

## GENERA IN ABELIAN EXTENSIONS

ROBERT GOLD

ABSTRACT. The principal genus in an abelian extension is characterized as the kernel of norm residue symbols at the ramified primes.

Let  $F$  be a finite algebraic number field and  $K$  a finite abelian extension of  $F$  with  $G = \text{Gal}(K/F)$ . Let  $\bar{K}$  be the Hilbert class field of  $K$  and let  $C_K$  be the ideal class group of  $K$ . By class field theory the fields lying between  $K$  and  $\bar{K}$  are in one-to-one correspondence with the subgroups of  $C_K$ . Let  $L$  be the genus field of  $K/F$ . Thus  $L$  is the maximal abelian extension of  $F$  contained in  $\bar{K}$ . The subgroup of  $C_K$  corresponding to  $L$  is known as the principal genus and the quotient of  $C_K$  modulo the principal genus is the group of genera. If  $G$  is cyclic and generated by some  $g \in G$ , then it is easily seen that the principal genus is  $C_K^{1-g}$ . If, for general  $G$ , one forms  $I_G = \sum_{g \in G} (1-g)\mathbb{Z}[G] \subseteq \mathbb{Z}[G]$ , then  $C_K^{I_G}$  corresponds to what Furuta in [1] calls the central class field of  $F$  in  $\bar{K}$ . But in general  $C_K^{I_G}$  is a proper subgroup of the principal genus.

Our definition of genera is relatively modern and is made in the context of class field theory and cohomology of groups. Gauss' original definition in [2] for quadratic extensions of the rationals was based solely on certain arithmetic characters of  $C_K$ . Hasse has shown in [4] when  $F = \mathbb{Q}$ , i.e. the absolutely abelian case, that the principal genus in the modern sense could still be characterized by characters. Even more recently, Halter-Koch [3] has shown that this can be done in a slightly loosened sense in the relative cyclic case as well, i.e. arbitrary  $F$  and cyclic  $G$ . We prove here that the principal genus for any abelian extension  $K/F$  can be described, in a sense to be made precise below, by arithmetic characters.

Let  $\bar{F}$  be the Hilbert class field of  $F$  and let  $C_F$  be the ideal class group of  $F$ . The relative norm from  $K$  to  $F$  on ideals of  $K$  induces a homomorphism  $N: C_K \rightarrow C_F$ . Note this is not the norm endomorphism of

---

Presented to the Society, November 16, 1973; received by the editors November 5, 1973.

AMS (MOS) subject classifications (1970). Primary 12A35, 12A65.

Key words and phrases. Genera, norm residue, genus field.

$C_K$  as a  $G$ -module. Let  $H$  be the principal genus. It is the subgroup of  $C_K$  corresponding to the genus field  $L$ . Thus  $C_K/H \cong \text{Gal}(L/K)$  and if  $\mathfrak{P}$  is a prime ideal of  $K$ , then the class of  $\mathfrak{P}$ , to be denoted by  $\overline{\mathfrak{P}}$ , is in  $H$  if and only if  $\mathfrak{P}$  is completely decomposed in  $L/K$ .

Let  $\mathfrak{p}$  be any prime divisor, finite or infinite, of  $F$ ; then the norm residue symbol locally at  $\mathfrak{p}$  defines a homomorphism from  $F^\times$  to  $G$  by  $\alpha \rightarrow \left(\frac{\alpha, K/F}{\mathfrak{p}}\right)$ . In particular, let  $\mathfrak{p}_1, \dots, \mathfrak{p}_t$  be the primes which are ramified in  $K/F$  and let  $f_i(\alpha) = \left(\frac{\alpha, K/F}{\mathfrak{p}_i}\right)$  for  $\alpha \in F^\times$ . Let  $f: F^\times \rightarrow G^t$  by  $f(\alpha) = (f_1(\alpha), \dots, f_t(\alpha))$ .

Let  $U_F$  be the group of units of  $F$ . And let  $S = f(U_F) \subseteq G^t$ . Note, as in [3], that if  $G$  is cyclic, then the kernel of  $f$  on  $U_F$  is  $U_F \cap N(K)$  and so  $\#(S) = [U_F : U_F \cap N(K)]$ . Compare the genus formula for cyclic extensions.

Let  ${}_N C_K$  be the kernel of  $N: C_K \rightarrow C_F$ . Under Artin reciprocity the map  $N$  corresponds with the restriction map  $\text{Gal}(\overline{K}/K) \rightarrow \text{Gal}(\overline{F}/F)$ . The kernel of the restriction map is  $\text{Gal}(\overline{K}/K\overline{F})$  and it follows that  ${}_N C_K$  corresponds to the composite  $K\overline{F}$ . It is clear that  $L \supseteq K\overline{F}$  and therefore  ${}_N C_K \supseteq H$ . So it suffices to characterize  $H$  among the subgroups of  ${}_N C_K$ .

