TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 271, Number 2, June 1982

ON THE CONSTRUCTION OF RELATIVE GENUS FIELDS[1]

BY

GARY CORNELL

ABSTRACT. We show how to construct the relative genus field in many cases. This is then applied to constructing fields with interesting class groups.

Introduction. One way to get information about the Hilbert class field of a number field E, H_E, and thus about the class group of E, C_E, is to study the largest subfield of H_E of the form EF_* where F_* is an abelian extension of some subfield F of E. The maximal such field is called the genus field of E relative to F, and we denote it by E_F^*.

The case when $F = Q$, the so-called absolute genus field, was first studied by Frohlich [**5, 6**]. In the relative case a very useful formula for the degree of E_F^*/F is due to Furuta [**7**]. Nonetheless it is often useful to construct the genus field explicitly. The project in the absolute case was carried out by Ishida in a series of papers which culminated in his monograph [**8**]. Among the reasons for believing that an explicit construction will be useful are the following: The given field E may contain two different subfields F and F' and perhaps the respective relative genus fields are disjoint. This would give more information about C_E than would be available from a formula. Also, if the method of constructing relative genus fields were somehow 'canonical' then it might be possible to show that certain classes of fields have class groups with interesting properties precisely because they would have a properly larger relative genus field with respect to some subfield. We give examples of this in the last section when we prove that any finite abelian group is the subgroup of the class group of an explicitly describable full cyclotomic field. While the fact that any finite abelian group is a subgroup of the class group of some abelian extension of Q is well known (see Washington [**12**] for a proof), it is easy to see that these ideal classes capitulate in the abelian closure of Q and in fact do not even survive to the full cyclotomic field with the same conductor as the given abelian number field. (This is because the ideal classes constructed come from the absolute genus field of the abelian extension and ultimately depend on the fact that a cyclic extension of Q, of degree and odd prime l, with two ramified primes, has an element of order l in the class group because there is an absolutely abelian extension of degree l^2 containing it which is unramified over it.)

Received by the editors December 18, 1979 and, in revised form, August 7, 1980.

1980 *Mathematics Subject Classification.* Primary 12A65; Secondary 12A50.

[1]This represents part of the author's Ph.D. dissertation written under the direction of Professor M. Rosen at Brown University.

0002-9947/81/0000-1072/$03.75

Other examples of the usefulness of the explicit construction, which will be given in subsequent papers, are to fields with infinite l-class field towers [**2**] and the existence of fields with class number > 1 in the (unique) $\hat{Z}$ extension of Q [**3**]. (By the $\hat{Z}$ extension of Q we mean the composite of all Z_p extensions for every prime p.)

The first section is preliminary and contains, among other things, a proof of what is often called "Abhyankar's lemma." This is probably the simplest method of insuring that composites produce unramified extensions. Since proofs of this result are not easily available, I have taken the liberty of including one. In addition, since most of our constructions will depend on class field theory, I have summarized the needed results here. Finally, a result on when the intersection of two ray class fields is trivial is also included. This is useful, in among other places, when discussing the relations between genus fields relative to different subfields. The next section contains the main results about the explicit construction of relative genus fields. Some of the results obtained here appear to contradict certain criticisms of Ishida's work made by Frey in [**4**]. (Note: The Frey who wrote the review is not the Frey referred to in the review as "the reviewer." This might otherwise lead the reader of the review to misunderstanding.) The third section contains some applications.

1. If $\mathfrak{a}$ is an ideal of a number field F then by $F^{\mathfrak{a}}$ we mean the (full) ray class field with conductor $\mathfrak{a}$. It contains the Hilbert class field of F, H_F, and its degree over F is $h_F \cdot |(\mathfrak{O}/\mathfrak{a})^*|/[U : U(\mathfrak{a})]$, where h_F is the class number of F, and U, respectively $U(\mathfrak{a})$, denotes the units, respectively the units congruent to 1 mod $\mathfrak{a}$ and $\mathfrak{O}$ is the ring of integers in F. Moreover, the Galois group of $F^{\mathfrak{a}}$ over H_F is isomorphic to the group $(\mathfrak{O}/\mathfrak{a})^*/U/U(\mathfrak{a})$. Notice the group $U/U(\mathfrak{a})$ is of finite rank as a Z-module because U is. Thus by making $\mathfrak{a}$ divisible by enough primes we can insure that the field $F^{\mathfrak{a}}$ properly contains H_F.

LEMMA 1. *Suppose* $\mathfrak{a}$ *is an ideal exactly divisible by* $\mathfrak{p}^n$, $n > 1$, $\mathfrak{p}$ *a prime. Set* $\mathfrak{b} = \mathfrak{a}\mathfrak{p}^{1-n}$; *then* $|F^{\mathfrak{a}} : F^{\mathfrak{b}}|$ *is a power of* p *where* p *is below* $\mathfrak{p}$ *in* Z.

