Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 52 (1977)

Artikel: On the projective class group of cyclic groups of prime power order.
Autor: Kervaire, M.A. / Pavaman Murthy, M.
DOI: https://doi.org/10.5169/seals-40007

Comment. Math. Helvetici **52** (1977) 415–452 Birkhäuser Verlag, Basel

On the projective class group of cyclic groups of prime power order

MICHEL A. KERVAIRE and M. PAVAMAN MURTHY

Let C_q denote the cyclic group of order q and $\mathbf{Z}C_q$ the integral group ring of C_q. If q is a prime, $q=p$ say, D. S. Rim [18] has proved that the projective class group $\tilde{K}_0(\mathbf{Z}C_p)$ is isomorphic to $\tilde{K}_0(\mathbf{Z}[\zeta])$, where ζ denotes a primitive p-th root of unity. In turn, it is well known that $\tilde{K}_0(\mathbf{Z}[\zeta])$ is isomorphic to the ideal class group of the ring $\mathbf{Z}[\zeta]$ of integers in the cyclotomic field $F_0=\mathbf{Q}(\zeta)$. See J. Milnor's book [17], §1, Corollary 1.11.

In this paper we study $\tilde{K}_0(\mathbf{Z}C_q)$ for $q=p^{n+1}$, where p is a prime number.

For instance, we obtain in §6 the following result. Let $C(F_n)$ denote the ideal class group of the cyclotomic field $F_n=\mathbf{Q}(\zeta_n)$, where ζ_n is a primitive p^{n+1}-st root of unity. If p is a semi-regular odd prime, there is an exact sequence

$$0\to(\tfrac{1}{2}(p-3)+\delta_p)\cdot\mathbf{Z}/p\mathbf{Z}\to\tilde{K}_0(\mathbf{Z}C_{p^2})\to C(F_0)\times C(F_1)\to 0.$$

Here, $N\cdot\mathbf{Z}/p\mathbf{Z}$ stands for the direct product of N copies of the group $\mathbf{Z}/p\mathbf{Z}$ of integers mod p, and δ_p is the number of Bernoulli numbers among $B_2, B_4, \ldots, B_{p-3}$ whose numerator (in reduced form) is divisible by p.

Recall that a prime p is *semi-regular* if it does not divide the order of the ideal class group of the maximal real subfield $F_0^+=\mathbf{Q}(\zeta_0+\zeta_0^{-1})$ in F_0.

Remark. It is an old conjecture that possibly every prime is semi-regular. This conjecture has been verified for $p\leqq 4001$ and for these primes a list of the Bernoulli numbers B_{2a} with $2\leqq 2a\leqq p-3$ whose numerator is divisible by p can be found in [4], pages 430, 431. As shown by the tables, the number δ_p oscillates between 0 and 3 for $p\leqq 4001$. The first prime p for which δ_p is non-zero is 37. According to the table, $\delta_p=1$ for $p=37$, 59, 67, 101, 103, 131, 149 and $\delta_p=0$ for all other primes $p\leqq 151$. Then, $\delta_p=2$ for $p=157$. Finally $\delta_p=3$, the maximum value of δ_p for $p\leqq 4001$, if $p=491$, 617, 1151, 1217, 1811, 1847, 2939 and 3833. It is known that there exist infinitely many primes with $\delta_p\neq 0$. See [4], Theorem 2, page 381.

Dedicated to Beno Eckmann on the occasion of his sixtieth birthday.

The surjective map

$$i_*: \tilde{K}_0(\mathbf{Z}C_{p^2}) \to \tilde{K}_0(\mathbf{Z}[\zeta_0]) \times \tilde{K}_0(\mathbf{Z}[\zeta_1]) = C(F_0) \times C(F_1)$$

in the above exact sequence is induced by the natural inclusion

$$i: \mathbf{Z}C_{p^2} \to \mathbf{Z} \times \mathbf{Z}[\zeta_0] \times \mathbf{Z}[\zeta_1]$$

of $\mathbf{Z}C_{p^2}$ into the maximal order of $\mathbf{Q}C_{p^2} = \mathbf{Q} \times \mathbf{Q}(\zeta_0) \times \mathbf{Q}(\zeta_1)$.

For arbitrary odd prime p, we prove that $\operatorname{Ker} i_*$ maps surjectively onto $\frac{1}{2}(p-3) \cdot \mathbf{Z}/p\mathbf{Z}$ and hence, at any rate, the order of $\operatorname{Ker} i_*$ is at least $p^{(1/2)(p-3)}$. Thus, for a prime $p \geqq 5$, there exist projective modules over the group ring $\mathbf{Z}C_{p^2}$ which become free over $\mathbf{Z}[\zeta_0]$ and $\mathbf{Z}[\zeta_1]$, under the natural maps $\mathbf{Z}C_{p^2} \to \mathbf{Z}[\zeta_\nu]$, $\nu = 0, 1$, but which are not even stably free as $\mathbf{Z}C_{p^2}$-modules.

For larger values of n, there still is a surjective map

$$i_*: \tilde{K}_0(\mathbf{Z}C(p^{n+1})) \to \prod_{\nu=0}^{n} \tilde{K}_0(\mathbf{Z}[\zeta_\nu]),$$

where ζ_ν is a primitive $p^{\nu+1}$-st root of unity, $C(p^{n+1})$ denotes the cyclic group of order p^{n+1}, and $\tilde{K}_0(\mathbf{Z}[\zeta_\nu])$ is isomorphic to the ideal class group $C(F_\nu)$ of the cyclotomic field $F_\nu = \mathbf{Q}(\zeta_\nu)$.

We shall see that the kernel W_n of i_* is an abelian p-group. Writing w_n for the exponent of p in the order of W_n, we shall find:

For p an odd prime number,

$$w_n \geqq \frac{1}{2}\left\{\frac{p^{n+1}-1}{p-1} - (n+1)^2\right\},$$

with equality if p is a *regular prime*, i.e. if $\delta_p = 0$ or equivalently, if p does not divide the class number of $F_0 = \mathbf{Q}(\zeta_0)$.

For $p = 2$, which is a regular prime, the group W_n is an abelian 2-group of order 2 to the power

$$w_n = 2^n - n(n+1)/2 - 1.$$

More complete information on W_n is given at the end of §1 and in §5, §6. The bulk of the proofs is contained in §§2–4.

The projective class group $\tilde{K}_0(\mathbf{Z}C_{15})$ is studied in §7. The result is in sharp contrast with the prime power order case.

Remark. On the occasion of a talk given by one of us at Princeton University in the Fall 1969, where the results of this paper have been presented, we were informed by S. Ullom that A. Frölich had already proved that W_n is a p-group and produced some lower bound for its order. (See [5], Part I.) Furthermore, the appearance of terms like $\mathbf{Z}/2\mathbf{Z}$ in $\tilde{K}_0(\mathbf{Z}C_{15})$ had also been observed by S. Ullom in certain $\tilde{K}_0(\mathbf{Z}C(2p^n))$. (Compare Prop. 3 in [20].) Finally, comparable results have been obtained by S. Galovich in his thesis [6].

§1. A fibre product

Let Λ be a ring with identity element and let I, J be two-sided ideals of Λ. We shall consider fibre products which are diagrams of rings as follows

$$\begin{array}{ccc} \Lambda/I\cap J & \longrightarrow & \Lambda/J \\ \downarrow & & \downarrow \\ \Lambda/I & \longrightarrow & \Lambda/I+J. \end{array}$$

J. Milnor has proved that such a diagram yields an exact sequence in K-theory known as the Milnor–Mayer–Vietoris sequence. We only need the following portion of it

$$\begin{aligned} &K_1(\Lambda/I)\times K_1(\Lambda/J)\to K_1(\Lambda/I+J)\to K_0(\Lambda/I\cap J)\\ &\quad\to K_0(\Lambda/I)\times K_0(\Lambda/J)\to K_0(\Lambda/I+J). \end{aligned}$$

(See J. Milnor [17] or H. Bass [2, Chap. VII, §4].)

We shall use this sequence in the case where the ring $R=\Lambda/I+J$ satisfies the following hypothesis:

The free R-modules R^m and R^n are isomorphic if and only if $m=n$.

Then, the map $K_0(\mathbf{Z})=\mathbf{Z}\to K_0(R)$ is injective, and one can replace K_0 by $\tilde{K}_0=K_0/\mathrm{Im}\,K_0(\mathbf{Z})$ in the above Milnor–Mayer–Vietoris sequence.

We study the following special case: Let $\Lambda=\mathbf{Z}[X]$ be the polynomial ring in one variable X over the ring of integers. Take $I=(X^{p^n}-1)$ and $J=(1+X^{p^n}+\cdots+X^{(p-1)p^n})$.

One verifies easily that $I\cap J=(X^{p^{n+1}}-1)$. Observing that the polynomial generating the ideal J is the cyclotomic polynomial whose roots are the primitive

p^{n+1}-st roots of unity, we get the fibre product diagram

$$\begin{array}{ccc} \mathbf{Z}[X]/(X^{p^{n+1}}-1) & \xrightarrow{i_2} & \mathbf{Z}[\zeta_n] \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ \mathbf{Z}[X]/(X^{p^n}-1) & \xrightarrow{j_1} & \mathbf{F}_p[x]/(x^{p^n}-1), \end{array}$$

where $i_2(X)=\zeta_n$, $j_2(\zeta_n)=x$ and $j_1(X)=x$.

Set $R_n=\mathbf{F}_p[x]/(x^{p^n}-1)$ and write $t=x-1$. Then, $x^{p^n}-1=t^{p^n} \bmod p$ and so $R_n=\mathbf{F}_p[t]/(t^{p^n})$ is a local ring with maximal ideal $T=(t)$. It is elementary to show that

$$\tilde{K}_0(R_n)=0,$$

and $\det: K_1(R_n)\to U(R_n)$ is an isomorphism, where det is induced by the determinant map $GL(R_n)\to U(R_n)$ and $U(R_n)$ denotes the group of invertible elements in R_n.

Since $\det: K_1(A)\to U(A)$ is (split) surjective for every commutative ring A with identity element, we can replace the above sequence by

$$U(\mathbf{Z}C(p^n))\times E_n \xrightarrow{j} U(R_n) \longrightarrow \tilde{K}_0(\mathbf{Z}C(p^{n+1})) \xrightarrow{i} \tilde{K}_0(\mathbf{Z}C(p^n)) \times \tilde{K}_0(\mathbf{Z}[\zeta_n]) \longrightarrow 0.$$

where $E_n=U(\mathbf{Z}[\zeta_n])$, and $C(p^n)$ is the cyclic group of order p^n.

Of course this is a special case of the general exact sequence involving Picard groups considered in [2, Chap. IX, §3] and [3].

The main problem is thus to evaluate the cokernel V_n of the map

$$j: U(\mathbf{Z}C(p^n))\times E_n \to U(R_n).$$

We then have the exact sequence

$$0\to V_n \to \tilde{K}_0(\mathbf{Z}C(p^{n+1}))\to \tilde{K}_0(\mathbf{Z}C(p^n))\times \tilde{K}_0(\mathbf{Z}[\zeta_n])\to 0$$

which gives us a hold on $\tilde{K}_0(\mathbf{Z}C(p^{n+1}))$ by induction on n, starting with D. S. Rim's theorem for $n=0$.

In the calculation of V_n a decisive rôle will be played by the action of the Galois group $G_n=\mathrm{Gal}\,(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ on the various rings involved.

Let $\kappa: G_n \to U(\mathbf{Z}/p^{n+1}\mathbf{Z})$ be the usual canonical isomorphism defined by $s(\zeta_n) = \zeta_n^{\kappa(s)}$, $s \in G_n$. We write x indifferently for the generator corresponding to X in $\mathbf{Z}[X]/(X^{p^{n+1}}-1) = \mathbf{Z}C(p^{n+1})$, $\mathbf{Z}[X]/(X^{p^n}-1) = \mathbf{Z}C(p^n)$ and $\mathbf{F}_p[X]/(X^{p^n}-1) = R_n$. If $s \in G_n$, then $\kappa(s)$ is an integer mod p^{n+1}, prime to p, and so $x^{\kappa(s)}$ makes good sense, whether we view x as generator of $C(p^{n+1})$, $C(p^n)$ or as an element of R_n.

The formula $s(x) = x^{\kappa(s)}$ turns $G_n = \mathrm{Gal}\,(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ into a group of automorphisms of the rings $\mathbf{Z}C(p^{n+1})$, $\mathbf{Z}C(p^n)$ and R_n. Moreover, the maps in the diagram

$$\begin{array}{ccc} \mathbf{Z}C(p^{n+1}) & \xrightarrow{i_2} & \mathbf{Z}[\zeta_n] \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ \mathbf{Z}C(p^n) & \xrightarrow{j_1} & R_n \end{array}$$

all commute with the action of G_n.

Now, the Milnor–Mayer–Vietoris sequence associated with a fibre product is natural with respect to maps of fibre products. The exact sequence

$$0 \to V_n \to \tilde{K}_0(\mathbf{Z}C(p^{n+1})) \to \tilde{K}_0(\mathbf{Z}C(p^n)) \times \tilde{K}_0(\mathbf{Z}[\zeta_n]) \to 0$$

thus becomes a sequence of G_n-modules.

In particular, let $c \in G_n$ be complex conjugation. Because $c(\zeta_n) = \bar{\zeta}_n = \zeta_n^{-1}$, it follows that on $\mathbf{Z}C(p^{n+1})$, $\mathbf{Z}C(p^n)$ and R_n, the operation of c is determined by $c(x) = x^{-1}$.

If M is a multiplicative G_n-module, we denote by M^+ the submodule of M consisting of elements $v \in M$ such that $c(v) = v$. Similarly, $M^- = \{v \in M \mid c(v) = v^{-1}\}$. Observe that if M is a finite abelian group of odd order then $M = M^+ \times M^-$.

Our main result is the following.

THEOREM 1.1. *Let* $U_n = U(R_n)$, $U_n^+ = \{u \in U_n \mid c(u) = u\}$, *and* $X_n \subset U_n$ *be the cyclic subgroup generated by* $x = 1 + t$, *where* $R_n = \mathbf{F}_p[t]/(t^{p^n})$, $n \geqq 1$.

For $p = 2$, $V_n = V_n^- \cong U_n/X_n \cdot U_n^+$.

For p an odd prime $V_n = V_n^+ \times V_n^-$, *and if p is semi-regular, then*

$$V_n^- \cong U_n/X_n \cdot U_n^+,$$

and

$$\mathrm{Char}\,(V_n^+) \subseteqq S^-(F_{n-1}) = S(F_{n-1}),$$

by a canonical injection, where $F_\nu = \mathbf{Q}(\zeta_\nu)$ *and* $S(F_\nu)$ *is the p-primary component of the ideal class group of* F_ν.

If the prime p is not known to be semi-regular, there is a surjective map of V_n *onto* $U_n/X_n \cdot U_n^+$.

