

# 3. Rings of integers

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **42 (1996)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **09.08.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

(2.5) PROPOSITION. *If  $N$  and  $M$  are factor equivalent then for any  $A[G]$ -linear embedding  $j: M \rightarrow N$  the function  $H \mapsto [N^H : j(M^H)]_A$  is factorizable.*

*Proof.* We have  $j = \varphi i$ , where  $i$  is an embedding as in (2.4) and  $\varphi$  is a  $K[G]$ -linear automorphism of  $N \otimes_A K$ . Using [15, Ch. III, § 1, Prop. 2] and the notation of (2.3) we see that

$$[N^H : j(M^H)]_A = d_\varphi(H) \cdot [N^H : i(M^H)]_A .$$

This is a product of two factorizable functions by (2.3) and by our choice of  $i$ .  $\square$

The fact that “factor equivalence” is an equivalence relation is an easy consequence of (2.5). If  $\mathfrak{p}$  is a prime of  $K$  not dividing  $\#G$  then condition (1) of (2.4) implies that the  $\mathfrak{p}$ -part of  $[N^H : i(M^H)]_A$  is factorizable. One can prove this with [16, § 15.2] and [16, § 14.4, Lemma 21].

(2.6) REMARK. The definitions of factorizability given by Fröhlich [8; 9] and Burns [2] for abelian groups  $G$  are in agreement with our definitions. They also define the notion called  $\mathbf{Q}$ -factorizability in the abelian case, which is a stronger condition than factorizability. However, the function that one wants to be factorizable in the definition of factor equivalence automatically satisfies this stronger condition if it is factorizable. Thus,  $\mathbf{Q}$ -factor equivalence is the same as factor equivalence.

In [4, § 3] a factorizable function  $f$  with values in  $I(\mathbf{Q})$  must also satisfy an additional condition: there should be a map  $g$  from the group of complex characters  $R_{\mathbf{C}}(G)$  to  $I(E)$ , where  $E$  is some normal number field containing all character values of  $G$ , such that  $g$  is  $\text{Gal}(E/\mathbf{Q})$ -equivariant, and such that  $g(1_H^G)$  is the  $E$ -ideal generated by  $f(H)$ . It is not hard to see that this condition is satisfied by all functions that are factorizable in our sense.

### 3. RINGS OF INTEGERS

Let  $A$  be a Dedekind domain with quotient field  $K$  of characteristic zero and let  $L$  a Galois extension of  $K$  with Galois group  $G$ . The integral closure  $B$  of  $A$  in  $L$  is again a Dedekind domain. Assume that for all primes of  $L$  the residue class field extension is separable.

(3.1) THEOREM. *The  $A[G]$ -lattices  $B$  and  $A[G]$  are factor equivalent.*

*Proof.* Define a  $B[G]$ -module structure on  $B \otimes_A B$  by letting  $B$  act on the left factor and  $G$  on the right. We will show first that  $B \otimes_A B$  and  $B[G]$  are factor equivalent as  $B[G]$ -lattices. Define the canonical  $B[G]$ -linear map  $\varphi: B \otimes_A B \rightarrow B[G]$  by

$$x \otimes y \mapsto \sum_{\sigma \in G} x\sigma(y) \cdot \sigma^{-1} .$$

Let  $H$  be a subgroup of  $G$ . If  $\sigma_1, \dots, \sigma_n$  are the  $K$ -embeddings of  $L^H$  in  $L$ , and if there is an  $A$ -basis  $\omega_1, \dots, \omega_n$  of  $B^H$ , then the restriction  $(B \otimes_A B)^H \rightarrow B[G]^H$  of  $\varphi$  is a  $B$ -linear map with matrix  $(\sigma_i(\omega_j))_{ij}$  on the bases  $\{1 \otimes \omega_j\}$  and  $\{b_i\}$ , where  $b_i$  is the formal sum of those  $\sigma \in G$  for which  $\sigma^{-1}$  restricts to  $\sigma_i$ . The square of the determinant of this matrix generates the discriminant  $\Delta(B^H/A)$  as an  $A$ -ideal. By localization it follows that even if  $B$  is not free over  $A$ , we have

$$[B[G]^H : \varphi(B \otimes_A B)^H]_B^2 = \Delta(B^H/A) \cdot B .$$

By Hasse's conductor discriminant product formula [15, Ch. VI, §3] the ideal  $\Delta(B^H/A)$  is a factorizable function of  $H$ , so  $B \otimes_A B$  and  $B[G]$  are factor equivalent  $B[G]$ -lattices.

In order to descend to  $A[G]$ -lattices, note that there exists an  $A[G]$ -linear injection  $i: A[G] \rightarrow B$  by the normal basis theorem, and consider the induced  $B[G]$ -linear map  $i_*: B[G] \rightarrow B \otimes_A B$  that sends  $b\sigma$  to  $b \otimes i(\sigma)$  for  $b \in B$  and  $\sigma \in G$ . We have

$$[(B \otimes_A B)^H : i_*(B[G])^H]_B = [B^H : i(A[G])^H]_A \cdot B ,$$

and by (2.5) we know that the left hand side is a factorizable function of  $H$ . But then the  $A$ -index  $[B^H : i(A[G])^H]_A$  is also factorizable.  $\square$

#### 4. $S$ -UNITS

Let  $L/K$  be a Galois extension of number fields with Galois group  $G$ , and let  $S$  be a finite  $G$ -stable set of primes of  $L$  containing the infinite primes. The ring of  $S$ -integers of  $L$  consists of all elements of  $L$  that are integral outside  $S$ . Its class number is written as  $h_S(L)$  and its unit group, the group of  $S$ -units of  $L$ , is denoted by  $U_S(L)$ . The group of roots of unity in  $L$  is denoted by  $\mu_L$  and its order is written as  $w(L)$ .