PROOF. Without loss of generality we may assume that we are looking at the case $[F^{\mathfrak{a}} : F^{\mathfrak{b}}]$ where $\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{p}$ and $\mathfrak{p} \mid \mathfrak{b}$. Then by class field theory the index has order $[U(\mathfrak{a}) : U(\mathfrak{b})] \cdot |(\mathfrak{O}/\mathfrak{a})^*|/|(\mathfrak{O}/\mathfrak{b})^*|$. Now the Chinese remainder theorem implies that $|(\mathfrak{O}/\mathfrak{a})^*|/|(\mathfrak{O}/\mathfrak{b})^*|$ is a power of p. So there only remains the index on the left. We can define a homomorphism $U(\mathfrak{a}) \to \mathfrak{a}/\mathfrak{b}$ by $1 + \alpha \to \bar{\alpha}$. This a homomorphism because $(1 + \alpha)(1 + \beta)$ maps to $\bar{\alpha} + \bar{\beta}$ since $\alpha\beta \in \mathfrak{b}$. The kernel is clearly $U(\mathfrak{b})$. Now since $\mathfrak{a}/\mathfrak{b}$ is isomorphic to $\mathfrak{O}/\mathfrak{p}$ which does have order a power of p, the result follows:

PROPOSITION 1. *Any tamely ramified abelian extension* E *of a number field* F *is contained in* $F^{\mathfrak{a}}$ *where* $\mathfrak{a}$ *is an ideal not divisible by the square of any prime ideal.*

PROOF. First E will be contained in some ray class field $F^{\mathfrak{a}'}$ where $\mathfrak{a}'$ is divisible only by the primes that ramify in E. We use induction on the number of primes s that divide $\mathfrak{a}'$. If $s = 1$ then $|EF^{\mathfrak{p}} : F^{\mathfrak{p}}|$ is a power of p by the lemma above. Also $EF^{\mathfrak{p}}/F^{\mathfrak{p}}$ is totally ramified because $F^{\mathfrak{p}^n}/H_F$ is. But the ramification degree of $EF^{\mathfrak{p}}/F^{\mathfrak{p}}$ divides that of E/F. Since E/F is tamely ramified, the degree $|EF^{\mathfrak{p}} : F^{\mathfrak{p}}|$ must be one.

We may assume by induction that the result is true for less than n primes. Suppose $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$. If $a_1 > 1$, let E_1 be the fixed field of the inertia group of $\mathfrak{p}_1$ in E. Then E_1/F is ramified only at $\mathfrak{p}_2, \ldots, \mathfrak{p}_n$ and, therefore, by induction, $E_1 \subset F^{\mathfrak{b}'}$ where $\mathfrak{b}' = \mathfrak{p}_2 \cdots \mathfrak{p}_n$. Therefore, $E_1 \subset F^{\mathfrak{b}}$ where $\mathfrak{b} = \mathfrak{p}_1 \mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_n^{a_n}$. Now $[EF^{\mathfrak{b}} : F^{\mathfrak{b}}]$ divides $[F^{\mathfrak{a}} : F^{\mathfrak{b}}] = p_1^m$ by the lemma. Since E/E_1 is tamely and totally ramified at the primes above $\mathfrak{p}_1$, we have that $[E : E_1]$ is prime to p_1, so as before $[EF^{\mathfrak{b}} : F^{\mathfrak{b}}] = 1$ and $E \subset F^{\mathfrak{p}_1 \mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_n^{a_n}}$. If $a_2 > 1$ we may proceed similarly to conclude that $E \subset F^{\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3^{a_3} \cdots \mathfrak{p}_n^{a_n}}$; in finitely many steps we have the result.

REMARK. Another method of proof is to use the "conductor-discriminant formula." While perhaps less direct, the above proof is included because it is closer to the flavor of the rest of the paper.

Given that $E \supset F_1 F_2$ we will be constructing the genus field of E relative to F_1, respectively relative to F_2, by taking certain subfields of the ray class fields of F_1, respectively F_2. If we knew that the ray class fields were also disjoint, we could derive much more information about C_E [where C_E will mean the class group of E]. What follows then is a theorem which gives sufficient conditions for this to be true.

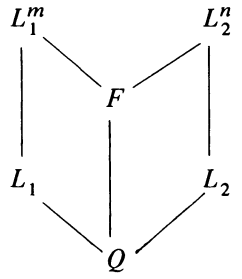
LEMMA 2. *Let $L \supset k$ be abelian, both fields normal over Q; let L' be another field, also normal over Q. If $L' \cap k = Q$, then $L \cap L'$ is abelian over Q.*

PROOF. By "Lagrange's theorem on natural irrationalities" $\mathrm{Gal}(L \cap L'/Q)$ is under the given hypothesis, isomorphic to $\mathrm{Gal}(L'k/k)$. This group is the homomorphic image of $\mathrm{Gal}(L/k)$ and so is abelian. The result follows.