An elementary calculation carried through in §2 yields the structure of $U_n/X_n \cdot U_n^+$. This group looks like this:

For $p=2$, $U_n/X_n \cdot U_n^+$ is the direct product for $\nu = 1, \ldots, n-2$ of $2^{n-\nu-2}$ copies of $\mathbf{Z}/2^\nu\mathbf{Z}$. In formula:

$$U_n/X_n \cdot U_n^+ = \prod_{\nu=1}^{n-2} 2^{n-\nu-2} \cdot \mathbf{Z}/2^\nu\mathbf{Z}.$$

For p an odd prime number, the formula reads

$$U_n/X_n \cdot U_n^+ = \prod_{\nu=1}^{n-1} \tfrac{1}{2}(p-1)^2 p^{n-\nu-1} \cdot \mathbf{Z}/p^\nu\mathbf{Z} \times \tfrac{1}{2}(p-3) \cdot \mathbf{Z}/p^n\mathbf{Z}.$$

We also get in Lemmas 2.1 and 2.2 an explicit description of the generators.

Remark. Iwasawa and Sims [15, page 92] have proved that for $p \leqq 4001$, the group $S^-(F_{n-1})$ is given by $S^-(F_{n-1}) \cong \delta_p \cdot \mathbf{Z}/p^n\mathbf{Z}$.

On the other hand, for $n=1$, we shall prove in §6 by a direct calculation that

$V_1^+ \cong \delta_p \cdot \mathbf{Z}/p\mathbf{Z}$ *for every semi-regular prime.*

It seems natural to conjecture that perhaps

$$\text{Char}\,(V_n^+) = S^-(F_{n-1}) \cong \delta_p \cdot \mathbf{Z}/p^n\mathbf{Z}$$

for all semi-regular primes and all $n \geqq 1$?

If p is a regular prime, e.g. $p=2$, then $S^-(F_n)=0$ for all $n \geqq 0$ and the above theorem determines $V_n = V_n^-$ completely. Its order is easily computed to be p to the power v_n, where

$$v_n = \tfrac{1}{2}(p^n-1) - n \quad \text{for} \quad p \text{ odd},$$

and

$$v_n = 2^{n-1} - n \qquad \text{for} \quad p=2.$$

Successive application of Theorem 1.1 to $\mathbf{Z}C(p^{n+1})$, $\mathbf{Z}C(p^n), \ldots, \mathbf{Z}C(p^2)$ and Rim's theorem gives

THEOREM 1.2. *Let p be a regular prime. The inclusion of $\mathbf{Z}C(p^{n+1})$ into the maximal order $\mathbf{Z} \times \prod_{\nu=0}^{n} \mathbf{Z}[\zeta_\nu]$ of $\mathbf{Q}C(p^{n+1})$ induces the exact sequence*

$$0 \to W_n \to \tilde{K}_0(\mathbf{Z}C(p^{n+1})) \to \prod_{\nu=0}^{n} \tilde{K}_0(\mathbf{Z}[\zeta_\nu]) \to 0,$$

where W_n is an abelian p-group with a filtration

$$W_n = H_1 \supset H_2 \supset \cdots \supset H_n \supset H_{n+1} = 0,$$

such that $H_m/H_{m+1} \cong V_m$ as given by the above formulas.

The proof is immediate. If $p_m : \tilde{K}_0(\mathbf{Z}C(p^{n+1})) \to \tilde{K}_0(\mathbf{Z}C(p^m))$ denotes the homomorphism induced by the obvious projection for $m = 1, \ldots, n+1$, define $H_m = W_n \cap \operatorname{Ker}(p_m)$. The isomorphism $H_m/H_{m+1} \cong V_m$ is induced by $p_{m+1} \mid H_m$. The map $H_m/H_{m+1} \to V_m$ thus obtained is clearly injective. Surjectivity follows easily from the surjectivity of $\tilde{K}_0(\mathbf{Z}C(p^{\nu+1})) \to \tilde{K}_0(\mathbf{Z}C(p^\nu)) \times \tilde{K}_0(\mathbf{Z}[\zeta_\nu])$.

This theorem provides, after a short computation, the order of W_n as asserted in the introduction.

The structure of W_n is determined, at least in principle, in §5. For $n \geqq 2$ and $p \geqq 5$ ($n \geqq 3$ for $p = 3$), it is definitely not the direct product of $V_1, \ldots, V_n$.

As an illustration, the following is a corollary of our methods.

THEOREM 1.3. *Let p be a regular prime and $C(p^n)$ denote the cyclic group of order p^n. Then, the natural map on units*

$$i_1 : U(\mathbf{Z}C(p^{n+1})) \to U(\mathbf{Z}C(p^n))$$

is surjective for all n.

Proof. Let $u \in U(\mathbf{Z}C(p^n))$. Denoting by x a generator of $C(p^n)$, we have $u = x^i \cdot v$, where v is symmetric, i.e. invariant under the involution $(x \mapsto x^{-1})$. Thus, with the notations of Theorem 1.1, $j_1(u) \in X_n \cdot U_n^+$, where j_1 is the map in the diagram

$$\begin{array}{ccc} U(\mathbf{Z}C(p^{n+1})) & \xrightarrow{i_2} & E_n \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle j_2} \\ U(\mathbf{Z}C(p^n)) & \xrightarrow{j_1} & U_n. \end{array}$$

By Theorem 4.1, j_2 is surjective on symmetric elements if p is a regular prime. Since the diagram comes from a fibre product, it follows that i_1 is surjective.

Remark. In §6 we will show that $j_1(U(\mathbf{Z}C_p)) \subset j_2(E_1)$ if p is semi-regular. It thus follows that

$$i_1 : U(\mathbf{Z}C(p^2)) \to U(\mathbf{Z}C(p))$$

is still surjective for p only semi-regular. However, we do not know whether surjectivity of $U(\mathbf{Z}C(p^{n+1})) \to U(\mathbf{Z}C(p^n))$ holds for $n \geqq 2$ under the weaker regularity hypothesis on p.

§2. The unit group of the ring $R_n = \mathbf{F}_p[x]/(x^{p^n} - 1)$

We set $t = x - 1 \in R_n$ and observe that $R_n = \mathbf{F}_p[t]/(t^{p^n})$. The group $U(R_n)$ of units of R_n, which consists of (truncated) polynomials in t with non-vanishing constant term, splits as a direct product

$$U(R_n) = \mathbf{F}_p^* \times U_n^{(1)},$$

where $U_n^{(1)}$ is the subgroup of $U(R_n)$ consisting of the units congruent to 1 mod tR_n. Set $T = tR_n$, the maximal ideal of R_n. The subgroups $U_n^{(i)} = 1 + T^i$, $i \geqq 1$, filter $U(R_n)$ and the map $T^i \to 1 + T^i$ given by $f \to 1 + f$ induces an isomorphism $T^i/T^{i+1} \cong U_n^{(i)}/U_n^{(i+1)}$ for $i \geqq 1$. With a minor change of notation from the preceding section, we set $U_n = U_n^{(1)}$. Then, since t^i-generates T^i/T^{i+1}, it follows that

Any set of elements $\xi_i \in U(R_n)$, $i = 1, \ldots, p^n - 1$ *satisfying*

$$\xi_i = 1 + t^i \bmod T^{i+1}$$

is a set of generators of U_n.

We repeat some notation. Let $c : R_n \to R_n$ be the $\mathbf{F}_p$-automorphism determined by $c(x) = x^{-1}$. A unit $u \in U(R_n)$ such that $c(u) = u$ will be called a symmetric unit. We denote by U_n^+ the subgroup of U_n consisting of symmetric units. Also, let X_n be the subgroup of U_n generated by $x = 1 + t$.

In the next two sections we shall prove e.g. that if p is a regular prime number, then

$$\mathbf{F}_p^* \times X_n \cdot U_n^+ = \mathrm{Im}\{j : U(\mathbf{Z}C(p^n)) \times E_n \to U(R_n)\}.$$

In this paragraph we determine the structure of

$$U_n/X_n \cdot U_n^+ \cong U(R_n)/\mathbf{F}_p^* \times X_n \cdot U_n^+.$$

Set $\alpha_i = 1+t^i$ for $i = 1, \ldots, p^n - 1$ and let γ_i be the class of α_i in $U_n/X_n \cdot U_n^+$.

LEMMA 2.1. *If p is an odd prime, then the elements γ_{2i+1} with $1 \leqq i \leqq \frac{1}{2}(p^n-3)$ and $2i+1$ prime to p form an independent set of generators of $U_n/X_n \cdot U_n^+$. The order of γ_{2i+1} is p^{a_i}, where a_i is uniquely determined by the inequalities*

$$p^{n-a_i} \leqq 2i+1 < p^{n-a_i+1}.$$

Proof. Consider the symmetric elements $s = x + x^{-1} - 2 = x^{-1}t^2$ and $\sigma_i = 1 + s^i \in U_n^+$ for $i = 1, \ldots, \frac{1}{2}(p^n-1)$. Since $\alpha_{2i+1} = 1 + t^{2i+1}$ and $\sigma_i = 1 + t^{2i} \bmod T^{2i+1}$, it follows by a remark above that the set $\{\alpha_{2i+1}, \sigma_{i+1}\}$ with $i = 0, 1, \ldots, \frac{1}{2}(p^n-3)$ generates U_n. Since $\alpha_1 = 1 + t = x \in X_n$ and $\sigma_{i+1} \in U_n^+$, the set $\{\gamma_{2i+1}\}$ with $i = 0, 1, \ldots, \frac{1}{2}(p^n-3)$ generates $U_n/X_n \cdot U_n^+$. Since further $\alpha_{(2i+1)p} = (\alpha_{2i+1})^p$, the subset of $\{\gamma_{2i+1}\}$ with $2i+1$ prime to p suffices to generate $U_n/X_n \cdot U_n^+$.

Now, α_{2i+1} is of order p^{a_i} in U_n, where $p^{n-a_i} \leqq 2i+1 < p^{n-a_i+1}$. Hence, the order of γ_{2i+1} divides p^{a_i}.

To show that the order of γ_{2i+1} is precisely p^{a_i} and moreover that $\gamma_3, \gamma_5, \ldots, \gamma_{p^n-1}$ with indices prime to p form an independent set of generators of $U_n/X_n \cdot U_n^+$, it suffices to check that $|U_n/X_n \cdot U_n^+| = \prod_i p^{a_i}$, where the product extends over $i = 1, 2, \ldots, \frac{1}{2}(p^n-1)$ with $2i+1$ prime to p, and $|U_n/X_n \cdot U_n^+|$ denotes the cardinality of the set $U_n/X_n \cdot U_n^+$.

It is easily checked that $|U_n/X_n \cdot U_n^+| = |U_n|/|X_n| \cdot |U_n^+| = p^{(1/2)(p^n-1)-n}$. (Recall that p is an odd prime.) On the other hand, for given a, the set of possible indices i such that $a_i = a$, i.e. the set $\{i \mid p^{n-a} \leqq 2i+1 < p^{n-a+1}\}$ contains $\frac{1}{2}(p-1)p^{n-a}$ integers for $a < n$ and $\frac{1}{2}(p-3)$ for $a = n$. Among these, there are $\frac{1}{2}(p-1)p^{n-a-1}$ multiples of p except if $a = n$, in which case there are none. Consequently, setting $p^{v_n} = \prod_i p^{a_i}$, we have

$$v_n = \sum_{a=1}^{n-1} a \cdot \tfrac{1}{2}(p-1)^2 p^{n-a-1} + n \cdot \tfrac{1}{2}(p-3).$$

We leave to the reader the verification that $v_n = \frac{1}{2}(p^n-1) - n$.

The case $p = 2$ is somewhat more complicated. Keeping the notation $\alpha_i = 1 + t^i$ and γ_i for the class of α_i in $U_n/X_n \cdot U_n^+$, we have the following lemma.

LEMMA 2.2. *If $p=2$, the elements γ_{4i+1} with $i=1,2,\ldots,2^{n-2}-1$ form an independent set of generators of $U_n/X_n\cdot U_n^+$. The order of γ_{4i+1} is 2^{a_i}, where a_i is uniquely determined by the inequalities*

$$2^{n-a_i}\leqq 4i+1<2^{n-a_i+1}.$$

Proof. Again, let $s=x+x^{-1}=x^{-1}t^2$ and set $\sigma_k=1+s^k$. We first prove that $\{\alpha_{4i+1},\sigma_{2i+1}\}$ with $i=0,1,\ldots$ is a set of generators of U_n. We prove this by induction on n. Let $U_n^{(j)}$ denote the subgroup $U_n^{(j)}=1+T^j$, where T is the ideal generated by t in $\mathbf{F}_2[t]/(t^{2^n})$. Also, let H_n be the subgroup of U_n generated by $\{\alpha_{4i+1},\sigma_{2i+1}\}$, $i=0,1,\ldots$.

Consider the exact sequence

$$1\to K_n\to U_n\xrightarrow{f}U_{n-1}\to 1$$

defining K_n and where f is induced by the natural projection $\mathbf{F}_2[t]/(t^{2^n})\to\mathbf{F}_2[t]/(t^{2^{n-1}})$. Thus, $K_n=U_n^{(2^{n-1})}=1+T^{2^{n-1}}$. Clearly, every element k of K_n satisfies $k^2=1$, and $f\mid H_n: H_n\to H_{n-1}$ is surjective. Assuming by induction that $H_{n-1}=U_{n-1}$, it first follows that every square in U_n belongs to H_n. Indeed, let $u\in U_n$. There exists an $h\in H_n$ such that $u=hk$ for some $k\in K_n$, and thus $u^2=h^2\in H_n$. Now, an easy calculation shows that $\sigma_{2i+1}=\alpha_{2i+1}^2\cdot\alpha_{4i+3}$ mod T^{4i+4}. It follows that

$$\sigma_{2i+1}\in\alpha_{2i+1}^2\cdot\alpha_{4i+3}U_n^{(4i+4)}.$$

Using $(U_n)^2\subset H_n$ and the easily verified fact that $U_n^{(j)}$ is generated by $\alpha_j,\alpha_{j+1},\ldots,\alpha_{2^n-1}$, it follows by decreasing induction on j that $U_n^{(j)}\subset H_n$ for all j. Thus $U_n=U_n^{(1)}\subset H_n$, and so $U_n=H_n$. The induction argument can be rooted at $n=1$ where $U_1=H_1$ is trivial to verify.

Since $\alpha_1\in X_n$ and $\sigma_j\in U_n^+$ for all j, it follows that the set $\{\gamma_5,\gamma_9,\ldots,\gamma_{2^n-3}\}$ generates $U_n/X_n\cdot U_n^+$. (For $n\leqq 2$ this set is empty and $U_n/X_n\cdot U_n^+=\{1\}$.)