Let  $\mathfrak{A}$  be an ideal of  $K$  such that  $\overline{\mathfrak{A}} \in {}_N C_K$ . Then  $N(\mathfrak{A})$  is principal in  $F$ . Say  $N(\mathfrak{A}) = (\alpha)$ ,  $\alpha \in F^\times$ . Choose any  $\epsilon \in U_F$ . Then  $f(\alpha\epsilon) = (f_1(\alpha\epsilon), \dots, f_t(\alpha\epsilon)) = f(\epsilon) \cdot f(\alpha)$ , and  $f(\epsilon) \in S$ . Furthermore if  $\overline{\mathfrak{A}} = \overline{\mathfrak{B}}$ , then  $\mathfrak{B} = (a) \cdot \mathfrak{A}$  and  $N(\mathfrak{B}) = (N(a)) \cdot N(\mathfrak{A})$ . However  $f(N(a)) = (1, \dots, 1)$ . From these facts we see that  $f$  induces a homomorphism  $f: {}_N C_K \rightarrow G^t/S$ . We may now state our theorem exactly.

**Theorem.** *Let  $K/F$  be a finite abelian extension of number fields with Galois group  $G$  and let  $H$  be the principal genus for  $K/F$ , the subgroup of  $C_K$  fixing the genus field for  $K/F$ . Let  $f: {}_N C_K \rightarrow G^t/S$  be the modified product of local norm residue symbols described above. Then  $H$  equals the kernel of  $f$ .*

**Proof.** To show  $\text{Ker}(f) \subseteq H$ : Let  $\mathfrak{P}$  be a prime ideal of  $K$  with  $\overline{\mathfrak{P}} \in \text{Ker}(f)$  and  $\mathfrak{P} \nmid \mathfrak{p}_i$ ,  $i = 1, \dots, t$ . In particular  $\overline{\mathfrak{P}} \in {}_N C_K$ , so let  $N(\mathfrak{P}) = \mathfrak{p}' = (\rho')$ . By definition of  $f_i$  we have  $(f_1(\rho'), \dots, f_t(\rho')) \in S = f(U_F)$ . Hence there is an  $\epsilon \in U_F$  such that  $f_i(\rho') = f_i(\epsilon)$  for  $i = 1, \dots, t$ . Let  $\rho = \rho' \epsilon^{-1}$  so that  $N(\mathfrak{P}) = \mathfrak{p}' = (\rho)$  and  $f_i(\rho) = 1$  for  $i = 1, \dots, t$ . Recall that

$$f_i(\rho) = \left(\frac{\rho, K/F}{\mathfrak{p}_i}\right) \quad \text{and} \quad \left(\frac{\rho, L/F}{\mathfrak{p}_i}\right) \Big|_K = \left(\frac{\rho, K/F}{\mathfrak{p}_i}\right) = 1.$$

Thus  $(\frac{\rho, L/F}{\mathfrak{p}_i})$  fixes  $K$  and is an element of  $\text{Gal}(L/K)$ . Now  $\rho$  is a  $\mathfrak{p}_i$ -unit for  $i = 1, \dots, t$ . Hence  $(\frac{\rho, L/F}{\mathfrak{p}_i}) \in T(\mathfrak{p}_i, L/F) \subseteq \text{Gal}(L/F)$ , where  $T$  indicates inertia subgroup. But  $\text{Gal}(L/K) \cap T(\mathfrak{p}_i, L/F) = \{1\}$  since  $L/K$  is unramified. Hence  $(\frac{\rho, L/F}{\mathfrak{p}_i}) = 1$  for  $i = 1, \dots, t$ .

Since the product of norm residue symbols is 1 and  $\rho$  is a unit at every unramified prime but  $\mathfrak{h}$ , we have

$$\left(\frac{\rho, L/F}{\mathfrak{p}}\right)^{-1} = \prod_{i=1}^t \left(\frac{\rho, L/F}{\mathfrak{p}_i}\right).$$

It follows that  $(\frac{\rho, L/F}{\mathfrak{p}}) = 1$ . Let  $\pi$  be a local uniformizing parameter at  $\mathfrak{p}$  in  $F$ . Then  $(\frac{\pi, L/F}{\mathfrak{p}})$  generates  $Z(\mathfrak{h}, L/F)$ , the decomposition group of  $\mathfrak{h}$ . Recall that  $\nu(\rho) = f(\mathfrak{p}/\mathfrak{p}) = \#(Z(\mathfrak{h}, K/F))$ . But

$$\left(\frac{\pi, L/F}{\mathfrak{p}}\right)^f = \left(\frac{\pi^f, L/F}{\mathfrak{p}}\right) = \left(\frac{\rho, L/F}{\mathfrak{p}}\right) = 1.$$

Hence  $\#(Z(\mathfrak{h}, L/F)) \leq f = \#(Z(\mathfrak{h}, K/F))$ . It follows that the two decomposition groups coincide and therefore that  $\mathfrak{P}$  is completely decomposed in  $L/K$ . Hence  $\overline{\mathfrak{P}} \in H$ .