Now look at L_1^m, L_2^n where m and n are integers from Z considered as integral ideals of L_1, respectively L_2.

THEOREM 1. *Suppose that n and the discriminant of L_2, $D(L_2)$, are relatively prime to $D(L_1)$. Then $F = L_1^m \cap L_2^n$ is abelian over Q and its conductor is divisible only by primes common to m and n.*

PROOF. The hypothesis on the discriminants implies that $L_1 \cap L_2^n = F$ is an unramified extension of Q and so must be Q. The previous lemma implies F is abelian over Q, since ray class fields for integral ideals are normal over Q. The statement on ramified primes follows by going up the LHS and RHS of the tower below:



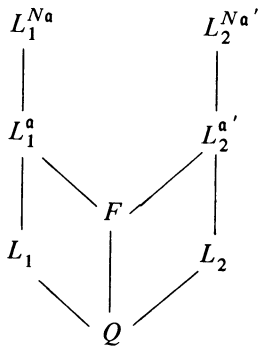
THEOREM 2. *Let $\mathfrak{a}$ be an ideal of L_1, $\mathfrak{a}'$ an ideal of L_2. Suppose that $\mathfrak{a}$ and $\mathfrak{a}'$ are not divisible by any proper ideal of Z. Suppose no prime dividing $\mathfrak{a}'$ and $D(k_2)$ ramifies in k_1; then $L_1^{\mathfrak{a}} \cap L_2^{\mathfrak{a}'} = Q$.*

PROOF. We know $L_1^{\mathfrak{a}} \subset L_1^{N(\mathfrak{a})/Q}$, $L_2^{\mathfrak{a}'} \subset L_2^{N(\mathfrak{a})/Q}$ and so

$$F = L_1^{\mathfrak{a}} \cap L_2^{\mathfrak{a}} \subset L_1^{N\mathfrak{a}} \cap L_2^{N\mathfrak{a}'} = F'.$$

Now by the previous theorem F' is abelian over Q and so F is a subfield of an abelian extension of Q and is in turn abelian.

In particular if p is a prime from Z ramified in F it is, say, the $e(p)$ power of an ideal in $\mathfrak{O}_F$. Now in the lattice of fields below:



p does not ramify in L_1 since, by hypothesis, no prime ramified in the RHS ramifies in L_1 and so $p = P_1 \cdots P_g$ in $\mathfrak{O}_{L_1}$. Now p is exactly the $e(p)$ power of an ideal in F and so is at least the $e(p)$ of an ideal in $L_1^{\mathfrak{a}}$ by unique factorization. Thus each of the p_i's $1 \leqslant i \leqslant g$, must ramify. Thus each P_i divides $\mathfrak{a}$ which contradicts the hypothesis that $\mathfrak{a}$ is not divisible by an ideal of Z.

We can extend the above trivially to

THEOREM 2'. *Let T be normal over Q. Suppose L_1, $L_1^{\mathfrak{a}}$ are as above. Then if $D(T)$ is prime to $D(L_1)$ we have $L_1^{\mathfrak{a}} \cap T = Q$.*

The next result to be taken up is "Abhyankar's lemma."

THEOREM 3. *Let E_1, E_2, F be local fields, E_1, E_2 finite extensions of F with ramification indices e_1, respectively e_2. Suppose E_2 is tamely ramified and $e_2 \mid e_1$. Then E_2E_1 is an unramified extension of E_1.*

PROOF. Let E_2^{nr} be the maximal unramified extension of F in E_2. So E_2 is totally ramified over E_2^{nr}. Now $E_1E_2^{nr}/E_1$ is unramified and so its ramification index over F is the same as E_1/F. So since the composite of an unramified extension with an unramified extension is unramified we may assume that E_2/F is totally and tamely ramified. Thus by the classification theorem for totally and tamely ramified extensions of local fields (see Lang [**11**, p. 52]), we know $E_2 = F(\pi^{1/e_2})$ for some prime element π in F. Now if Π is a prime element in E_1 we have $u\Pi^{e_1} = \pi$, u a unit in E_1. So $E_1E_2 = E_1(u^{1/e_2}\Pi^{e_1/e_2}) = E_1(u^{1/e_2})$ since $e_2 \mid e_1$. But if $(e, p) = 1$, an extension by an eth root of a unit is always unramified.

Suppose then that we are given global fields E_1, E_2, F whose ramification indices at $\mathfrak{p}$ satisfy the above. Then the composite E_1E_2/E_1 will be unramified at $\mathfrak{p}$ since this is a local question. If this were so at each $\mathfrak{p}$ then E_1E_2/E_1 would be unramified everywhere.