Now, the order of α_{4i+1} is 2^{a_i}, where $2^n\leqq(4i+1)2^{a_i}<2^{n+1}$. Thus, the order of γ_{4i+1} divides 2^{a_i}. In order to show that γ_{4i+1} is precisely of order 2^{a_i} and that the set $\{\gamma_{4i+1}\mid i=1,2,\ldots,2^{n-2}-1\}$ is a set of independent generators of $U_n/X_n\cdot U_n^+$ it suffices to check that $|U_n/X_n\cdot U_n^+|=\prod_i 2^{a_i}$, where the product extends over $i=1,2,\ldots,2^{n-2}-1$. We have $|U_n|=2^{2^n-1}$, $|X_n|=2^n$ and $|U_n^+|=2^{2^{n-1}}$. Since $|X_n\cap U_n^+|=|\{1,x^{2^{n-1}}\}|=2$, we have $|U_n/X_n\cdot U_n^+|=2^{2^{n-1}-n}$. On the other hand, for a given $a\in[1,n]$, the set of indices $i\in[1,2^{n-2}-1]$ such that $a_i=a$, i.e. the set $\{i\in[1,2^{n-2}-1]\mid 2^{n-a}\leqq 4i+1<2^{n-a+1}\}$ contains 2^{n-a-2} integers except for $a=n-1$ and $a=n$ where the set is empty. Thus, $\prod_i 2^{a_i}=2^{v_n}$, where $v_n=\sum_{a=1}^{n-2}a2^{n-a-2}=2^{n-1}-n$.

Remark. The above argument actually yields the structure of the group $U_n/X_n \cdot U_n^+$ as

$$U_n/X_n \cdot U_n^+ = \prod_{\nu=1}^{n-1} \tfrac{1}{2}(p-1)^2 p^{n-\nu-1} \cdot \mathbf{Z}/p^\nu\mathbf{Z} \times \tfrac{1}{2}(p-3) \cdot \mathbf{Z}/p^n\mathbf{Z} \quad \text{for} \quad p \text{ odd},$$

and

$$U_n/X_n,\ U_n^+ = \prod_{\nu=1}^{n-2} 2^{n-\nu-2} \cdot \mathbf{Z}/2^\nu\mathbf{Z} \quad \text{for} \quad p=2.$$

We record for later use the following lemma about U_n in the case $p=2$.

LEMMA 2.3. *Suppose* $p=2$. *Denote by* N *the subgroup of* U_n *for* $n \geqq 2$ *consisting of the elements of the form* $u \cdot c(u)$, $u \in U_n$. *Then,*

$$X_n \cdot U_n^+ = X_n \cdot N \cup \sigma_1 X_n \cdot N,$$

where $\sigma_1 = 1 + x^{-1}t^2$.

Proof. It follows from the proof of the preceding lemma that the elements α_1, σ_{2i+1}, $i=0, 1, \ldots$ generate $X_n \cdot U_n^+$. A straightforward calculation, using $c(t) = x^{-1}t$ and $s = x^{-1}t^2$ yields the formula

$$\alpha_{2k+1} \cdot c(\alpha_{2k+1}) = 1 + \sum_{l=0}^{k-1} \binom{k+l}{2l} s^{k+l+1}.$$

Now, for $k>0$ and only then, we can rewrite this as

$$\alpha_{2k+1} \cdot c(\alpha_{2k+1}) = \sigma_{k+1} \cdot \prod_{\nu>0} \sigma_{k+\nu+1}^{e_\nu}$$

for some irrelevant exponents e_ν. By descending induction on $k>0$, starting with $\sigma_k = 1 \in N$ for k large, the formula yields in succession $\sigma_{2^{n-1}-1} \in N$, $\sigma_{2^{n-1}-2} \in N, \ldots, \sigma_3 \in N$. Since $\alpha_1 \in X_n$, we thus have

$$X_n \cdot U_n^+ = X_n \cdot N \cup \sigma_1 X_n \cdot N \cup \sigma_1^2 X_n \cdot N \cup \cdots \cup \sigma_1^{2^{n-1}-1} X_n \cdot N.$$

But $\sigma_1^2 = \sigma_1 \cdot c(\sigma_1) \in N$, and so

$$X_n \cdot U_n^+ = X_n \cdot N \cup \sigma_1 X_n \cdot N.$$

Remark. It is easy to check that actually $\sigma_1 \notin X_n \cdot N$. For instance, map U_n onto $U_2 = U(\mathbf{F}_2[t]/(t^4))$ by the natural projection. Then, $X_n \cdot N$ maps into the subgroup X_2 of U_2 generated by $\alpha_1 = 1+t = x$. On the other hand, σ_1 maps to $1+x+x^{-1} = 1+t^2+t^3 = \alpha_1^2 \cdot \alpha_3 \notin X_2$.

§3. Upper bounds for $\operatorname{Im}\{j : U(\mathbf{Z}C(p^n)) \times E_n \to U(R_n)\}$

We begin the study of the map j. Recall that $E_n = U(\mathbf{Z}[\zeta_n])$, where ζ_n is a primitive p^{n+1}-st root of unity, $R_n = \mathbf{F}_p[t]/(t^{p^n})$, and if x is a choice of generator for $C(p^n)$, $j(x) = j(\zeta_n) = 1+t$.

In this section, we prove that $\operatorname{Im} j \subset \mathbf{F}_p^* \times X_n \cdot U_n^+$ with the notations of Section 2. The main fact is a well known lemma about units in cyclotomic fields.

KUMMER'S LEMMA. *Let $u \in E_n$. Then, for some integer i, the unit $\zeta_n^i u$ is real,* i.e. $c(\zeta_n^i u) = \zeta_n^i u$, *where c is complex conjugation.*

We recall the proof for convenience: Complex conjugation is an element c of the Galois group $\operatorname{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$. Since this group is abelian, we have $|s(cu/u)| = |csu/su| = 1$ for all $s \in \operatorname{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$, where $|z|$ is the absolute value of the complex number z. By an elementary theorem, this implies

$$cu/u = \pm\zeta_n^j,$$

for some integer j. (See [9], 3.4.) If the "plus" sign holds and $j = 2i$, it follows that $c(\zeta_n^i u) = \zeta_n^i u$ as desired.

If p is odd, then replacing j by $j + p^{n+1}$ if necessary, we may assume that j is even, $j = 2i$ say. We claim that in this case, the "minus" sign cannot occur in the above formula. Indeed, if $c(u) = -\zeta_n^i u$, then observing that $c(u) = u \bmod (\zeta_n - 1)$, we would have $2u = 0 \bmod (\zeta_n - 1)$. Since u is a unit, it would follow $2 = 0 \bmod (\zeta_n - 1)$ which contradicts $p \neq 2$.

If $p = 2$, we may assume that $c(u) = +\zeta_n^j u$ after replacing -1 by $\zeta_n^{2^n}$ if necessary. We claim that j is necessarily even. Consider the norm map N from $\mathbf{Q}(\zeta_n)$ to $\mathbf{Q}(\zeta_1)$. We have $N(\zeta_n) = (-1)^{n-1}\zeta_1$, taking say $\zeta_n = e^{2\pi i/2^{n+1}}$. Thus

$$c(Nu) = N(cu) = N(\zeta_n^j u) = \pm\zeta_1^j \cdot Nu.$$

The only possibilities for the unit Nu are $1, -1, \zeta_1, -\zeta_1$. In each case the equation $c(Nu) = \pm\zeta_1^j \cdot Nu$ implies j even.

Kummer's lemma extends to our group rings. Let $c : \mathbf{Z}C(p^n) \to \mathbf{Z}C(p^n)$ be the automorphism induced by $c(x) = x^{-1}$, where x denotes a generator of $C(p^n)$.

LEMMA 3.1. *Let* $u \in U(\mathbf{Z}C(p^n))$. *Then, for some integer* i, *one has* $c(x^i u) = x^i u$.

Proof. The ring $\mathbf{Z}C(p^n)$ is a subring of the maximal order $\mathbf{Z} \times \prod_{\nu=0}^{n-1} \mathbf{Z}[\zeta_\nu]$ of $\mathbf{Q}C(p^n)$. Denote by u_ν, $\nu = 0, 1, \ldots, n-1$ the images of u in the various components $\mathbf{Z}[\zeta_\nu]$ of the maximal order. Applying Kummer's lemma in each $\mathbf{Z}[\zeta_\nu]$, we have $c(\zeta_\nu^{i_\nu} u_\nu) = \zeta_\nu^{i_\nu} u_\nu$ for some collection of integers i_ν. It follows that cu/u is a unit of finite order in $U(\mathbf{Z}C(p^n))$. By Higman's theorem [10], we must have $cu/u = \pm x^j$. Now, projecting to $\mathbf{Z}$ by the augmentation shows that $cu/u = +x^j$ holds. Projecting to the factor $\mathbf{Z}[\zeta_{n-1}]$ yields $\zeta_{n-1}^j = \zeta_{n-1}^{2i}$ for some i, and therefore $j = 2i \bmod p^n$. We then have $c(x^i u) = x^i u$.

LEMMA 3.2. *With the notations of Section* 2, *we have*

$$\operatorname{Im} j \subset \mathbf{F}_p^* \times X_n \cdot U_n^+$$

for all prime numbers p.

Proof. The conjugation c operates on $U(\mathbf{Z}C(p^n))$, E_n and $U(R_n) = U(\mathbf{F}_p[t]/(t^{p^n}))$. The map

$$j : U(\mathbf{Z}C(p^n)) \times E_n \to U(R_n)$$

is a map of C-modules, C being the cyclic group of order 2 generated by c.

Lemma 3.2 is then immediate from Kummer's lemma and its extension to the group ring $\mathbf{Z}C(p^n)$.

Observe that in this section we did not need nor use any regularity hypothesis on the prime p. Thus, we have

COROLLARY 3.3. *For all primes* p *and all* $n \geqq 0$, *there is a surjection*

$$V_n = U(R_n)/\operatorname{Im} j \to U_n/X_n \cdot U_n^+.$$

This is the last statement in Theorem 1.1. (Obviously $U_n/X_n \cdot U_n^+ \cong U(R_n)/X_n \cdot U(R_n)^+$.)

Proof. It suffices to show that $\mathbf{F}_p^* \subset U(R_n)$ is contained in the image of j. This is well known: For s any integer prime to p, $\zeta_n^{sp^n} - 1/\zeta_n^{p^n} - 1$ is a unit in F_n and,

writing $\zeta = \zeta_n^{p^n}$, we have

$$j\left(\frac{\zeta^s - 1}{\zeta - 1}\right) = 1 + x^{p^n} + \cdots + x^{(s-1)p^n} = s,$$

since $x^{p^n} = 1$ in R_n.

§4. Lower bounds for $\operatorname{Im}\{j : U(\mathbf{Z}C(p^n)) \times E_n \to U(R_n)\}$

In this section we finish up the proof of Theorem 1.1. Let $\mathcal{V}_n = \operatorname{Coker}\{j : E_n \to U(R_n)\}$, where $E_n = U(\mathbf{Z}[\zeta_n])$. Observe that V_n is canonically a quotient of $\mathcal{V}_n$.

We claim first that it suffices to prove Theorem 1.1 with $\mathcal{V}_n$ in place of V_n.

Indeed, if $p = 2$, Theorem 1.1 for $\mathcal{V}_n$ says that $\mathcal{V}_n = U_n/X_n \cdot U_n^+$, or equivalently $j(E_n) = \mathbf{F}_p^* \times X_n \cdot U_n^+$. In this case, $V_n = \mathcal{V}_n$ follows from Lemma 3.2 which asserts that $j(U(\mathbf{Z}C(p^n))) \subset \mathbf{F}_p^* \times X_n \cdot U_n^+$.

If p is an odd prime and $v \in \mathcal{V}_n^-$ maps to $1 \in V_n^-$, then we can lift v to $u \in U(R_n)$ so that $c(u) = u^{-1}$ and $u \in j\{U(\mathbf{Z}C(p^n)) \times E_n\} \subset \mathbf{F}_p^* \times X_n \cdot U_n^+$. The unit u is then necessarily contained in the subgroup X_n of $U(R_n)$ generated by x. Since $j(\zeta_n) = x$, we have $u \in j(E_n)$, and hence $v = 1$. Thus, $V_n^- = \mathcal{V}_n^- \cong U_n/X_n \cdot U_n^+$. Furthermore, since the map $\mathcal{V}_n^+ \to V_n^+$ is also surjective, the dual map $\operatorname{Char} V_n^+ \to \operatorname{Char} \mathcal{V}_n^+$ is injective and a canonical injection $\operatorname{Char} \mathcal{V}_n^+ \to S(F_{n-1})$ will give rise to a canonical injection $\operatorname{Char} V_n^+ \to S(F_{n-1})$ as desired.

We conjecture that $\mathcal{V}_n = V_n$ for all $n \geqq 0$ and will prove this for $n = 1$ in Section 6.

For convenience, we restate what we now have to prove.

THEOREM 4.1. *Let* $\mathcal{V}_n = \operatorname{Coker}\{j : E_n \to U(R_n)\}$, $n \geqq 1$. *If* $p = 2$, *then* $\mathcal{V}_n \cong U_n/X_n \cdot U_n^+$ *using the notations of Section* 2. *If* p *is a semi-regular odd prime, then* $\mathcal{V}_n = \mathcal{V}_n^- \times \mathcal{V}_n^+$, *where* $\mathcal{V}_n^- \cong U_n/X_n \cdot U_n^+$ *and* $\operatorname{Char} \mathcal{V}_n^+ \subset S(F_{n-1})$ *with canonical imbedding, where* $S(F_{n-1})$ *is the* p*-component of the ideal class group of* $\mathbf{Q}(\exp(2\pi i/p^n))$.

The proof will rely on the work of Iwasawa on cyclotomic fields and on class field theory. For the reader's convenience we give below, in an appendix to this section, a review of the results we need from Iwasawa's work, including their (trivial) extension to the case $p = 2$ which is only partly covered in Iwasawa's papers. (The case $p = 2$ is irrelevant for the applications Iwasawa has in mind. Here, of course, there is no reason to leave it out.) For the class field theory

needed, references are [1] and [7]. See also the beautiful introduction given by S. Lang in [16].

Recall the notation $F_n = \mathbf{Q}(\zeta_n)$, where ζ_n is a primitive p^{n+1}-st root of unity.

We are interested in two class fields over F_n as follows.

First, define the ray (or congruence) ideal group $H_n = H_n(F_n)$ as the group of those principal (fractional) ideals in F_n which possess a generating element a such that $a = 1 \bmod \mathfrak{p}_n^{p^n}$, where $\mathfrak{p}_n$ is the ideal generated by $\zeta_n - 1$ in F_n. Thus, $H_n = \{(a) \mid a \in F_n,\ a = 1 \bmod \mathfrak{p}_n^{p^n}\}$, where the condition $a = 1 \bmod \mathfrak{p}_n^{p^n}$ means that the $\mathfrak{p}_n$-valuation of $a - 1$ is at least p^n. Since F_n has no real place, the additional requirement on H_n in order to be a ray group (namely $\rho(a) > 0$ for all real $\mathbf{Q}$-imbeddings $\rho : F_n \to \mathbf{R}$) evaporates.

Let K_n/F_n be the p-part of the ray class field extension associated with the ray group H_n. Thus K_n/F_n is an abelian extension with Galois group

$$\mathrm{Gal}\,(K_n/F_n) \cong (I_0(F_n)/H_n)_p,$$

where $I_0(F_n)$ stands for the group of ideals of F_n which are prime to $\mathfrak{p}_n$, and $(I_0(F_n)/H_n)_p$ is the p-primary component of $I_0(F_n)/H_n$.

It is well known that no prime of F_n ramifies in K_n/F_n except those dividing the conductor of H_n and therefore, $\mathfrak{p}_n$ is the only possibly ramified prime in K_n/F_n. See for instance [7], Führer–Verzweigungs–Satz, page 136.

