

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 42 (1996)
Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: FACTOR EQUIVALENCE RESULTS FOR INTEGERS AND UNITS
Autor: De Smit, Bart
Kapitel: 4. S-UNITS
DOI: <https://doi.org/10.5169/seals-87884>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 05.12.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

(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 φ 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 σ^{-1} restricts to σ_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 μ_L and its order is written as $w(L)$.

Define the $\mathbf{Z}[G]$ -lattice X_S to be the kernel of the map $\mathbf{Z}[S] \rightarrow \mathbf{Z}$ that sends each $\mathfrak{p} \in S$ to 1. We have a canonical map $\log_L: U_S(L) \rightarrow \mathbf{R} \otimes_{\mathbf{Z}} X_S$ sending x to the formal sum $\sum_{\mathfrak{p} \in S} (\log |x|_{\mathfrak{p}}) \otimes \mathfrak{p}$ in $\mathbf{R}[S]$. Here the normalization of the valuation at a prime \mathfrak{p} of L , lying over a prime p of \mathbf{Q} , is given by $|u|_{\mathfrak{p}} = |N_{L_{\mathfrak{p}}/\mathbf{Q}_p}(u)|_p$, where $|\cdot|_p$ is the usual valuation on the completion \mathbf{Q}_p of \mathbf{Q} (with $\mathbf{Q}_p = \mathbf{R}$ if $p = \infty$). Dirichlet's unit theorem says that \log_L embeds $U_S(L)/\mu_L$ as a discrete cocompact lattice in $\mathbf{R} \otimes_{\mathbf{Z}} X_S$. The S -regulator $R_S(L) \in \mathbf{R}_{>0}$ is defined to be the covolume of this lattice when the measure on $\mathbf{R} \otimes_{\mathbf{Z}} X_S$ is normalized to give $1 \otimes X_S$ covolume 1.

For a subgroup H of G we let $S(H)$ be the set of primes of L^H that extend to a prime in S . We will write $h_S(L^H)$ for $h_{S(H)}(L^H)$ and $R_S(L^H)$ for $R_{S(H)}(L^H)$. Brauer [1] has shown that the function $H \mapsto h_S(L^H)R_S(L^H)/w(L^H)$ is a factorizable function with values in $\mathbf{R}_{>0}$. The easiest way to see this is by noting that this quotient is the absolute value of the leading coefficient in the Taylor series expansion at $s = 0$ of the zeta-function $\zeta_{L^H, S}(s)$ of L^H ; see Tate [17, Ch. I, 2.2]. Since $\zeta_{L^H, S}(s)$ is equal to the Artin L -series $L_S(1_H^G, s)$, the factorizability result then follows from the fact that $L_S(\chi_1 + \chi_2, s) = L_S(\chi_1, s)L_S(\chi_2, s)$.

The group G acts on S , so it acts on $\mathbf{Z}[S]$ and on X_S . The map \log_L induces an $\mathbf{R}[G]$ -linear isomorphism $\mathbf{R} \otimes_{\mathbf{Z}} U_S(L) \xrightarrow{\sim} \mathbf{R} \otimes_{\mathbf{Z}} X_S$. It follows that the $\mathbf{Q}[G]$ -modules $\mathbf{Q} \otimes_{\mathbf{Z}} U_S(L)$ and $\mathbf{Q} \otimes_{\mathbf{Z}} X_S$ are isomorphic; see [3, p. 110]. In particular, there exists a $\mathbf{Z}[G]$ -linear embedding $i: X_S \rightarrow U_S(L)$.

For a prime \mathfrak{p} of L^H all primes \mathfrak{q} of L lying over \mathfrak{p} have the same local degree, which we denote by $n_{\mathfrak{p}}(L/L^H)$. Let $n(H)$ be the product of all $n_{\mathfrak{p}}(L/L^H)$ with $\mathfrak{p} \in S(H)$, and let $l(H)$ be their least common multiple.

(4.1) THEOREM. *For any $\mathbf{Z}[G]$ -linear embedding $i: X_S \hookrightarrow U_S(L)$, the function*

$$H \mapsto [U_S(L)^H : i(X_S)^H] \frac{n(H)}{l(H) h_S(L^H)}$$

with values in $\mathbf{Q}_{>0}$ is factorizable.