2. The explicit construction. We make the convention that $e_{\mathfrak{p}_i}(E/F)$ denotes the g.c.d. of the ramification indices at the primes above $\mathfrak{p}_i$ in E. This agrees with the usual notation when E/F is abelian.

Suppose E/F is tamely ramified. Then any abelian extension F_* of F whose composite with E is unramified over E must also be tamely ramified. Thus by Proposition 1 of §1 we have

THEOREM 4. *Let E/F be tamely ramified with ramification at $\mathfrak{p}_1,\dots,\mathfrak{p}_n$. Then the genus field E_F^* of E relative to F is the composite of E with an abelian extension of F whose conductor is divisible only by primes to the first power.*

Which field is it? Put $\mathfrak{a} = \mathfrak{p}_1\dots\mathfrak{p}_n$ and $\mathfrak{b}_i = \mathfrak{p}_1\dots\hat{\mathfrak{p}}_i\dots\mathfrak{p}_n$ ($\hat{}$ denotes deletion). Then the galois group of $E^{\mathfrak{a}}$ over $E^{\mathfrak{b}}$ is cyclic or of order $d_i = |N_{\mathfrak{p}_i} - 1|/|U(\mathfrak{a}):U(\mathfrak{b})|$. Put $d^*(\mathfrak{p}_i) = \text{g.c.d.}(e_{\mathfrak{p}_i}(E/F), d_i)$. Then there is a unique subfield F_i of $F^{\mathfrak{a}}$ of degree $d^*(\mathfrak{p}_i)$ over $K^{\mathfrak{b}}$: Put $F_* = \cap F_i$.

THEOREM 5. *F_* is the largest abelian extension of F whose composite with E is E_F^*.*

PROOF. By Abhyankar's lemma F_i yields an extension of E which is unramified at $\mathfrak{p}_i$ and abelian. Also no larger field than F_i can do this. This is because $F^{\mathfrak{a}}/F^{\mathfrak{b}}$ is totally ramified at all the primes above $\mathfrak{p}_i$. By putting $F_* = \cap F_i$ as above, we see that F_* yields an unramified abelian extension of E. Suppose F' is any other abelian extension of F whose composite with E is unramified over E; then F' is certainly tamely ramified and so $F' \subset F^{\mathfrak{a}}$. Now each of the F_i's was the maximal subfield of $F^{\mathfrak{a}}$ whose composite with E was unramified at $\mathfrak{p}_i$, thus $F' \subset F_i$ for each i and the result follows.

It is easy to see now what the mistake in [**4**] was. The assumption the reviewer made would only be true if given relatively prime ideals $\mathfrak{a}_1$, $\mathfrak{a}_2$ in $\mathfrak{O}_F$ then the ray class field $K^{\mathfrak{a}_1\mathfrak{a}_2} = K^{\mathfrak{a}_1}K^{\mathfrak{a}_2}$. This obviously does not hold in general and will depend on a unit index.

That is, to construct the relative genus field it is not sufficient to work "one prime at a time," i.e. by looking at the various subfields F_i of the $F^{\mathfrak{p}_i}$ whose degree over H_F satisfy

$$|F_1 : H_F| = \text{g.c.d.}\left(e_{\mathfrak{p}_i}(E/F), |F^{\mathfrak{p}_i} : H_F|\right)$$

and taking composita.

In one important case (besides $F = Q$) this can be done, however. Let F be an imaginary quadratic field; then we usually have $|F^{a_1a_2} : F^{a_1}F^{a_2}| = \varepsilon$, where $\varepsilon = |U_F|$. So if we take the maximal subfields K, K_1, K_2 of, respectively, $F^{a_1a_2}$, F^{a_1}, F^{a_2} of degree a power of l where $l \nmid \varepsilon$, then $K = K_1K_2$. This leads then to the following: Suppose $|E : F|$ is relatively prime to ε. Then E_i = the unique subfield contained in $F^{\mathfrak{p}_i}$ of degree $d^*(\mathfrak{p}_i)$ over H_F and $K = E_1E_2,\dots,E_n$. So under the above hypothesis we have

THEOREM 6. $E_F^* = EK$. (*Notice* $(|E : F|, 6) = 1$ *is enough.*)

Now we return again to the general case.

THEOREM 7. *Suppose E/F is abelian with at most one ramified prime $\mathfrak{p}$; then $E_F^* = EH_F$.*

PROOF. E_F^* is the composite of abelian extensions of F and is thus abelian. E_F^* has ramification only at $\mathfrak{p}$ and is by Class Field Theory contained in $F^{\mathfrak{p}^n}$, some n. We know $F^{\mathfrak{p}^n}/H_F$ is totally ramified at all the primes above $\mathfrak{p}$ and so $F^{\mathfrak{p}^n}/EH_F$ is also. Thus no extension of EH_F can be unramified. Since EH_F is certainly unramified we are done.