The other class field L_n we need is the p-part of the Hilbert class field of F_n. It is also an abelian extension, with Galois group

$$\mathrm{Gal}\,(L_n/F_n) \cong (I(F_n)/P(F_n))_p = S(F_n),$$

where $I(F_n)$ is the ideal group of F_n and $P(F_n)$ the subgroup of principal ideals. Thus as above, $S(F_n)$ is the p-primary component of the ideal class group of F_n. The extension L_n/F_n is the p-part of the class field extension associated with the ray group $P(F_n)$.

Since $H_n \subset P(F_n)$, we have the inclusions

$$F_n \subset L_n \subset K_n.$$

Observe now that since $K_n/\mathbf{Q}$ and $L_n/\mathbf{Q}$ are Galois extensions, the group $G_n = \mathrm{Gal}\,(F_n/\mathbf{Q})$ operates on $\mathrm{Gal}\,(K_n/F_n)$ and its subgroup $\mathrm{Gal}\,(K_n/L_n)$ via the group extension

$$1 \to \mathrm{Gal}\,(K_n/F_n) \to \mathrm{Gal}\,(K_n/\mathbf{Q}) \to G_n \to 1.$$

The key lemma which bridges class field theory with our problem is the following.

LEMMA 4.2. *There is a canonical isomorphism of G_n-modules*

$$\theta : \mathrm{Gal}\,(K_n/L_n) \to U(R_n)/jE_n = \mathscr{V}_n,$$

where as before, $R_n = \mathbf{F}_p[t]/(t^{p^n})$ and $E_n = U(\mathbf{Z}[\zeta_n])$.

Proof. Let $P_{\text{int.}}$ denote the set of integral principal ideals of F_n which are prime to $\mathfrak{p}_n$. There is a surjection

$$J : P_{\text{int.}} \to U(R_n)/j(E_n)$$

sending the ideal (a), where $a \in \mathbf{Z}[\zeta_n]$, to the class mod $j(E_n)$ of $j(a)$. Since a is prime to $\mathfrak{p}_n = (\zeta_n - 1)$, $j(a)$ is indeed a unit in R_n. Since a is determined by (a) modulo E_n, the map J is well defined. It is clearly surjective. Now, let P_0 be the group of principal fractional ideals in F_n which are prime to $\mathfrak{p}_n$. Define

$$J : P_0 \to U(R_n)/j(E_n)$$

by $J(a) = J(b)/J(c)$, where $a = b/c$ with $b, c \in \mathbf{Z}[\zeta_n]$, both prime to $\mathfrak{p}_n$. Clearly, the kernel of $J : P_0 \to U(R_n)/j(E_n)$ consists of the principal ideals generated by some element $a = 1 \bmod \mathfrak{p}_n^{p^n}$, i.e. Ker $J = H_n$. Hence J induces an isomorphism

$$J : P_0/H_n \to U(R_n)/j(E_n)$$

(with apologies for the abuse of notation) which commutes with the action of G_n.

Now, the Artin map of class field theory yields a commutative diagram

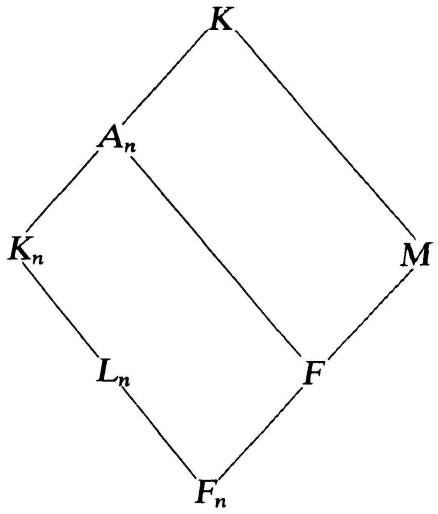
$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}\,(K_n/L_n) & \longrightarrow & \mathrm{Gal}\,(K_n/F_n) & \longrightarrow & \mathrm{Gal}\,(L_n/F_n) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi_K} & & \downarrow{\scriptstyle \psi_L} & & \\
1 & \longrightarrow & P_0/H_n & \longrightarrow & (I_0/H_n)_p & \longrightarrow & (I/P)_p & \longrightarrow & 1,
\end{array}$$

with ψ_0, ψ_K, ψ_L isomorphisms.

Define $\theta = J\psi_0$.

It is well known that the Artin maps ψ_0, ψ_K, ψ_L all commute with the action of $G_n = \mathrm{Gal}\,(F_n/\mathbf{Q})$, as follows right away from the definitions, and thus θ is a map of G_n-modules and an isomorphism. The lemma is proved.

Following Iwasawa [13], we now consider the diagram of fields as illustrated below.



The tower $K_n \supset L_n \supset F_n$ has already been described.

Let $F = \bigcup_{n \geq 0} F_n$, and let K be the maximal abelian p-extension of F such that only the prime $\mathfrak{p}$ (the unique extension of $\mathfrak{p}_n$ to F) ramifies in K. The construction of such infinite field extensions is given in [12], Section 6.

Note that $K_n \subset K$, because $K_n \cdot F/F$ is an abelian p-extension in which at most the prime $\mathfrak{p}$ ramifies.

The field A_n is the largest abelian extension of F_n contained in K. Then, A_n contains F and also the p-part of all the class fields of F_n contained in K, e.g. K_n.

Finally we define M, still following Iwasawa. Let $E = \bigcup_{n \geq 0} E_n$, where E_n is the group of units of $F_n \subset F$. Consider the Kummer extensions $M_m = F(E^{1/p^m})$, $m = 1, 2, \ldots$. By an obvious broadening of Kummer theory (as presented in [1], Chap. VI, Theorem 4) to these infinite field extensions, $\mathfrak{p}$ is the only prime of F which has a chance to ramify in M_m/F. Since M_m/F is an abelian p-extension, it follows that $M_m \subset K$ for all m. Set $M = \bigcup_{m \geq 0} M_m$.

All extensions in sight in the diagram (including those over $\mathbf{Q}$) are Galois and thus the various Galois groups, e.g. $\mathrm{Gal}(K_n/L_n)$, $\mathrm{Gal}(K/F)$, etc. are all modules over $G_n = \mathrm{Gal}(F_n/\mathbf{Q})$ via the group extension

$$1 \to \mathrm{Gal}(K/F_n) \to \mathrm{Gal}(K/\mathbf{Q}) \to G_n \to 1.$$

It will be convenient to view K as a subfield of the complex numbers and to denote complex conjugation uniformly by c on every intermediate Galois extension of $\mathbf{Q}$.

Recall that we want to calculate $\mathrm{Gal}(K_n/L_n)$ with the action on it of complex conjugation. (Lemma 4.2.)

We gather informations on the Galois groups of interest to us in the diagram.

LEMMA 4.3. $\mathrm{Gal}(M/F) = \mathrm{Gal}^-(M/F)$, *i.e. for every* $s \in \mathrm{Gal}(M/F)$, *we have* $csc^{-1} = s^{-1}$.

The proof is elementary. Let μ be the group of roots of unity in F. By (elementary) Kummer theory, we have for each m a canonical isomorphism

$$\chi : \mathrm{Gal}(M_m/F) \to \mathrm{Hom}(E \cdot F^{\cdot p^m}/F^{\cdot p^m}, \mu).$$

It suffices to show that $cs_m c^{-1} = s_m^{-1}$ for all m, where s_m is the projection of s into $\mathrm{Gal}(M_m/F)$. We write s for s_m again. Then, by definition of χ

$$\chi_{csc^{-1}}(u) = csc^{-1}(v)/v,$$

where $v^{p^m} = u$, $u \in E \cdot F^{\cdot p^m}$ and $v \in M_m$.

By Kummer's lemma, we may assume that $u \in E^+$. (Compare §3.) Indeed, $u \in E^+$ holds up to multiplication by some root of unity which in $F^{\cdot}$ is a p^m-th power. If p is odd, v can then obviously be chosen real. If $p = 2$, u can even be taken positive since in that case -1 is a 2^m-th power in $F^{\cdot}$. In all cases we may thus assume that $c(v) = v$.

But then, we have

$$\chi_{csc^{-1}}(u) = csc^{-1}(v)/v = c(sv/v) = (sv/v)^{-1},$$

since sv/v is a root of unity. Hence,

$$\chi_{csc^{-1}}(u) = \chi_s(u^{-1}) = \chi_s^{-1}(u) = \chi_{s^{-1}}(u).$$

This holds for every $u \in E \cdot F^{\cdot p^m}/F^{\cdot p^m}$ and since χ is an isomorphism, it follows that $csc^{-1} = s^{-1}$.

As to the extension K/M, we have a theorem of Iwasawa describing its Galois group. Let

$$S = \varinjlim \{S(F_n)\},$$

the limit being taken with respect to the obvious maps $S(F_n) \to S(F_{n+1})$ induced by the inclusions $F_n \to F_{n+1}$.

The relationship between S and the extension K/M is given by the following theorem.

THEOREM OF IWASAWA. *There is a canonical isomorphism of* Gal $(F/\mathbf{Q})$*-modules*

$$\chi : S \to \text{Char Gal}\,(K/M).$$

Here, Char Gal (K/M) means the group of continuous homomorphisms Hom (Gal (K/M), μ), where μ, the group of roots of unity in F, is equipped with the discrete topology. The action of Gal $(F/\mathbf{Q})$ on Char Gal (K/M) is given by

$$(s\chi)(\sigma) = s(\chi(s^{-1} \cdot \sigma)),$$

where $s \in \text{Gal}\,(F/\mathbf{Q})$, $\sigma \in \text{Gal}\,(K/M)$ and $s^{-1} \cdot \sigma$ is given by the operations of Gal $(F/\mathbf{Q})$ on Gal (K/M) via the group extension

$$1 \to \text{Gal}\,(K/F) \to \text{Gal}\,(K/\mathbf{Q}) \to \text{Gal}\,(F/\mathbf{Q}) \to 1.$$

Caution: Iwasawa uses the action $(s\chi)(\sigma) = \chi(s^{-1} \cdot \sigma)$. Then, of course, χ is no longer a Gal $(F/\mathbf{Q})$-map. We prefer the above formulation because we wish to keep track of the Gal $(F/\mathbf{Q})$-module structure and Gal $(F/\mathbf{Q})$ operates naturally on μ. Observe that complex conjugation c can be viewed as an element in Gal $(F/\mathbf{Q})$.

Finally, we shall need to know that Gal (K/F) surjects by restriction onto Gal (K_n/F_n). By elementary Galois theory, this is equivalent to proving:

LEMMA 4.4. $K_n \cap F = F_n$.

Proof. Since $[F_{n+1} : F_n] = p$, a prime, and every subfield of F strictly larger than F_n contains F_{n+1}, the assertion is equivalent to showing that F_{n+1} *is not contained in* K_n.

To prove this, we view K_n/F_n and F_{n+1}/F_n as class field extensions.

We have readily constructed K_n as class field over F_n associated with the ray group

$$H_n = \{(a) \in P(F_n) \mid a = 1 \bmod \mathfrak{p}_n^{p^n}\}.$$

As is well known, F_{n+1} is class field over F_n associated with the ray group

$$H = \{\mathfrak{a} \in I(F_n) \mid N\mathfrak{a} = 1 \bmod p^{n+2}\}.$$

(Recall that F_{n+1} is obtained from F_n by adjunction of the p^{n+2}-nd roots of unity. The norm is from F_n to $\mathbf{Q}$. See [7], Satz 131.)

Class field theory asserts that K_n contains F_{n+1} if and only if the ray group of K_n, namely H_n, is contained in the ray group of F_{n+1}. Thus, in order to prove $F_{n+1} \not\subset K_n$, it suffices to exhibit an element $a \in F_n$ such that $a \equiv 1 \bmod \mathfrak{p}_n^{p^n}$, but $|N(a)| \not\equiv 1 \bmod p^{n+2}$. We then have $(a) \in H_n$ and $(a) \notin H$.

If p is an odd prime, take $a = 1+p$. Then, the congruence $a \equiv 1 \bmod \mathfrak{p}_n^{p^n}$ results from $(p) = \mathfrak{p}_n^{p^n(p-1)}$ in $I(F_n)$. On the other hand, since $a \in \mathbf{Q}$, we have

$$N(a) = (1+p)^{p^n(p-1)} = 1 + p^n(p-1)p + \sum_{r \geqq 2} \binom{p^n(p-1)}{r} p^r.$$

It is easily verified that for $r \geqq 2$ and p an odd prime, we have

$$\binom{p^n(p-1)}{r} p^r \equiv 0 \bmod p^{n+2}.$$

Therefore,

$$|N(a)| = N(a) \equiv 1 - p^{n+1} \bmod p^{n+2},$$

and the lemma is proved for p odd.

If $p = 2$ and $n \geqq 1$, take $a = 1+2i \in F_n$. (Here, $i = \zeta_1$ is a primitive 4-th root of unity.) Then, $a \equiv 1 \bmod \mathfrak{p}_n^{2^n}$, since $(2) = \mathfrak{p}_n^{2^n}$. Further,

$$N(1+2i) = (1+2^2)^{2^{n-1}} = 1 + 2^{n-1} \cdot 2^2 + \sum_{r \geqq 2} \binom{2^{n-1}}{r} 2^{2r} \equiv 1 + 2^{n+1} \bmod 2^{n+2},$$

and the lemma follows for $p = 2$ also, at least for $n \geqq 1$.

We do not need the lemma for $p = 2$ and $n = 0$. It is however still true. In that case take $a = 3$ in the above argument.

We now proceed to prove Theorem 4.1.

Let first $p = 2$. Then, by Weber's theorem, the class number of F_n is odd, i.e. $S(F_n) = 0$ for all n. (See e.g. [11], Theorem III.) Hence, Iwasawa's theorem in that case implies $K = M$. By Lemma 4.3 it follows that $\mathrm{Gal}(K/F) = \mathrm{Gal}^-(K/F)$, where as earlier $\mathrm{Gal}^-(K/F) = \{\sigma \in \mathrm{Gal}(K/F) \mid c\sigma c^{-1} = \sigma^{-1}\}$. Since the restriction map $\mathrm{Gal}(K/F) \to \mathrm{Gal}(K_n/F_n)$ is surjective and clearly commutes with the action of complex conjugation, we also have $\mathrm{Gal}(K_n/F_n) = \mathrm{Gal}^-(K_n/F_n)$. Now, $\mathrm{Gal}(L_n/F_n) = S(F_n) = 0$. Thus $L_n = F_n$ in this case, and $\mathrm{Gal}(K_n/L_n) = \mathrm{Gal}^-(K_n/L_n)$. Using Lemma 4.2, this can be reworded

$$\mathcal{V}_n = \mathcal{V}_n^-.$$

Going back to the notations in §2, we now show that this implies $\mathcal{V}_n = U_n/X_n \cdot U_n^+$.

