_{\delta\in\Delta} \delta(I) \\ &= x^\nu \cdot N_{K_{n+1}/K_n}(I) \cdot S_{n+1} \quad \text{by definition of the ideal norm.} \end{aligned}$$

Hence $S_{n+1} \cdot P_0 = x^\nu \cdot N(I) \cdot S_{n+1}$ (omitting subscripts) and x^ν is already in K_n, so $N(I)$ agrees with the fractional S_n-ideal $P_0 x^{-\nu}$, and we are done. □

Note added in proof. The descent technique of §I.2 actually goes back to H. Miki in the field case. See H. Miki, *On $\mathbb{Z}_p$-extensions of complete p-adic power series fields and function fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **21** (1974), 377–393.

References

1. E. Artin, *Über Einheiten relativ galoisscher Zahlkörper*, J. Math. **167** (1931) 153–156; Gesammelte Werke, pp. 197–200.
2. A. Borevich, *Kummer extensions of rings*, J. Soviet Math. **11** (1979), 514–534.
3. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton Univ. Press, Princeton, N. J., 1956.
4. S. U. Chase, D. K. Harrison, and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965) (reprinted with corrections 1968).
5. L. Childs, *The group of unramified Kummer extensions of prime degree*, Proc. London Math. Soc. **35** (1977), 407–422.
6. ____, *Cyclic Stickelberger cohomology and descent of Kummer extensions*, Proc. Amer. Math. Soc. **90** (1984), 505–510.

7. R.Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.
8. C. Greither, *Cyclic Galois extensions and normal bases*, Habilitationsschrift, Universität München, 1988.
9. ____, , *Cyclic extensions and normal bases*, Proc. Internat. Number Theory Conference (Quebec 1987), De Gruyter, 1989, pp. 322–329.
10. C. Greither and R. Miranda, *Galois extensions of prime degree*, J. Algebra **124** (1989), 354–366.
11. R. Haggenmüller, *Über Invarianten separabler Galoiserweiterungen kommutativer Ringe*, Dissertation, Universität München, 1979.
12. ____, *Über die Gruppe der Galoiserweiterungen vom Primzahlgrad*, Habilitationsschrift, Universität München, 1985.
13. D. K. Harrison, *Abelian extensions of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965) (reprinted with corrections 1968).
14. H. Hasse, *Die Multiplikationsgruppe der abelschen Körper mit fester Galoisgruppe*, Abh. Math. Sem. Univ. Hamburg **16** (1949), 29–40.
15. K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.
16. G. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. **122** (1966), 461–479.
17. I. Kersten, *Eine neue Kummertheorie für zyklische Galoiserweiterungen vom Grad p^2*, Algebra-Bericht Nr. 45, Fischer, München, 1983.
18. I. Kersten and J. Michaliček, *Kummer theory without roots of unity*, J. Pure Appl. Algebra **50** (1988), 21–72.
19. ____, *On Γ-extensions of totally real and complex multiplication fields*, Math. Rep. Acad. Sci. Canada **9** (1987), 309–314.
20. ____, *$\mathbb{Z}_p$-extensions of complex multiplication fields*, Ber. Math. Sem. Univ. Hamburg Ser. A **1** (1987).
21. M.-A. Knus and M. Ojanguren, *Théorie de la déscente et algèbres d'Azumaya*, Lecture Notes in Math., vol. 389, Springer, 1974.
22. H.-W. Leopoldt, *Zur Arithmetik in abelschen Zahlkörpern*, J. Reine Angew. Math. **209** (1962), 54–71.
23. S. Mac Lane, *Homology*, Grundlehren der Math. Wiss., no. 114, Springer, 1963.
24. A. S. Merkurjev, *On the structure of Brauer groups of fields*, Math. USSR Izv. **27** (1986), no. 1, 141–157.
25. D. Saltman, *Generic Galois extensions and problems in field theory*, Adv. in Math. **43** (1982), 250–283.
26. S. Wang, *A counterexample to Grunwald's theorem*, Ann. of Math. (2) **49** (1948), 1008–1009.
27. L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math., no. 83, Springer, 1982.

MATHEMATISCHES INSTITUT DER UNIVERSITÄT MÜNCHEN, THERESIENSTRASSE 39, 80000 MÜNCHEN 2, FEDERAL REPUBLIC OF GERMANY