If E/F is abelian and H_E is the Hilbert class field of E, then E_F^* is the fixed field of the commutator subgroup of $\mathrm{Gal}(H_E/F)$. If E/F is cyclic with generator σ then by the functoriality of the Artin map we have that $\mathrm{Gal}(E_F^*/E) \approx C_E/C_E^{1-\sigma}$. Combine the above with the exact sequence

$$0 \to C_E^{\langle\sigma\rangle} \to C_E \to C_E \to C_E/C_E^{1-\sigma} \to 0.$$

We can derive as corollaries of the previous theorem the following results:

COROLLARY 1 (IWASAWA [9]). *Suppose that E/F is a p-extension with only one prime ramified. Moreover, suppose this prime is totally ramified; then $p \mid h_F \Leftrightarrow p \mid h_E$.*

PROOF. By induction we may reduce to the case when E/F is cyclic of degree p. Now a p-group acting on a p-group must have nontrivial fixed points so $p \mid h_E \Leftrightarrow p \mid\mid C_E^{\langle\sigma\rangle}\mid$. But by the 4-term exact sequence above this has order equal to $\mid C_E/C_E^{1-\sigma}\mid$. By the previous theorem and the discussion above this is equal to $\mid EH_F\colon E\mid = \mid H_F\colon E \cap H_F\mid$ so $p \mid\mid EH_F\colon E\mid \Leftrightarrow p \mid\mid H_F\colon E \cap H_F\mid$. The result follows since E is totally ramified and $E \cap H_F = F$.

COROLLARY 2 (KISILEVSKY [10]). *Suppose E/F is cyclic unramified of degree n. Then*

$$\mid C_E^G\mid = \mid C_F\mid/n = h_F/n.$$

PROOF. As before $\mid C_E^G\mid = \mid C_E/C_E^{1-\sigma}\mid$, but this has order $\mid H_F\colon E \cap H_F\mid$. Now $\mid H_F\colon F\mid = h_F = \mid H_F\colon E \cap H_F\mid\mid E \cap H_F\colon F\mid$; since E is unramified of degree n the result follows.

A proposition which complements the previous theorem is the following:

PROPOSITION 2. *Suppose $E = E_1E_2$, each E_1 abelian over F, suppose E_2 is ramified only at $\mathfrak{p}$ and $\mathfrak{p}$ is unramified in E_1. Then $E_F^* = E_1^*E_2$ (where E_1^* denotes the genus field of E_1 relative to F).*

PROOF. The fixed field K of the inertia group of $\mathfrak{p}$ is the maximal subfield of E_F^* unramified at $\mathfrak{p}$ over F. This field contains E_1^*. The field K/E_1^* must be unramified at all $\mathfrak{p}' \neq \mathfrak{p}$ since ramification degrees multiply in towers. So K/E_1^* is unramified at all primes and thus $K = E_1^*$. Now $E_F^*/E_2E_1^* = E_2K$ is totally ramified at $\mathfrak{p}$, so we must have $E_F^* = E_1^*E_2$.

In trying to construct the relative genus field, things are often easier if $\mid E\colon F\mid$ is a prime power. The next theorem shows that if E/F is abelian this reduction is always possible.

Suppose then that E/F is abelian and $(E:F) = l_1^{a_1} \cdots l_n^{a_n}$. Let E_i be the unique subfield of E of degree $l_i^{a_i}$ over F. Let E_i^* be the genus field of E_i relative to F.

THEOREM 8. $E_F^* = E_1^* \cdots E_n^*$.

PROOF. E_F^* is the composite of E with an abelian extension K^* of F and each E_i^* is the composite of E_i with an abelian extension E_i^* of F. We need to show $K^* = E_1^* \cdots E_n^*$.

Now each E_i^* yields an unramified extension of E_i and so by translation, also an unramified extension of E. Since the composite of unramified extensions is unramified we have $K^* \subset E_1^* E_2^* \cdots E_n^*$.

We need to prove the reverse inclusion. Let $\Gamma = \mathrm{Gal}(K^*/F)$ and write $\Gamma = \Gamma_1 \cdots \Gamma_n \Gamma'$ where each of the Γ_i's is the l_ith sylow subgroup and $l_i \nmid |\Gamma'|$ for all i. Let K_i be the unique subfield of K^* such that $|K_i : F| = |\Gamma_i|$. We claim $K_1 K_m$ an unramified extension of E_i and so $K_i K_m \subset E_i^*$, $1 \leqslant i \leqslant n$, and the result would follow.