Indeed, $\mathcal{V}_n = \mathcal{V}_n^-$ means that for every unit $u \in U(R_n)$, there exists a unit $e \in E_n$ such that $c(u) = j(e) \cdot u^{-1}$, i.e. $u \cdot c(u) = j(e) \in j(E_n)$. With the notation $N = \{u \cdot c(u), u \in U(R_n)\}$ of §2, this means that $N \subset j(E_n)$. On the other hand, $X_n \subset j(E_n)$ since $x = j(\zeta_n)$, and so $X_n \cdot N \subset j(E_n)$. But, by Lemma 2.3, we had $X_n \cdot U_n^+ = X_n \cdot N \cup \sigma_1 X_n \cdot N$, where $\sigma_1 = 1 + x + x^{-1}$. Since $X_n \cdot N \subset j(E_n)$, the statement $\mathcal{V}_n = U_n/X_n \cdot U_n^+$, or equivalently $j(E_n) = \mathbf{F}_2 \times X_n \cdot U_n^+$ will follow if we verify that $\sigma_1 \in j(E_n)$. This is immediate:

$$\sigma_1 = x^{-1}(1 + x + x^2) = j\{\zeta_n^{-1} \cdot (\zeta_n^3 - 1)/(\zeta_n - 1)\}.$$

Next, let p be an odd prime.

We first dispose of the statement $\mathcal{V}_n^- \cong U_n/X_n \cdot U_n^+$. By §3, we know that $E_n = \langle \zeta_n \rangle \cdot E_n^+$. Therefore, $\mathcal{V}_n$ surjects onto $U_n/X_n \cdot U_n^+$. Since $U_n/X_n \cdot U_n^+$ is equal to its subgroup of antisymmetric elements, i.e. $U_n/X_n \cdot U_n^+ = (U_n/X_n \cdot U_n^+)^-$, we have a surjection

$$\mathcal{V}_n^- \to U_n/X_n \cdot U_n^+.$$

If $v \in \mathcal{V}_n^-$ maps to $1 \in U_n/X_n \cdot U_n^+$, then v is represented by a unit $x^i u \in U_n$ with u both symmetric and antisymmetric. Since p is odd, it follows that $u = 1$ and thus $v = 1$. ($X_n \subset j(E_n)$.)

This proves $\mathcal{V}_n^- \cong U_n/X_n \cdot U_n^+$.

It remains to evaluate $\mathcal{V}_n^+$. Assume now that p is semi-regular, i.e. $S(F_0^+) = 0$. Iwasawa has proved in [11] that this implies $S(F_n^+) = 0$ for all $n \geqq 0$, where $S(F_n^+)$ is the p-primary component of the ideal class group of $F_n^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1})$. Furthermore, it is well known that the inclusion $F_n^+ \to F_n$ induces an isomorphism $S(F_n^+) \cong S^+(F_n)$. (See Statement 4.5 in the appendix below.) Therefore for all n, $S(F_n) = S^-(F_n)$, and $S = S^-$.

Since p is odd, $\mathrm{Gal}(K/F)$ splits as $\mathrm{Gal}^+(K/F) \times \mathrm{Gal}^-(K/F)$ and hence, $\{\mathrm{Char}\ \mathrm{Gal}(K/M)\}^- = \mathrm{Char}\ \mathrm{Gal}^+(K/M)$. Thus, Iwasawa's theorem becomes

$$S = S^- \cong \mathrm{Char}\ \mathrm{Gal}^+(K/M) = \mathrm{Char}\ \mathrm{Gal}^+(K/F).$$

The last isomorphism because $\mathrm{Gal}(M/F) = \mathrm{Gal}^-(M/F)$ by Lemma 4.3.

Since $\mathrm{Gal}^+(L_n/F_n) = S^+(F_n) = 0$, it follows that $\mathrm{Gal}^+(K_n/F_n) = \mathrm{Gal}^+(K_n/L_n)$, and Lemma 4.4 provides a surjection $\mathrm{Gal}^+(K/F) \to \mathrm{Gal}^+(K_n/L_n) = \mathcal{V}_n^+$.

We thus get a canonical injection

$$\text{Char } \mathcal{V}_n^+ = \text{Char Gal}^+(K_n/L_n) \to \text{Char Gal}^+(K/F) \cong S^-,$$

and it remains to show that this subgroup is contained in $S^-(F_{n-1})$.

According to Iwasawa [13], Theorem 15, page 553, $S^-(F_{n-1})$ injects into $S^- = \varinjlim S^-(F_\nu)$ and is precisely the fixed point set in S^- under the action of $\Gamma_{n-1} = \text{Gal}(F/F_{n-1}) \subset \text{Gal}(F/\mathbf{Q})$.

This will imply $\text{Char Gal}^+(K_n/L_n) \subset S^-(F_{n-1})$. Indeed, the action of Γ_{n-1} on $\text{Gal}(K_n/L_n)$ factors through the action of the quotient $\text{Gal}(F_n/F_{n-1}) \subset G_n = \text{Gal}(F_n/\mathbf{Q})$ of Γ_{n-1}. We see now that this action is trivial. If $s \in \text{Gal}(F_n/F_{n-1})$ is the generator such that $s(\zeta_n) = \zeta_n^{1+p^n}$, we have $s(x) = x^{1+p^n} = x$ in $R_n = \mathbf{F}_p[x]/(x^{p^n} - 1)$ and therefore $\text{Gal}(F_n/F_{n-1})$ operates trivially on $U(R_n)/j(E_n) = \mathcal{V}_n \cong \text{Gal}(K_n/L_n)$. The action is a fortiori trivial on $\text{Gal}^+(K_n/L_n)$. Now, every character $\chi : \text{Gal}^+(K_n/L_n) \to \mu$, where μ is the group of roots of unity in F, takes its values in the subgroup generated by ζ_{n-1}. This, because $u^{p^n} = 1$ for all $u \in U(R_n)$ such that $u = 1 \bmod tR_n$, and so the order of every element in $\text{Gal}(K_n/L_n)$ divides p^n. Since $\text{Gal}(F_n/F_{n-1})$ operates trivially on ζ_{n-1}, it follows that $\text{Gal}(F_n/F_{n-1})$, and hence $\text{Gal}(F/F_{n-1})$, operates trivially on $\text{Char Gal}^+(K_n/L_n)$. Therefore $\text{Char Gal}^+(K_n/L_n) \subset S^-(F_{n-1})$.

Appendix to §4. Résumé of some of Iwasawa's work

Beside the isomorphism

$$\chi : S = \varinjlim S(F_n) \to \text{Char Gal}(K/M),$$

we have used the following results of Iwasawa taken from [11] and [13].

(4.5) $S(F_n^+) \to S^+(F_n)$ is an isomorphism for all $n \geqq 0$;

(4.6) $S(F_0^+) = 0$, resp. $S(F_0) = 0$, implies $S(F_n^+) = 0$, resp. $S(F_n) = 0$, for all $n \geqq 0$;

(4.7) The natural map $S^-(F_{n-1}) \to S^-(F_n)$ is an injection and the fixed point set of $\text{Gal}(F/F_{n-1})$ on $S^- = \varinjlim S^-(F_n)$ is precisely $S^-(F_{n-1})$.

The notations which agree with those of Iwasawa are carried over from the preceding sections.

Here are some indications of proofs.

First, the map $\chi : S \to \text{Char Gal}(K/M)$ is defined as follows. Let $\mathfrak{a}$ be an ideal in F_n representing some element $A \in S$. For some integer m we have $\mathfrak{a}^{p^{m+1}} = (a)$,

$a \in F_n$. We may assume that F_n contains the p^{m+1}-st roots of unity, replacing if necessary $\mathfrak{a}$ and a by their images under an inclusion $F_n \to F_{n'}$, where $n' \geqq \max\{m, n\}$. Consider the Kummer extension $F_n(\alpha)$, where $\alpha^{p^{m+1}} = a$. Since for every prime $\mathfrak{p}$ in F_n the $\mathfrak{p}$-completion of $\mathfrak{a}$ is principal, it follows that a is a p^{m+1}-st power in the $\mathfrak{p}$-completion of F_n, up to a $\mathfrak{p}$-adic unit. Hence, by Kummer theory, it follows that no other prime than $\mathfrak{p}_n$ ramifies in $F_n(\alpha)/F_n$. (Compare [1], Theorem 4, page 22.) Therefore, $F(\alpha) \subset K$. Set

$$\chi_A(\sigma) = \sigma\alpha/\alpha \in \mu_m$$

for all $\sigma \in \mathrm{Gal}\,(K/M)$, where μ_m is the group of p^{m+1}-st roots of unity in F.

It is immediate to verify that χ is a well defined homomorphism $\chi : S \to \mathrm{Char\ Gal}\,(K/M)$. Also, with $s \in \mathrm{Gal}\,(F/\mathbf{Q})$,

$$\chi_{sA}(\sigma) = \sigma(s\alpha)/s\alpha = s(s^{-1}\sigma s\alpha/\alpha) = s\chi_A(s^{-1}\sigma s) = (s \cdot \chi_A)(\sigma).$$

Thus χ is a homomorphism of $\mathrm{Gal}\,(F/\mathbf{Q})$-modules.

Suppose χ_A is the trivial character. For some choice of $\mathfrak{a}$ such that $\mathfrak{a}^{p^{m+1}} = (a)$, $a \in F_n$, $n \geqq m$, and $\alpha^{p^{m+1}} = a$, this implies $\alpha \in M$. We may assume that $\alpha \in M_{m+1}$, the Kummer field generated by the p^{m+1}-st roots of units E of F. Since $\alpha^{p^{m+1}} = a \in F$, it follows from elementary Kummer theory that $\alpha^{p^{m+1}} \in E \cdot F^{p^{m+1}}$, and so, increasing n again if necessary, we can assume $a = u \cdot c^{p^{m+1}}$ with $u \in E_n$, $c \in F_n$. Then, $\mathfrak{a}^{p^{m+1}} = (c)^{p^{m+1}}$ and $\mathfrak{a} = (c)$ is principal, i.e. $A = 1$. Thus, χ is injective.

In order to prove surjectivity, let $\xi : \mathrm{Gal}\,(K/M) \to \mu$ be a continuous character. Since $\mathrm{Gal}\,(K/F)$ is abelian, there is an extension $\Xi : \mathrm{Gal}\,(K/F) \to \mu$ with image μ_m for some m. Let Φ be the fixed field of $\mathrm{Ker}\,\Xi$. Then, Φ/F is finite cyclic and Ξ breaks up into

$$\mathrm{Gal}\,(K/F) \xrightarrow{\Psi} \mathrm{Gal}\,(\Phi/F) \xrightarrow{\Xi'} \mu_m.$$

Viewing $\Xi' : \mathrm{Gal}\,(\Phi/F) \to \mu_m \in \Phi^*$ as a cocycle and applying Hilbert Theorem 90, we find an element $\alpha \in \Phi^*$ such that $\Xi'(\sigma') = \sigma'\alpha/\alpha$ for all $\sigma' \in \mathrm{Gal}\,(\Phi/F)$. Hence, $\Xi(\sigma) = \Psi\sigma(\alpha)/\alpha$ for all $\sigma \in \mathrm{Gal}\,(K/F)$. By a familiar argument, it follows that $\alpha^{p^{m+1}} \in F$. (Observe that $\Xi(\sigma)^{p^{m+1}} = 1$.) We have $\alpha^{p^{m+1}} = a \in F_n$ for some $n \geqq m$. Moreover, since $\zeta_n - 1 \in F_n$ is invariant by $\mathrm{Gal}\,(\Phi/F)$, we may assume that α is prime to $\mathfrak{p}_n = (\zeta_n - 1)$. Since further at most $\mathfrak{p}_n$ ramifies in $F_n(\alpha)/F_n$, because only $\mathfrak{p}_n$ ramifies in Φ/F_n, and since $\mathrm{Gal}\,(F_n(\alpha)/F_n)$ clearly leaves the ideal (α) fixed, it follows that (α) is the extension to $F_n(\alpha)$ of an ideal $\mathfrak{a}$ in F_n. Now, $\mathfrak{a}^{p^{m+1}} = (a)$, and

denoting by A the class of $\mathfrak{a}$ in S, we have

$$\chi_A(\sigma) = \sigma\alpha/\alpha = \Psi\sigma(\alpha)/\alpha = \Xi(\sigma) = \xi(\sigma)$$

for all $\sigma \in \mathrm{Gal}(K/M)$. Thus, $\chi_A = \xi$ and χ is surjective.

LEMMA 4.5. *The inclusion $F_n^+ \to F_n$ induces an isomorphism*

$$S(F_n^+) \to S^+(F_n).$$

The proof is quite elementary. For $p = 2$, both sides are zero by Weber's theorem and there is nothing to prove. Suppose now that p is an odd prime and let $\mathfrak{a}$ be some ideal in F_n^+ such that $\mathfrak{a}^{p^m} = (a)$ and $i\mathfrak{a} = (\alpha)$, where $a \in F_n^+$, $\alpha \in F_n$ and i is the injection of the ideal groups. Then, $\mathfrak{a}^2 = (\alpha \cdot \bar{\alpha})$ because they have equal extensions in F_n. Since $\mathfrak{a}^{p^m}$ is also principal and 2 is prime to p^m, it follows that $\mathfrak{a}$ itself is principal. This proves that $S(F_n^+) \to S(F_n)$ is injective.

Clearly, the image is contained in $S^+(F_n)$. Let $\mathfrak{A}$ be a representative of an element in $S^+(F_n)$. We may assume that $\mathfrak{A} = \mathfrak{B}^{p+1}$ for some $\mathfrak{B} \in S^+(F_n)$. We have $\bar{\mathfrak{B}} = \mathfrak{B} \cdot (\beta)$ for some $\beta \in F_n$. From $\mathfrak{B} = \bar{\bar{\mathfrak{B}}} = \bar{\mathfrak{B}} \cdot (\bar{\beta}) = \mathfrak{B} \cdot (\beta \cdot \bar{\beta})$ we conclude that $\beta \cdot \bar{\beta} = v$ is a unit of F_n^+. Raising to the $(p+1)$-st power and setting $\alpha = \beta^{p+1}$ and $u = v^{(1/2)(p+1)}$, we have $\alpha \cdot \bar{\alpha} = u \cdot \bar{u}$. Therefore, $\bar{\mathfrak{A}} = \mathfrak{A} \cdot (\alpha) = \mathfrak{A} \cdot (\alpha \cdot u^{-1})$. Since $\alpha u^{-1} \cdot \overline{\alpha u^{-1}} = 1$, Hilbert's Theorem 90 gives us an element $\gamma \in F_n$ so that $\alpha u^{-1} = \gamma \cdot \bar{\gamma}^{-1}$, and then $\overline{\mathfrak{A} \cdot (\gamma)} = \mathfrak{A} \cdot (\gamma)$. Thus every element of $S^+(F_n)$ has a representative $\mathfrak{A}$ such that $\bar{\mathfrak{A}} = \mathfrak{A}$. We may further assume that $\mathfrak{A}$ is prime to $\mathfrak{p}_n = (\zeta_n - 1) = \mathfrak{p}_n$. But then, since no prime other than $\mathfrak{p}_n$ ramifies in F_n/F_n, it follows that $\mathfrak{A}$ is the extension in F_n of some ideal in F_n^+. Therefore, $S(F_n^+) \to S^+(F_n)$ is surjective and the lemma is proved.