To show  $\text{Ker}(f) \supseteq H$ : Let  $c$  be any class in  $H \subseteq C_K$ . We can find a prime ideal  $\mathfrak{P}$  such that  $\overline{\mathfrak{P}} = c \in H$  and  $\mathfrak{P} \nmid \mathfrak{p}_i, i = 1, \dots, t$ . Hence  $\mathfrak{P}$  is completely decomposed in  $L/K$ . Recall  $H \subseteq {}_N C_K$  and let  $N(\mathfrak{P}) = \mathfrak{p}^f = (\rho)$ . Let  $\mathfrak{f}$  be the conductor of  $L/F$ . Thus  $\text{Gal}(L/F) \cong I_{\mathfrak{f}}(F)/N(I_{\mathfrak{f}}(L))S_{\mathfrak{f}}(F)$ . Now  $L$  is the maximal abelian extension of  $F$  in  $\overline{K}$ , hence by the norm limitation theorem  $N(I_{\mathfrak{f}}(\overline{K})) \cdot S_{\mathfrak{f}}(F) = N(I_{\mathfrak{f}}(L)) \cdot S_{\mathfrak{f}}(F)$ . We know that  $\mathfrak{p}^f \in N(I_{\mathfrak{f}}(L))$  since  $\mathfrak{P}$  is completely decomposed in  $L/K$  and  $f = f(\mathfrak{P}/\mathfrak{p})$ . Hence  $\mathfrak{p}^f \in N(I_{\mathfrak{f}}(\overline{K})) \cdot S_{\mathfrak{f}}(F)$ . So let  $\mathfrak{p}^f = N_{\overline{K}/F}(\mathfrak{Q}) \cdot (\alpha)$  for  $\mathfrak{Q} \in I_{\mathfrak{f}}(\overline{K})$  and  $\alpha \in F^\times, \alpha \equiv 1 \pmod{\mathfrak{f}}$ . Hence  $(\rho) = N_{\overline{K}/F}(\mathfrak{Q}) \cdot (\alpha)$ . Since  $\alpha \equiv 1 \pmod{\mathfrak{f}}$  and  $\mathfrak{f}$  is the conductor of  $L/F$ , we have  $(\frac{\alpha, L/F}{\mathfrak{p}_i}) = 1$  for  $i = 1, \dots, t$ . It follows that  $f_i(\alpha) = 1$  for each  $i$ , by restriction from  $L$  to  $K$ .

Let  $\mathfrak{Q}$  be any prime ideal of  $\overline{K}$ . Then  $N_{\overline{K}/K}(\mathfrak{Q}) = \mathfrak{q}^f$ , where  $f = f(\mathfrak{Q}/\mathfrak{q})$  is also the order of  $\mathfrak{q}$  in the group  $C_K$ . It follows that the norm of every prime, and hence of every ideal, from  $\overline{K}$  to  $K$  is principal. (This is part of the correspondence:  $\overline{K} \rightarrow \{1\} \subseteq C_K$ .) So let  $N_{\overline{K}/K}(\mathfrak{Q}) = (a), a \in K$ . Then  $N(\mathfrak{P}) = (\rho) = (\alpha \cdot N_{K/F}(a))$ . But  $f_i(\alpha) = 1$  and  $f_i(N(a)) = 1$  for all  $i$ . It follows immediately that  $\overline{\mathfrak{P}} \in \text{Ker}(f)$ .

REFERENCES

1. Y. Furuta, *Über die zentrale Klassenzahl eines Relativgaloisschen Zahlkörpers*, J. Number Theory 3 (1971), 318–322. MR 45 #6795.

2. C. F. Gauss, *Untersuchungen über höhere Arithmetik*, Chelsea, New York, 1965. MR 32 #5488.

3. F. Halter-Koch, *Ein Satz über die Geschlechter relativ-zyklischer Zahlkörper von Primzahlgrad und seine Anwendung auf biquadratisch-bizyklische Körper*, J. Number Theory 4 (1972), 144–156. MR 46 #1756.

4. H. Hasse, *A supplement to Leopoldt's theory of genera in abelian number fields*, J. Number Theory 1 (1969), 4–7. MR 39 #2733.

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, COLUMBUS, OHIO  
43210