Consider the tower of fields $E_i \to E_i K_i K_m \to E K_i K_m$. Since $E K_i K_m / E$ is unramified we see that the ramification indices of $E_i K_i K_m / E_i$ divide the degree $|E : E_i| = l_2^{a_2} \cdots l_n^{a_n}$. But they must also divide $|E_i K_i K_m : E_i|$ which is relatively prime to $l_2 \cdots l_n$. Thus the ramification index is one for each prime and the result follows.

REMARKS. (1) Obviously E/F nilpotent is enough.

(2) Thus when L/K is abelian we may always assume L/K is a prime power when we are trying to construct L_K^*.

Suppose we are trying to construct the genus field of E/F when E/F is not necessarily tamely ramified. Then the field F_*, constructed in Theorem 5, is obviously the largest tamely ramified abelian extension of F contained in E_F^*. With this remark we have

THEOREM 9. *Suppose E/F is abelian of degree l^n with tame ramification at all but one prime λ. Then $E_E^* = EF_*$.*

PROOF. Let F_1 be the fixed field of the inertia subgroup $T_\lambda(E/F)$. Now $E \cap F_*$ is the maximal subfield of E which is tamely ramified over F. Thus $|EF_* : F_*| = |E : E \cap F_*| = e_\lambda(E/F)$. We also have $|E_F^* : F_*| \geqslant e_\lambda(E/F)$. Since F_* is maximal we must have $F = F_1$. So since $|E_F^* : F_1| = e_\lambda(E_F^* : F) = e_\lambda(F/K)$ we must have $E_F^* = EF_*$.

REMARK. Thus by combining what has gone before with the above we can construct the genus field for any abelian extension E/F provided that there is at most one wildly ramified prime above l for each $l \mid |E : F|$.

We now want to discuss the cases not covered by the remark above. Unfortunately, a general treatment seems difficult and we confine ourselves to the case when F is an imaginary quadratic field. While it is possible to give a treatment without using Furuta's formula it is much easier to use it. We quote the result from [7].

Let g_F^E be the "genus number," i.e., the degree $|E_F^*: E|$. Then we have

THEOREM (FURUTA [7]).

$$g_F^E: \frac{h_F \cdot \prod e'_{\mathfrak{p}}}{|K_0: F||\varepsilon: \eta|},$$

where h_F is the class number of F, $e'_{\mathfrak{p}}$ is the ramification index in the maximal abelian subfield of the completion $E_{\mathfrak{p}}$ over $F_{\mathfrak{p}}$ and K_0 is the maximal subfield of E abelian over F and $|\varepsilon: \eta|$ denotes the index of the units that are everywhere local norms in the full group of units.

THEOREM 10. *Let E be an extension of an imaginary quadratic field F with $l \nmid |U_F|$ and ramification only at λ_1, λ_2 with $(\lambda_1)(\lambda_2) = (l)$ in F. Then $E_F^* = ET_1$ with T_1 the unique abelian extension of F contained in the full ray class field $F^{\lambda_1^n}$ of degree $e_{\lambda_1}(E/F)$.*

PROOF. Since $\mathrm{Gal}(F^{\lambda_1^n}/H_F) \approx (\mathfrak{O}/\lambda_1^n)^*$ it is a cyclic group since λ_i is a prime of degree one above an odd prime. Thus there is a unique field of the type specified.

Put F_1 equal to the fixed field of the inertia group of λ_2. Then F_1/F is ramified only at λ_1, and $|E_F^*: F_1| = e_{\lambda_2}(E_F^*/F)$. Now by Furuta's formula, the degree $|E_F^*: F| = e(\lambda_1)e(\lambda_2)h_F$ since $l \nmid |U_F|$.

Thus F_1 must be T_1 since its degree over F is $e(\lambda_1)h_F$ and T_1 is the unique abelian extension of F with ramification only at λ_1 of degree $e(\lambda_1)$. Now $E \cap F_1$ is the fixed field of the inertia group $T_{\lambda_2}(E/F)$. So

$$|EF_1: F_1| = |E: E \cap F_1| = |T_{\lambda_2}(E/F)| = e_{\lambda_2}(E/F)$$

and we have that

$$|EF_1: F| = |EF_1: F_1||F_1: F| = e(\lambda_2)e(\lambda_1)h_F.$$

The final case we discuss is when E/F has tame ramification at $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and wild ramification at both λ_1, λ_2, $(\lambda_1)(\lambda_2) = (l)$ and $l \nmid |U_F|$.

THEOREM 11. *Let E/F be abelian with ramification described as above. Then $E_F^* = EF_*T_1$ with F_* as in Theorem 5, and T_1 as in the previous theorem.*

PROOF. Let T be the group generated by $T_{\mathfrak{p}_i}(E_F^*/F)$, for all i, along with $T_{\lambda_2}(E_F^*/F)$. Since E_F^*/F is abelian its order is at most $\prod_{\mathfrak{p}_i} e_{\mathfrak{p}_i}(E/F) \cdot e_{\lambda_2}(E/F)$.