A nice and simple proof of (4.6) is given in Iwasawa's note [11]. There is no point in repeating it here.

COROLLARY. *If p is a semi-regular prime, i.e. $S(F_0^+) = 0$, then $S(F_n) = S^-(F_n)$ for all $n \geqq 0$.*

LEMMA 4.7. *The map $S^-(F_{n-1}) \to S^-(F_n)$ is injective and $S^-(F_{n-1})$ is precisely the fixed point set in S^- of the Galois group* $\mathrm{Gal}(F/F_{n-1})$.

Proof. We may assume p odd. Let temporarily $G = \mathrm{Gal}(F_n/F_{n-1})$. Facts from Galois cohomology (Theorems 11 and 13 of [13]):

$$H^2(G, C(F_n)) \cong H^2(G, E_n),$$
$$H^1(G, C(F_n)) \cong \mathrm{Ker}\{C(F_{n-1}) \to C(F_n)\} = \mathrm{Ker}\{S(F_{n-1}) \to S(F_n)\}.$$

These isomorphisms are proved using class field theory. For the proofs we refer the reader to [13], pages 550 and 551. The last equality follows by an argument similar to the one used in the proof of Lemma 4.5.

The groups on the left, as well as on the right, are modules over the cyclic group of order 2 operating by complex conjugation c on the coefficients $C(F_{n-1})$, $C(F_n)$, E_n. Moreover, the isomorphisms commute with the action of c. Thus $H^k(G, C(F_n))^-$ makes sense.

Since $E_{n-1} = \mu_{n-1} \cdot E_{n-1}^+$ and the elements of μ_{n-1} are norms from E_n, it follows that $H^2(G, C(F_n))^- \cong H^2(G, E_n)^- \cong (E_{n-1}/NE_n)^- = 0$, where N is the norm from F_n to F_{n-1}.

Since $C(F_n)$ is finite, the Herbrand quotient

$$|H^2(G, C(F_n))|/|H^1(G, C(F_n))| = 1.$$

The usual argument for proving this yields

$$|H^1(G, C(F_n))^-| = |H^2(G, C(F_n))^-| = 1$$

in the present situation. Hence, $\operatorname{Ker}\{S^-(F_{n-1}) \to S^-(F_n)\} = 0$.

Observe that in the situation where p is assumed to be semi-regular, $H^2(G, E_n) \cong E_{n-1}/NE_n$ is of order prime to p because NE_n contains the subgroup E_{n-1}^* of circular units in E_{n-1} whose index in E_n equals the class number of F_n^+. (See [8], §11, Satz 3.) Therefore, in this case, $H^1(G, C(F_n))$ is a p-group of order prime to p, i.e. $H^1(G, C(F_n)) = 0$. But we do not need this.

It is clear that $S^-(F_{n-1})$ is fixed under $\operatorname{Gal}(F/F_{n-1})$. Conversely, in order to prove that every element of S^- fixed under $\operatorname{Gal}(F/F_{n-1})$ belongs to $S^-(F_{n-1})$ it suffices to prove that if $\mathfrak{a}$ is an ideal in F_m whose class is fixed under $\operatorname{Gal}(F_m/F_{m-1})$, then $\mathfrak{a}$ is an extension of an ideal in F_{m-1}, $m \geqq n$. We have then, $s\mathfrak{a} = \mathfrak{a} \cdot (a_s)$ and the map

$$a : \operatorname{Gal}(F_m/F_{m-1}) \to F_m^\cdot/E_m$$

sending s to a_s is a 1-cocycle. Since $H^1(\operatorname{Gal}(F_m/F_{m-1}), F_m^\cdot/E_m)$ injects into $H^2(\operatorname{Gal}(F_m/F_{m-1}), E_m)$ by the cohomology exact sequence and Hilbert's Theorem 90, $H^2(\operatorname{Gal}(F_m/F_{m-1}), E_m)^- = 0$ implies $H^1(\operatorname{Gal}(F_m/F_{m-1}), F_m^\cdot/E_m)^- = 0$. It is easily verified that the cohomology class of a is antisymmetric under the action of complex conjugation, as a consequence of the fact that the class of $\mathfrak{a}$ is. It follows that there exists $c \in F_m^\cdot/E_m$ such that $a_s = c/sc$ for all $s \in \operatorname{Gal}(F_m/F_{m-1})$. Hence, $s(\mathfrak{a} \cdot (c)) = \mathfrak{a} \cdot (c)$. Since $\mathfrak{a} \cdot (c)$ also represents the class of $\mathfrak{a}$, we may as well assume that $s(\mathfrak{a}) = \mathfrak{a}$. As $\mathfrak{a}$ may be further assumed to be prime to $\mathfrak{p}_m$, this implies that $\mathfrak{a}$ is the extension to F_m of an ideal of F_{m-1}.

§5. Structure of W_n for regular primes

Let again $C(p^{n+1})$ denote a cyclic group of order p^{n+1} with generator x. We identify $\mathbf{Q}C(p^{n+1})$ with the product of fields $\mathbf{Q}e \times \prod_{\nu=0}^{n} \mathbf{Q}(\zeta_\nu)e_\nu$ under the isomorphism sending x to $e+\sum_{\nu=0}^{n} \zeta_\nu e_\nu$, where $\zeta_\nu = \exp(2\pi i/p^{\nu+1})$, and where $1 = e+e_0+\cdots+e_n$ is the decomposition of 1 as a sum of primitive orthogonal idempotents in $\mathbf{Q}C(p^{n+1})$.

The subring $\mathbf{Z}C(p^{n+1})$ is contained in the maximal order $\mathscr{A}_n = \mathbf{Z}e \times \prod_{\nu=0}^{n} A_\nu e_\nu$ of $\mathbf{Q}C(p^{n+1})$, where $A_\nu = \mathbf{Z}[\zeta_\nu]$.

Recall that W_n denotes the kernel of the homomorphism

$$i_*: \tilde{K}_0(\mathbf{Z}C(p^{n+1})) \to \tilde{K}_0(\mathscr{A}_n)$$

induced by the inclusion $i: \mathbf{Z}C(p^{n+1}) \to \mathscr{A}_n$.

Theorem 1.2 of Section 1 which is an immediate consequence of Theorem 1.1 enables us to calculate the order of W_n for regular primes as advertised in the introduction. In this section we discuss the structure of the group.

Let $t_0 = \zeta_0 - 1$. We regard t_0 as an element in all the A_ν as $\zeta_0 = \zeta_\nu^{p^\nu}$. Denote by c_n the ideal

$$c_n = p^{n+1}\mathbf{Z}e \times p^n t_0 A_0 e_0 \times \cdots \times p^{n-\nu} t_0 A_\nu e_\nu \times \cdots \times t_0 A_n e_n.$$

It is easily verified that $c_n \subset \mathbf{Z}C(p^{n+1}) \subset \mathscr{A}_n$. More precisely, if $i: \mathbf{Z}C(p^{n+1}) \to \mathscr{A}_n$ denotes the inclusion given by $i(x) = e+\sum_{\nu=0}^{n} \zeta_\nu e_\nu$, we have the formulas

$$p^{n+1}e = i\left\{\prod_{\nu=0}^{n} (1+x^{p^\nu}+\cdots+x^{(p-1)p^\nu})\right\},$$

and

$$p^{n-\nu} t_0 \zeta_\nu^k e_\nu = i\left\{x^k(x^p-1)\prod_{\lambda=\nu+1}^{n} (1+x^{p^\lambda}+\cdots+x^{(p-1)p^\lambda})\right\},$$

which are easily verified, looking at the right hand side componentwise. These identities show that a $\mathbf{Z}$-base of c_n is contained in $\mathbf{Z}C(p^{n+1})$.

Thus, there is a fibre product

$$\begin{array}{ccc} \mathbf{Z}C(p^{n+1}) & \longrightarrow & \mathscr{A}_n \\ \downarrow & & \downarrow \\ \mathbf{Z}C(p^{n+1})/c_n & \longrightarrow & \mathscr{A}_n/c_n \end{array}$$

which in turn yields an exact sequence

$$U(\mathbf{Z}C(p^{n+1})/c_n)\times U(\mathscr{A}_n)\xrightarrow{J_n} U(\mathscr{A}_n/c_n)\xrightarrow{\Phi_n}\tilde{K}_0(\mathbf{Z}C(p^{n+1}))$$

$$\longrightarrow\prod_{r=0}^{n}\tilde{K}_0(\mathbf{Z}[\zeta_\nu])\longrightarrow 0.$$

We have used here that $\mathbf{Z}C(p^{n+1})/c_n$ and $\mathscr{A}_n/c_n$ are semi-local rings.

Hence, $W_n=\operatorname{Coker} J_n$.

Recall that there is an involution on $\mathbf{Z}C(p^{n+1})$ determined by $x\to x^{-1}$ and also on $\mathscr{A}_n$, resp. $\mathscr{A}_n/c_n$ given by complex conjugation in each A_ν. We denote by $\mathscr{U}_n^+$ the subgroup of $U(\mathscr{A}_n/c_n)$ consisting of symmetric elements (i.e. elements left fixed by the involution). Let $\mathscr{X}_n\subset U(\mathscr{A}_n/c_n)$ stand for the subgroup consisting of the units of the form $e+\sum_{\nu=0}^{n}\zeta_\nu^{k_\nu}e_\nu$.

THEOREM 5.1. *Let p be a regular odd prime. Then, the map $\Phi_n: U(\mathscr{A}_n/c_n)\to\tilde{K}_0(\mathbf{Z}C(p^{n+1}))$ of the above exact sequence induces an isomorphism*

$$\operatorname{Im}\Phi_n=W_n\cong U(\mathscr{A}_n/c_n)/\mathscr{X}_n\mathscr{U}_n^+J_n(U(\mathbf{Z}C(p^{n+1})/c_n)).$$

Note that $\mathscr{A}_n/c_n$ and $S_n=\mathbf{Z}C(p^{n+1})/c_n$ are finite rings and their generators $t_\nu e_\nu=(\zeta_\nu-1)e_\nu$, viz. $t=x-1$ are nilpotent. Thus, the calculation of the groups of units $U(\mathscr{A}_n/c_n)$, $\mathscr{U}_n^+$, and $J_n(S_n)$ however complicated, is elementary, i.e. does not require the knowledge of a basis in $U(\mathscr{A}_n)$.

Proof. We have to show that

$$\operatorname{Ker}\Phi_n=\mathscr{X}_n\cdot\mathscr{U}_n^+\cdot J_n(S_n),$$

where $S_n=\mathbf{Z}C(p^{n+1})/c_n$.

It is clear by Kummer's lemma that

$$\operatorname{Ker}\Phi_n=J_n\{U(S_n)\times U(\mathscr{A}_n)\}\subset\mathscr{X}_n\cdot\mathscr{U}_n^+\cdot J_n(S_n).$$

(Compare Section 3.)

Obviously, $\mathscr{X}_n\subset J_nU(\mathscr{A}_n)$.

Thus, the only non-trivial statement is

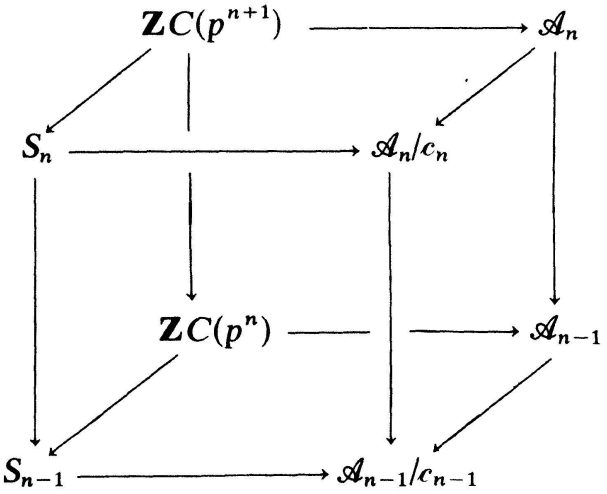
$$\mathscr{U}_n^+\subset\operatorname{Im}J_n.$$

We prove this by induction on n, using the regularity of p and of course the results in Section 4.

First, there is a projection of the fibre product

$$\begin{array}{ccc} \mathbf{Z}C(p^{n+1}) & \longrightarrow & \mathscr{A}_n \\ \downarrow & & \downarrow \\ S_n & \longrightarrow & \mathscr{A}_n/c_n \end{array}$$

to its analogue for $n-1$. This projection yields a commutative cube



where the projection $\mathscr{A}_n \to \mathscr{A}_{n-1}$ merely forgets the last component in A_n.

This diagram provides a map π of exact sequences

$$\begin{array}{ccccccc} U(S_n)\times U(\mathscr{A}_n) & \xrightarrow{J_n} & U(\mathscr{A}_n/c_n) & \xrightarrow{\Phi_n} & W_n & \longrightarrow & 0 \\ \downarrow{\scriptstyle \pi_0} & & \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi} & & \\ U(S_{n-1})U(\mathscr{A}_{n-1}) & \xrightarrow{J_{n-1}} & U(\mathscr{A}_{n-1}/c_{n-1}) & \xrightarrow{\Phi_{n-1}} & W_{n-1} & \longrightarrow & 0 \end{array}$$

Since $U(\mathscr{A}_n) = U(\mathscr{A}_{n-1}) \times U(A_n)$, and $\pi_0 \mid U(\mathscr{A}_n)$ simply drops the last component, it follows that π_0 is surjective. On $U(S_{n-1})$ the surjectivity of π_0 is evident since an element of $S_{n-1} = \mathbf{Z}C(p^n)/c_{n-1}$ is a unit if and only if as a polynomial in $t = x-1$, its constant term is prime to p. For p odd, it follows that π_0 is surjective on symmetric elements.

Thus, given a symmetric unit $u \in U(\mathscr{A}_n/c_n)$, in order to show that $u \in \operatorname{Im} J_n$ we may assume using induction on n that $\pi_1(u) = 1$. (For $p=2$, this argument definitely breaks down. We do not know whether or not Theorem 5.1 survives in that particular case.)

Now, using the decomposition

$$U(\mathscr{A}_n/c_n) = U(\mathbf{Z}/p^{n+1}\mathbf{Z}) \times \prod_{\nu=0}^{n} U(A_\nu/p^{n-\nu}t_0A_\nu),$$

we can write u in components $u = v \cdot u_0 \cdot u_1 \cdot \cdots \cdot u_n$ with $v \in U(\mathbf{Z}/p^{n+1}\mathbf{Z})$ and $u_\nu \in U(A_\nu/p^{n-\nu}t_0A_\nu)$. The induction hypothesis $\pi_1(u) = 1$ means that $v \equiv 1 \bmod p^n\mathbf{Z}$ and $u_\nu \equiv 1 \bmod p^{n-\nu-1}t_0A_\nu$ for $\nu = 0, 1, \ldots, n-1$.

It is clear that each u_ν, $\nu = 0, \ldots, n-1$ is symmetric.

We need the following lemma:

LEMMA 5.2. *We have*

$$v, u_0, \ldots, u_{n-1} \in U^+(A_n/t_0A_n) \cdot J_n(U(S_n)),$$

where $U^+(A_n/t_0A_n)$ *denotes the subgroup of symmetric units in* $U(A_n/t_0A_n)$.