The fixed field of T is the maximal subfield of E_F^* ramified only at λ_1. The degree $|E_F^*: F|$ is $\prod_i e_{\mathfrak{p}_i} e_{\lambda_1} e_{\lambda_2} \cdot h_F$ by Furuta's formula (we are again assuming $l \nmid |U_F|$). Let F_1 be the fixed field of T; then F_1/H_F has ramification only at the primes above λ_1. Thus the degree $|F_1: H_F| \leq e(\lambda_1)$. Moreover, F_1/H_F is totally ramified at all the primes above λ_1. Now we have

$$|E_F^*: F| \leq \prod e(\mathfrak{p}_i)e(\lambda_2) \cdot |F_1: F| \leq \prod e(\mathfrak{p}_i)e(\lambda_2)e(\lambda_1)h_F.$$

So since $|E_F^*: F|$ equals the RHS we must have $|F_1: H_F| = e(\lambda_1)$ and F_1 is the unique field contained in $F^{\lambda_1^n}$ of degree $e(\lambda_1)$ over H_F. There remains only to prove that $L_F^* = LF_*T_1$.

Now $|EF_*F_1 : F| = |E : E \cap F_*F_1| \cdot |F_*F_1 : F|$. Notice that $(E \cap F_*F_1)$ is the inertial subfield of λ_2 since it is the maximal subfield of E unramified over F at λ_2. Thus the degree $|E : E \cap F_*F_1| = e(\lambda_2)$. Thus the degree $|E : E \cap F_*F_1| = e(\lambda_2)$. Since we already know that $|F_*F_1 : F| = \prod_{\mathfrak{p}} e(\mathfrak{p})e(\lambda_1) \cdot h_F$, we are done.

REMARK. Notice because of the reductions possible for abelian E/F we have shown how to construct the genus field E_F^* for all imaginary quadratic fields F save those for which 2 splits and both primes above 2 ramify in E. The problem in this situation is the lack of a way of singling out the right extension ramified at the primes above 2.

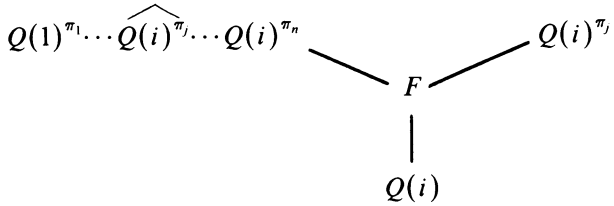
3. Applications. While many applications are possible, we confine ourselves in this section to those dealing with the construction of number fields with "interesting" class groups.

The first application is to cyclotomic fields. But as mentioned previously we must choose the cyclotomic field so as to contain a "useful" subfield. Now if n is any integer such that $4 | n$, we know $Q(\zeta_n)$ contains $Q(i)$, a field whose abelian extensions are easy to describe. Let $\pi_1, \ldots, \pi_n$ be primes above integer primes $p_1, \ldots, p_n$ that split in $Q(i)$. (Notice that the p_i's must be $\equiv 1$ (4).) Then we have

PROPOSITION 3. (1) *The galois group of* $Q(i)^{\pi_i}$ *is cyclic of order* $(p_i - 1)/4$.

(2) *The field* $Q(i)^{\pi_1} \ldots Q(i)^{\pi_n}$ *is galois over* $Q(i)$ *with galois group isomorphic to the direct product of cyclic groups of order* $(p_1 - 1)/4, \ldots, (p_n - 1)/4$.

PROOF. The first statement follows from class field theory because $Q(i)$ has class number one. The second will follow if we can show that any of them are disjoint from the composite of the rest. Look at the diagram below (where $\hat{}$ denotes deletion).



(F is the intersection.) By going up the left-hand side the only primes that ramify in F are (possibly) $\pi_1, \ldots, \hat{\pi}_j, \ldots, \pi_n$. Via the right-hand side it is only π_j. Thus F is an unramified abelian extension of $Q(i)$ and so since $Q(i)$ has class number one, $F = Q(i)$. Q.E.D.

Let G be any finite abelian group. So by the fundamental theorem of abelian groups $G \approx C_{t_1} \times \cdots \times C_{t_n}$, where the C_{t_i} are cyclic groups of order t_i. We want to find an N such that $Q(\zeta_N)$ contains G as a subgroup of its class group. Choose primes $p_1, \ldots, p_n$ such that $p_i \equiv 1$ $(4t_i)$. Then put $N = 4p_1 \cdots p_n$.