Observing that A_n/t_0A_n is precisely the ring $R_n = \mathbf{F}_p[t]/(t^{p^n})$ of Section 4 (under the correspondence $t \leftrightarrow \zeta_n - 1$), we know from Section 4 that

$$U^+(A_n/t_0A_n) \subset jU(A_n) \subset J_nU(\mathcal{A}_n)$$

if p is a regular prime.

Therefore, Lemma 5.2 will imply that $v \cdot u_0 \cdot \cdots \cdot u_{n-1} \operatorname{Im} J_n$ and since $u_n \in U^+(A_n/t_0A_n) \subset J_nU(\mathcal{A}_n)$, this yields $u_\nu \in \operatorname{Im} J_n$ and Theorem 5.1 follows.

Proof of Lemma 5.2. We give the argument for u_ν, $\nu = 0, \ldots, n-1$. The argument for v is similar and left to the reader.

Write $u_\nu = 1 + p^{n-\nu-1}t_0a$ and choose a lift $z \in S_n = \mathbf{Z}C(p^{n+1})/c_n$ of a arbitrarily. (The composition $\mathbf{Z}C(p^{n+1}) \to \mathbf{Z} \times \prod_{\nu=0}^n A_\nu \to A_\nu$ is surjective for each ν.) Set

$$w = 1 + (x^{p^\nu} - 1) \prod_{\lambda=\nu+1}^{n-1} (1 + x^{p^\lambda} + \cdots + x^{(p-1)p^\lambda}) \cdot z,$$

regarded as an element of $U(S_n)$.

We look at the components of $J_n(w)$ in $U(\mathcal{A}_n/c_n) = U(\mathbf{Z}/p^{n+1}\mathbf{Z}) \times \prod_{\lambda=0}^n U(A_\lambda/p^{n-\lambda}t_0A_\lambda)$. It is clear that all components of $J_n(w)$ are 1 except the one in $U(A_\nu/p^{n-\nu}t_0A_\nu)$ which equals u_ν and a possibly non-trivial component w_n in the last factor $w_n \in U(A_n/t_0A_n)$.

Therefore,

$$u_\nu \equiv w_n^{-1} \bmod J_nU(S_n),$$

with $w_n \in U(A_n/t_0A_n)$.

It remains to secure a symmetric w_n. Let p^N be the order of u. Then, $u_\nu = (u_\nu c u_\nu)^{(1/2)(p^N+1)}$ since p is odd, and so, replacing w by $(w \cdot cw)^{(1/2)(p^N+1)}$ if necessary, we get a symmetric w_n.

This completes the proof of Lemma 5.2 and thus of Theorem 5.1.

A more explicit description of W_n appears in S. Galovich's paper [6].

§6. Direct method for $n = 1$

For $n = 1$, the cokernel of the map

$$j: U(\mathbf{Z}C_p) \times E_1 \to U(\mathbf{F}_p[x]/(x^p - 1))$$

can be calculated for p a semi-regular prime without appeal to class field theory.

Recall that E_1 denotes the group of units in $\mathbf{Z}[\zeta_1]$, where ζ_ν is a primitive $p^{\nu+1}$-st root of unity and j is the restriction to units of the map of rings sending a generator of C_p to x and ζ_1 to x.

THEOREM 6.1. *If p is a semi-regular odd prime, there is an exact sequence*

$$0 \to (\tfrac{1}{2}(p-3) + \delta_p) \cdot \mathbf{Z}/p\mathbf{Z} \to \tilde{K}_0(\mathbf{Z}C_{p^2}) \to \tilde{K}_0(\mathbf{Z}[\zeta_0]) \times \tilde{K}_0(\mathbf{Z}[\zeta_1]) \to 0,$$

where δ_p is the number of Bernoulli numbers among $B_2, B_4, \ldots, B_{p-3}$ whose numerator is divisible by p.

Using the Milnor–Mayer–Vietoris sequence of Section 1, the theorem is equivalent to

$$\operatorname{Coker} j \cong (\tfrac{1}{2}(p-3) + \delta_p) \cdot \mathbf{Z}/p\mathbf{Z}.$$

We prove this in two steps. Step 1. $j(U(\mathbf{Z}C_p)) \subset j(E_1)$. Thus $\operatorname{Coker} j = \operatorname{Coker} j \mid E_1$; Step 2. $\operatorname{Coker}\{j: E_1 \to U(R_1)\} \cong (\tfrac{1}{2}(p-3) + \delta_p) \cdot \mathbf{Z}/p\mathbf{Z}$, where $R_1 = \mathbf{F}_p[x]/(x^p - 1)$.

Step 1. Set $t = x - 1$. Thus, $R_1 = \mathbf{F}_p[t]/(t^p)$. Consider the commutative diagram

$$\begin{array}{ccc} U(\mathbf{Z}C_p) & \xrightarrow{j} & U(R_1) \\ \downarrow & & \downarrow \theta \\ E_0 & \xrightarrow{j_0} & U(\mathbf{F}_p[t]/(t^{p-1})), \end{array}$$

where $E_0 = U(\mathbf{Z}[\zeta_0])$. The left vertical map sends a generator of C_p to ζ_0. The map j_0 sends ζ_0 to $1 + t$. It is well defined since ζ_0 is a root of the polynomial

$1+X+\cdots+X^{p-1}$ and in $\mathbf{F}_p[X]$, we have

$$1+X+\cdots+X^{p-1}=\frac{X^p-1}{X-1}=\frac{(X-1)^p}{X-1}=(X-1)^{p-1}.$$

Finally θ is the obvious map reducing mod (t^{p-1}).

Observe first that the kernel of θ is generated by the unit $1+t^{p-1}$ which belongs to $j(E_1)$. In fact,

$$\begin{aligned} j\{(\zeta_1^{1+p}-1)/(\zeta_1-1)\} &= j(1+\zeta_1+\cdots+\zeta_1^p)=1+x+\cdots+x^p \\ &= 1+(1+x+\cdots+x^{p-1})=1+(x-1)^{p-1}=1+t^{p-1}. \end{aligned}$$

Therefore, it suffices to prove

$$j_0(E_0)\subset \theta j(E_1).$$

Let E_0^* be the subgroup of circular units in E_0, i.e. the subgroup of E_0 generated by $\pm\zeta_0$ and the units of the form $(\zeta_0^s-1)/(\zeta_0-1)$, where s is prime to p.

We use the classical result in the theory of cyclotomic fields:

The index $[E_0:E_0^*]$ *equals the class number* h_0^+ *of the maximal real subfield* $Q(\zeta_0+\zeta_0^{-1})$ *of* $Q(\zeta_0)$.

A proof is given in Borevich–Shafarevich [4], Theorem 2, Chap. 5, Sec. 5, page 362.

Thus our hypothesis, p a semi-regular prime, implies that $[E_0:E_0^*]$ is prime to p.

The group $U(\mathbf{F}_p[t]/(t^{p-1}))$ splits as a direct product $\mathbf{F}_p^{\cdot}\times U_0$, where U_0 is the subgroup of unipotent units, congruent 1 mod (t). The factor $\mathbf{F}_p^{\cdot}$ is contained in $\theta j(E_1)$. For s prime to p, $(\zeta_0^s-1)/(\zeta_0-1)$ is a unit in $\mathbf{Z}[\zeta_1]$, with e.g. $\zeta_0=\zeta_1^p$, and

$$\theta j\{(\zeta_0^s-1)/(\zeta_0-1)\}=\theta j(1+\zeta_0+\cdots+\zeta_0^{s-1})=1+x^p+\cdots+x^{p(s-1)}=s.$$

Thus, we only have to worry about the unipotent component of $j_0(E_0)$. But, U_0 is clearly a p-group. Since the index $[E_0:E_0^*]$ is prime to p, it follows that the unipotent components of $j_0(E_0)$ and $j_0(E_0^*)$ are equal. It thus suffices to prove that $j_0(E_0^*)\subset\theta j(E_1)$. Trivial magic does this. Namely,

$$j_0\{(\zeta_0^s-1)/(\zeta_0-1)\}=1+x+\cdots+x^{s-1}=\theta j\{(\zeta_1^s-1)/(\zeta_1-1)\}.$$

Step 2. We now come to the proof of

$$\text{Coker}\,\{j:E_1\to U(R_1)\}\cong(\tfrac{1}{2}(p-3)+\delta_p)\cdot\mathbf{Z}/p\mathbf{Z}.$$

Again, since the kernel of θ is generated by $1+t^{p-1}$ which belongs to the image of j, as we have just seen, the assertion is equivalent to

$$\text{Coker } \theta j \cong (\tfrac{1}{2}(p-3)+\delta_p)\cdot \mathbf{Z}/p\mathbf{Z}.$$

Also, $\mathbf{F}_p^{\cdot} \subset \text{Im } \theta j$, so we concentrate on the unipotent component of $\theta j(E_1)$.

Let E_1^* be the subgroup of E_1 generated by the circular units $\pm\zeta_1$ and $(\zeta_1^s-1)/(\zeta_1-1)$ with s prime to p. Again, *the index* $[E_1 : E_1^*]$ *is finite and equal to the class number* h_1^+ *of the maximal real subfield* $Q(\zeta_1+\zeta_1^{-1})$ *of* $Q(\zeta_1)$. (See [8], Satz 3, page 24.

Remark. Actually, the result we use is a slight variation of what we have quoted. But it is easily seen that these are equivalent.

On the other hand, h_0^+ prime to p implies h_n^+ prime to p for all $n=0$ by Iwasawa [11]. It follows that the unipotent components of $\theta j(E_1)$ and $\theta j(E_1^*)$ are equal.

An easy calculation shows that the unipotent component of $\theta j(E_1^*)$ is generated by $u_1 = \theta j(\zeta_1)$ and the units

$$u_r = \theta j\{(\zeta_1^r-1)(\zeta_0-1)/(\zeta_1-1)(\zeta_0^r-1)\},$$

for $r=2,\ldots,p-2$.

We introduce the map

$$\log : U_0 \to T,$$

where T is the ideal of t in $\mathbf{F}_p[t]/(t^{p-1})$, and

$$\log(1+f) = f-\tfrac{1}{2}f^2+\cdots+\frac{1}{p-2}f^{p-2}, \qquad f\in T.$$

Actually, log is an isomorphism. U_0 is a multiplicative vector space over $\mathbf{F}_p$ of dimension $p-2$ with basis $1+z$, $1+z^2,\ldots,1+z^{p-2}$, where z is any element in T, $z\notin T^2$. The logarithms $\log(1+z)$, $\log(1+z^2),\ldots,\log(1+z^{p-2})$ form a basis of T. We now choose z such that $x=e^z$, i.e.

$$z=\log x=\log(1+t)=t-\tfrac{1}{2}t^2+\cdots+\frac{1}{p-2}t^{p-2}.$$

We have $u_1=\theta j\zeta_1 = x = e^z$, and

$$u_r=\frac{1}{r}(1+x+\cdots+x^{r-1})=\frac{e^{rz}-1}{rz}\cdot\left(\frac{e^z-1}{z}\right)^{-1}$$

for $r=2,\ldots,p-2$. It follows that

$$\log u_1 = z, \quad \log u_r = \log\left(\frac{e^{rz}-1}{rz}\right) - \log\left(\frac{e^z-1}{z}\right),$$

for $r=2,\ldots,p-2$.

We seek a formula expressing $\log(e^X-1)/X$.

Recall the definition of the Bernoulli numbers

$$\frac{X}{e^X-1} = 1 + \sum_{s=1}^{\infty} (B_s/s!)X^s$$

in $\mathbf{Q}[[X]]$. We review the properties of the Bernoulli numbers B_s which we need.

First $B_1 = \frac{1}{2}$. Next, write $f(X) = X/(e^X-1) - 1 + \frac{1}{2}X$. It is easily verified that $f(-X) = f(X)$. Hence,

(*) *B_s vanishes for s odd >1.*

Now, an easy calculation shows that

$$\frac{d}{dX}\log\left(\frac{e^X-1}{X}\right) - \frac{1}{2} = \frac{1}{X}\left(\frac{X}{e^X-1} - 1 + \tfrac{1}{2}X\right) = \sum_{s=2}^{\infty} (B_s/s!)X^{s-1},$$

and integrating formally,

$$\log\left(\frac{e^X-1}{X}\right) = \tfrac{1}{2}X + \sum_{s=2}^{\infty} (B_s/s\cdot s!)X^s.$$

Thus, in $Q[X]/(X^{p-1})$ we have

$$\log\left(\frac{e^X-1}{X}\right) = \log\left(1 + \frac{X}{2!} + \cdots + \frac{X^{p-2}}{(p-1)!}\right) \in \mathbf{Z}\left[\frac{1}{(p-1)!}\right][X]/(X^{p-1}).$$

Therefore,

(**) *The denominators of $B_2, B_4, \ldots, B_{p-3}$ are not divisible by p.*

It follows that

$$\log\left(\frac{e^z-1}{z}\right) = \tfrac{1}{2}z + \sum_{s=2}^{p-2} (B_s/s\cdot s!)\cdot z^s$$

makes sense and holds true in $\mathbf{F}_p[t]/(t^{p-1})$ for any z in T, the ideal generated by t.

Going back to the calculation of $\log u_r$, we get

$$\log u_1 = z,$$

$$\log u_r = \tfrac{1}{2}rz + \sum_{s=2}^{p-2} (B_s/s \cdot s!)(rz)^s - \tfrac{1}{2}z - \sum_{s=2}^{p-2} (B_s/s \cdot s!)z^s$$

$$= \tfrac{1}{2}(r-1)z + \sum_{s=2}^{p-2} \frac{r^s - 1}{s \cdot s!} \cdot B_s z^s,$$

for $r = 2, \ldots, p-2$. •

Thus, we observe that modulo the subspace $\mathbf{F}_p z$ of the vector space T over $\mathbf{F}_p$, the elements $\log u_2, \ldots, \log u_{p-2}$ are the transforms of the basis $z^2, \ldots, z^{p-2}$ of $T/\mathbf{F}_p z$ by the matrix M, where

$$M_{ij} = \frac{i^j - 1}{j \cdot j!} \cdot B_j, \qquad 2 \leqq i, j \leqq p-2.$$

But, $M = A \cdot B$, where $A_{ik} = (i^k - 1)/k \cdot k!$ and B is the diagonal matrix of Bernoulli numbers diag $(B_2, B_3, \ldots, B_{p-2})$.

The first factor A is invertible as a matrix over $\mathbf{F}_p$ as is easily verified. The second has rank $\frac{1}{2}(p-3) - \delta_p$, where δ_p is the number of Bernoulli numbers among $B_2, B_4, \ldots, B_{p-3}$ which vanish mod p. ($B_3 = B_5 = \cdots = B_{p-2} = 0$.)

The rank of the subgroup of U_0 generated by $u_1, \ldots, u_{p-2}$ is thus seen to be $1 + \frac{1}{2}(p-3) - \delta_p = \frac{1}{2}(p-1) - \delta_p$. The cokernel of j has therefore the rank $p-2-\frac{1}{2}(p-1) + \delta_p = \frac{1}{2}(p-3) + \delta_p$ as asserted.