THEOREM 12. $Q(\zeta_N)$ *contains* G *as a subgroup of its class group.*

PROOF. By the previous remarks we need only show that the field $F = Q(i)^{\pi_1} \cdots Q(i)^{\pi_n}$ intersected with $Q(\zeta_N)$ is just $Q(i)$. Suppose this is the case. Then since

the ramification degree of the π_i's is just $(p_1 - 1)/4$ in F and its ramification degree in $Q(\zeta_N)$ is $p_i - 1$, Abhyankar's lemma would apply. To show the intersection is just $Q(i)$ is easy; just notice that the intersection is an abelian extension of Q and so if any of the π_i's ramified its conjugate would also. But none of the conjugates ramify in F. So the intersection would again be an unramified abelian extension of $Q(i)$ which has none. Q.E.D.

REMARKS. It is easy to see that the genus field of $Q(\zeta_N)$ with respect to $Q(i)$ provides a counterexample to the statements of [**4**].

Now there was really nothing special about showing that the intersection of $Q(\zeta_N)$ with F was $Q(i)$. The same argument would show that the intersection of Q^{ab} with F is also $Q(i)$ (where Q^{ab} denotes the maximal abelian extension of Q, e.g. the field of all the roots of unity). Thus we have a method of constructing unramified abelian extensions of Q^{ab} of any type. This leads to the following theorem which was suggested by M. Rosen.

The idea is to replace Q by some fixed field F, $Q(i)$ by any finite abelian extension E of F and $Q(\zeta_n)$ by some (very) large ray class field K of F containing E, then show that K has a properly larger genus field relative to E which does not intersect the maximal abelian extension of F, F^{ab}, in too large a way.

THEOREM 13. *Let F be any number field and F^{ab} its maximal abelian extension. Then F^{ab} has an unramified abelian extension M such that the galois group of M over F^{ab} is any finite abelian group. Moreover, M can be chosen so as to be of the form $M = F^{ab}E^*$, where E^* is some (abelian) extension of any pregiven field E which is finite and abelian over F.*

(We may say that we can "induce" finite abelian unramified extensions of F^{ab} from any previously given finite abelian unramified extension E of F. Of course, the extension E^* of E needed may not itself be galois over F.)

PROOF. Let E be the given abelian extension of F and $G \approx C_{t_1} \times \cdots \times C_{t_n}$ as before. Let s be the rank of the unit group of E. Then by taking more than s primes of E whose absolute norms are all $\equiv 1\ (t_i)$ and putting $\mathfrak{a}_i$ to be their product, we can insure that the galois group of $E^{\mathfrak{a}_i}/E$ contains C_{t_i}. We can even take the primes dividing the $\mathfrak{a}_i$ to be above primes of degree one of F. All this is possible by the density theorem. If we put $\mathfrak{a}$ to be their product then the galois group of $E^{\mathfrak{a}}/E$ would, as in the proof of Proposition 2, contain G if not for the existence of the Hilbert class field of E. This is, however, a finite extension of E, so by throwing even more primes into $\mathfrak{a}$, we can indeed make the galois group of $E^{\mathfrak{a}}/E$ contain G. Now let K be the ray class field of F at the primes below the ones dividing $\mathfrak{a}$, as in the proof of Theorem 2. $KE^{\mathfrak{a}}/K$ is an unramified abelian extension of K. Now the intersection of K (or of F^{ab}) with $E^{\mathfrak{a}}$ is as in the proof of Theorem 2 an unramified abelian extension of F and is therefore contained in the Hilbert class field of F, H_F. This is again a finite extension of F and so by throwing even more primes of E into $\mathfrak{a}$ and changing K accordingly we can insure that $F^{ab}E^{\mathfrak{a}}$ is an unramified abelian extension of F^{ab} which contains G. Q.E.D.

The above fact has applications to the Picard group of Q^{ab} as may be seen in the forthcoming work of Brumer [**1**].

BIBLIOGRAPHY

1. A. Brumer, *On the Picard group of* Q^{ab} (to appear).
2. G. Cornell, *Relative genus theory and the class group of l-extensions* (in preparation).
3. _____, *A note on the* $\hat{Z}$*-extension of* Q (in preparation).
4. G. Frey, MR **50** #2126.
5. A. Fröhlich, *The genus field and genus group in finite number fields*. I, Mathematica **6** (1959), 40–46.
6. _____, *The genus field and genus group in finite number fields*. II, Mathematica **6** (1959), 142–146.
7. Y. Furuta, *The genus field and genus number in finite number fields*, Nagoya Math. J. **29** (1967), 281–285.
8. M. Ishida, *The genus field of algebraic number fields*, Lecture Notes in Math., vol. 555, Springer-Verlag, Berlin and New York, 1976.
9. K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1955).
10. H. Kisilevsky, *Some results related to Hilbert's theorem* 94, J. Number Theory **2** (1970), 199–206.
11. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.
12. L. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, Berlin and New York, 1982.

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, NEW BRUNSWICK, NEW JERSEY 08903

Current address: Department of Mathematics, University of Connecticut, Storrs, Connecticut 06268