This finishes the proof of Theorem 5.1.

§7. Calculation of $\tilde{K}_0(\mathbf{Z}C_{15})$

Let ω, ζ, $\omega\zeta$ denote primitive 3-rd, 5-th and 15-th roots of unity respectively. Consider the map

$$i_*: \tilde{K}_0(\mathbf{Z}C_{15}) \to \tilde{K}_0(\mathbf{Z}[\omega]) \times \tilde{K}_0(\mathbf{Z}[\zeta]) \times \tilde{K}_0(\mathbf{Z}[\omega\zeta])$$

induced by the inclusion of $\mathbf{Z}C_{15}$ in the maximal order of $\mathbf{Q}C_{15}$.

We shall prove that Ker $i_* \cong \mathbf{Z}/2\mathbf{Z}$. On the right hand side, the factors $\tilde{K}_0(\mathbf{Z}[\omega])$, $\tilde{K}_0(\mathbf{Z}[\zeta])$ and $\tilde{K}_0(\mathbf{Z}[\omega\zeta])$ are isomorphic to the ideal class groups of $\mathbf{Q}(\omega)$, $\mathbf{Q}(\zeta)$ and $\mathbf{Q}(\omega\zeta)$ respectively. It is easily verified that all three class groups

are zero. This yields:

THEOREM 7.1. $\tilde{K}_0(\mathbf{Z}C_{15}) \cong \mathbf{Z}/2\mathbf{Z}$.

Thus, in the case of a cyclic group of composite order (here C_{15}), Ker i_* may involve primes which do not divide the order of the group.

The proof is by direct calculation.

We start with the fibre product

$$\begin{array}{ccc} \mathbf{Z}C_{15} & \longrightarrow & \mathbf{Z}[\zeta]C_3 \\ \downarrow & & \downarrow \\ \mathbf{Z}C_3 & \longrightarrow & \mathbf{F}_5C_3 \end{array}$$

and the resulting exact sequence as in Section 1,

$$U(\mathbf{Z}C_3) \times U(\mathbf{Z}[\zeta]C_3) \to U(\mathbf{F}_5C_3) \to \tilde{K}_0(\mathbf{Z}C_{15}) \to \tilde{K}_0(\mathbf{Z}C_3) \times \tilde{K}_0(\mathbf{Z}[\zeta]C_3) \to 0.$$

We want to prove

(1) $\tilde{K}_0(\mathbf{Z}[\zeta]C_3) \cong \tilde{K}_0(\mathbf{Z}[\zeta]) \times \tilde{K}_0(\mathbf{Z}[\omega\zeta])$,

(2) Coker $\{j : U(\mathbf{Z}C_3) \times U(\mathbf{Z}[\zeta]C_3) \to \mathbf{F}_5C_3\} \cong \mathbf{Z}/2\mathbf{Z}$.

This will yield the desired result, since $\tilde{K}_0(\mathbf{Z}C_3) \cong \tilde{K}_0(\mathbf{Z}[\omega])$ by Rim's theorem.

We begin with the calculation of $\tilde{K}_0(\mathbf{Z}[\zeta]C_3)$. Consider the fibre product

$$\begin{array}{ccc} \mathbf{Z}[\zeta]C_3 & \longrightarrow & \mathbf{Z}[\omega\zeta] \\ \downarrow & & \downarrow \\ \mathbf{Z}[\zeta] & \longrightarrow & \mathbf{F}_3[\zeta], \end{array}$$

with the obvious maps. It is easy to check that $\mathbf{F}_3[\zeta] = \mathbf{F}_3[X]/(1+X+X^2+X^3+X^4)$ is a field. (Indeed, 3^4 is the lowest power of 3 which is congruent 1 mod 5 and thus $\mathbf{F}_{3^4}$ is the smallest field in characteristic 3 containing a primitive 5-th root of unity.) We write $\mathbf{F}_3(\zeta)$ instead of $\mathbf{F}_3[\zeta]$.

Moreover, $U(\mathbf{Z}[\omega\zeta]) \to U(\mathbf{F}_3(\zeta))$ is surjective because $\omega - \zeta$ is a unit in $\mathbf{Z}[\omega\zeta]$, with inverse $\zeta^2 - \omega(1+\zeta^3)$, and $\omega - \zeta$ projects to $1 - \zeta \in \mathbf{F}_3(\zeta)$ which generates the cyclic group of non-zero elements (of order 80).

It follows that the sequence

$$U(\mathbf{Z}[\zeta]) \times U(\mathbf{Z}[\omega\zeta]) \to U(\mathbf{F}_3(\zeta)) \to \tilde{K}_0(\mathbf{Z}[\zeta]C_3) \to \tilde{K}_0(\mathbf{Z}[\zeta]) \times \tilde{K}_0(\mathbf{Z}[\omega]) \to 0$$

yields the assertion (1).

For use in proving (2), we note that the above fibre product also yields the following information.

A unit in $\mathbf{Z}[\omega\zeta]$ is the image of a unit in $\mathbf{Z}[\zeta]C_3$ if and only if its projection to $\mathbf{F}_3(\zeta)$ is in the image of $U(\mathbf{Z}[\zeta]) \to U(\mathbf{F}_3(\zeta))$.

We now show that this image consists precisely of the squares in $U(\mathbf{F}_3(\zeta))$.

It is well known that $U(\mathbf{Z}[\zeta])$ is the direct product of its torsion subgroup generated by $-\zeta$ and an infinite cyclic group generated by the fundamental unit $\varepsilon = \zeta^{-1} + 1 + \zeta$.

It is somewhat more convenient to work with the generators $-\zeta$ and $\zeta\varepsilon = 1 + \zeta + \zeta^2$. In $\mathbf{F}_3(\zeta)$, we have

$$1 + \zeta + \zeta^2 = 1 - 2\zeta + \zeta^2 = (1-\zeta)^2, \quad -\zeta = (1-\zeta)^{72}.$$

Therefore, we have the following criterion:

A unit in $\mathbf{Z}[\omega\zeta]$ is the image of a unit in $\mathbf{Z}[\zeta]C_3$ if and only if its projection into $\mathbf{F}_3(\zeta)$ is an even power of $1-\zeta$.

Using this, we proceed to prove (2), i.e.

$$\text{Coker}\{j : U(\mathbf{Z}C_3) \times U(\mathbf{Z}[\zeta]C_3) \to U(\mathbf{F}_5C_3)\} \cong \mathbf{Z}/2\mathbf{Z}.$$

First, every unit in $\mathbf{Z}C_3$ can be regarded as a unit in $\mathbf{Z}[\zeta]C_3$ under the obvious inclusion $\mathbf{Z}C_3 \to \mathbf{Z}[\zeta]C_3$. Moreover, $u \in U(\mathbf{Z}C_3)$ and the corresponding element in $U(\mathbf{Z}[\zeta]C_3)$ have the same j-image in $\mathbf{F}_5C_3$. It suffices therefore to prove that

$$\text{Coker}\{j : U(\mathbf{Z}[\zeta]C_3) \to U(\mathbf{F}_5C_3)\} \cong \mathbf{Z}/2\mathbf{Z}.$$

We use the diagram (no, not a fibre product):

$$\begin{array}{ccc} U(\mathbf{Z}[\zeta]C_3) & \xrightarrow{i_1 \times i_2} & U(\mathbf{Z}[\zeta]) \times U(\mathbf{Z}[\omega\zeta]) \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j'} \quad \downarrow{\scriptstyle j''} \\ U(\mathbf{F}_5C_3) & \longrightarrow & U(\mathbf{F}_5) \times U(\mathbf{F}_5(\omega)), \end{array}$$

where $i_1(x) = 1$, $i_2(x) = \omega$ with x a generator of C_3, and $j'(\zeta) = 1$, $j''(\zeta) = 1$.

LEMMA 7.2. *If $u \in U(\mathbf{Z}[\omega\zeta])$ belongs to* Ker j'', *then $u = i_2(v)$ for some $v \in U(\mathbf{Z}[\zeta]C_3)$.*

Proof. Let $f : \mathbf{Z}[\omega\zeta] \to \mathbf{F}_3(\zeta)$ be the projection with $f(\omega) = 1$. By the criterion above, $u \in i_2\{U(\mathbf{Z}[\zeta]C_3)\}$ if and only if $f(u)$ is a square.

In order to calculate $f(u)$, we use the commutative diagram

$$\begin{array}{ccc} \mathbf{Z}[\omega\zeta] & \xrightarrow{f} & \mathbf{F}_3(\zeta) \\ \downarrow N & & \downarrow \text{squaring} \\ \mathbf{Z}[\zeta] & \xrightarrow{\rho} & \mathbf{F}_3(\zeta), \end{array}$$

where ρ is reduction mod 3 and $N:\mathbf{Z}[\omega\zeta]\to\mathbf{Z}[\zeta]$ is the norm map. Since Nu is a unit in $\mathbf{Z}[\zeta]$ it must be of the form $Nu=(-\zeta)^\lambda(1+\zeta+\zeta^2)^\mu$. We claim that μ is even. Look at the composition $\mathbf{Z}[\omega\zeta]\xrightarrow{N}\mathbf{Z}[\zeta]\to\mathbf{F}_5$. The unit Nu projects to $(-1)^\lambda 3^\mu$. On the other hand, since $j''(u)=1$, we have $u=1+(1-\zeta)(a+b\omega)$ for some $a, b\in\mathbf{Z}[\zeta]$. It follows that Nu projects to 1 in $\mathbf{F}_5$. Combining the two, we must have

$$(-1)^\lambda 3^\mu = 1 \bmod 5.$$

This is possible only if μ is even. Write $\mu=2m$.

Coming back to the diagram, we have

$$f(u)^2=\rho Nu=\rho\{(-\zeta)^\lambda(1+\zeta+\zeta^2)^{2m}\}=(1-\zeta)^{4m+72\lambda},$$

and hence $f(u)=\pm(1-\zeta)^{2m+36\lambda}$ which is a square since $-1=(1-\zeta)^{40}$. We conclude that $u\in i_2\{U(\mathbf{Z}[\zeta]C_3)\}$ and Lemma 7.2 is proved.

It is now easy to show that $\operatorname{Coker} j\cong\mathbf{Z}/2\mathbf{Z}$.

Identifying $\mathbf{F}_5C_3$ with $\mathbf{F}_5\times\mathbf{F}_5(\omega)$ under $x\to(1,\omega)$, where x is a choice of generators of C_3, observe first that the unit $-x(1+\zeta x)\in\mathbf{Z}[\zeta]C_3$, with inverse $-x^2(1+\zeta+\zeta^2)(1-\zeta x+\zeta^2x^2)$, maps by j to $j(-x(1+\zeta x))=(3,1)\in\mathbf{F}_5^\cdot\times\mathbf{F}_5(\omega)^\cdot$. Hence, the factor $\mathbf{F}_5^\cdot\times\{1\}$ is in the image of j and thus $\operatorname{Coker} j=\operatorname{Coker}(j''\cdot i_2)$.

Now, $\mathbf{F}_5(\omega)^\cdot$ is generated by $\omega-1$ of order 24 and $\omega-1=j''(\omega-\zeta)$.

By the criterion above, we know that $(\omega-\zeta)^2\in i_2\{U(\mathbf{Z}[\zeta]C_3)\}$. Thus, $(\omega-1)^2\in\operatorname{Im}(j''\cdot i_2)$.

It remains to show that $\omega-1\notin\operatorname{Im}(j''\cdot i_2)$. But, if $j''(\omega-\zeta)=\omega-1=j''i_2w$, then $u=(\omega-\zeta)\cdot i_2(w^{-1})\in\operatorname{Ker} j''$.

By Lemma 7.2, this implies $u=i_2(v)$ for some $v\in U(\mathbf{Z}[\zeta]C_3)$, and consequently $\omega-\zeta=i_2(vw)\in\operatorname{Im} i_2$. This contradicts the criterion above, since $f(\omega-\zeta)=1-\zeta$ is not a square in $\mathbf{F}_3(\zeta)$.

This completes the proof of $\operatorname{Ker} i_*\cong\mathbf{Z}/2\mathbf{Z}$, where

$$i_*:\tilde{K}_0(\mathbf{Z}C_{15})\to\tilde{K}_0(\mathbf{Z}[\omega])\times\tilde{K}_0(\mathbf{Z}[\zeta])\times\tilde{K}_0(\mathbf{Z}[\omega\zeta]).$$

The verification that the ideal class groups of $\mathbf{Q}(\omega)$, $\mathbf{Q}(\zeta)$ and $\mathbf{Q}(\omega\zeta)$ are zero is easy and left to the reader.

BIBLIOGRAPHY

[1] ARTIN, E. and TATE, J., *Class Field Theory*, Benjamin (1968).
[2] BASS, H., *Algebraic K-Theory*, Benjamin (1968).
[3] BASS, H. and MURTHY, P., *Grothendieck groups and Picard groups of abelian group rings*, Ann. of Math. *86* (1967), 16–73.
[4] BOREVICH, Z. I. and SHAFAREVICH, J. R., *Number Theory*, Academic Press, New York (1966).
[5] FRÖHLICH, A., *On the classgroup of integral group rings of finite abelian groups I, II*, Mathematika *16* (1969), 143–152 and *19* (1972), 51–56.
[6] GALOVICH, S., *The class group of a cyclic p-group*, Journal of Algebra *30* (1974), 368–387.
[7] HASSE, H., *Vorlesungen über Klassenkörpertheorie*, Physica Verlag, Würzburg (1967).
[8] HASSE, H., *Ueber die Klassenzahl abelscher Zahlkörper*, Akademie Verlag, Berlin (1952).
[9] HECKE, E., *Vorlesungen über die Theorie der algebraischen Zahlen*, Chelsea, New York (1948).
[10] HIGMAN, G., *The units of group rings*, Proc. London Math. Soc. *46* (1940), 231–248.
[11] IWASAWA, K., *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg *20* (1956), 257–258.
[12] IWASAWA, K., *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. *65* (1959), 183–226.
[13] IWASAWA, K., *On the theory of cyclotomic fields*, Ann. of Math. *70* (1959), 530–561.
[14] IWASAWA, K., *On some modules in the theory of cyclotomic fields*, J. Math. Soc. Japan *16* (1964), 42–82.
[15] IWASAWA, K. and SIMS, C., *Computation of invariants in the theory of cyclotomic fields*, J. Math. Soc. Japan *18* (1966), 86–96.
[16] LANG, S., *Algebraic number theory*, Addison-Wesley, 2nd edition (1970).
[17] MILNOR, J., *Introduction to algebraic K-theory*, Annals of Math. Studies 72, Princeton Univ. Press (1971).
[18] RIM, D. S., *Modules over finite groups*, Ann. of Math. *69* (1959), 700–712.
[19] SERRE, J. P., *Classes des corps cyclotomiques*, Séminaire Bourbaki, Exposé 174 (1958/1959).
[20] ULLOM, S., *A note on the class group of integral group rings of some cyclic groups*, Mathematika *17* (1970), 79–81.

Institut de Mathématiques
2–4, rue du Lièvre
1211 Genève

University of Chicago
Chicago, Illinois

Received September 1976