Proof. For \mathbf{Z} -lattices L_1, L_2 spanning the same real vector space V we define the "index" $[L_2 : L_1] \in \mathbf{R}_{>0}$ as follows: choose a Haar measure on V such that L_2 has covolume 1 and let $[L_2 : L_1]$ be the covolume of L_1 . Note that this notion coincides with the usual index in the case that $L_1 \subset L_2$, and that $[L_1 : L_2][L_2 : L_3] = [L_1 : L_3]$. Moreover, for any \mathbf{R} -linear automorphism φ of V we have $[L_1 : \varphi(L_1)] = |\det \varphi|$.

For each subgroup H of G we have an injective map $j_H: \mathbf{Z}[S(H)] \rightarrow \mathbf{Z}[S]$ sending \mathfrak{p} to $\sum_{\mathfrak{q}|\mathfrak{p}} n_{\mathfrak{p}}(L/L^H) \cdot \mathfrak{q}$. This map respects the logarithm map in the sense that we have a commutative diagram

$$\begin{array}{ccc} U_S(L^H) & \xrightarrow{\log_{L^H}} & \mathbf{R} \otimes X_{S(H)} \\ \parallel & & \downarrow 1 \otimes j_H \\ U_S(L)^H & \xrightarrow{\log_L} & \mathbf{R} \otimes X_S^H, \end{array}$$

where the vertical map on the left is inclusion. We therefore have

$$R_S(L^H) = [X_{S(H)} : \log_{L^H} U_S(L^H)] = \frac{[X_S^H : \log_L U_S(L)^H]}{[X_S^H : j_H(X_{S(H)})]}.$$

The composite map $X_S \xrightarrow{i} U_S(L) \xrightarrow{\log_L} \mathbf{R} \otimes X_S$ induces an $\mathbf{R}[G]$ -linear automorphism φ of $\mathbf{R} \otimes X_S$. With the notation of (2.3) one has

$$|d_{\varphi}(H)| = [X_S^H : \varphi(X_S^H)] = [X_S^H : \log_L U_S(L)^H] \frac{[U_S(L)^H : i(X_S^H)]}{w(L^H)}.$$

Combining these two formulas, and dividing by $h_S(L^H)$, we get

$$(4.2) \quad [U_S(L)^H : i(X_S^H)] \frac{[X_S^H : j_H(X_{S(H)})]}{h_S(L^H)} = |d_{\varphi}(H)| \frac{w(L^H)}{h_S(L^H) R_S(L^H)}.$$

The right hand side is factorizable by (2.3) and Brauer's theorem. It remains to show that $[X_S^H : j_H(X_{S(H)})] = n(H)/l(H)$. In order to do this we compare the sequence defining $X_{S(H)}$ with the H -invariants of the sequence defining X_S :

$$\begin{array}{ccccccc} 0 & \longrightarrow & X_{S(H)} & \longrightarrow & \mathbf{Z}[S(H)] & \longrightarrow & \mathbf{Z} \longrightarrow 0 \\ & & \downarrow & & \downarrow j_H & & \downarrow \#H \\ 0 & \longrightarrow & X_S^H & \longrightarrow & \mathbf{Z}[S]^H & \longrightarrow & \mathbf{Z}. \end{array}$$

The rows in this commutative diagram are exact and the vertical maps are injective. The cokernel C of the map j_H is the group $\bigoplus_{\mathfrak{p} \in S(H)} \mathbf{Z}/n_{\mathfrak{p}}(L/L^H)\mathbf{Z}$, which has order $n(H)$. It is not hard to see that the image of C in the cokernel of the rightmost vertical map has order $l(H)$. With the snake lemma our claim follows. \square

(4.3) REMARK. One can shorten this proof somewhat by using results in Tate's book on the Stark conjectures. Tate shows in [17, Ch. II, 1.1] that $[U_S(L) : i(X_S)]/h_S(L)$ is equal to the Stark-quotient $A(1, i)$, where 1 denotes the trivial character of the trivial Galois group of L over L . Compatibility of the Stark-quotient with respect to inflation and addition of characters implies that the number on the left in (4.2) equals $A(1_H^G, i)$, and that it is a factorizable function of H .

(4.4) REMARK. In order to say that (4.1) determines the factor equivalence class of $U_S(L)$ we should define factor equivalence for $\mathbf{Z}[G]$ -modules with \mathbf{Z} -torsion. This can be done by replacing condition (2) in (2.4) by the condition that the quotient of the order of cokernel and kernel of the map $M^H \rightarrow N^H$ should be factorizable.

Alternatively, one can look at $\bar{U}(L) = U_S(L)/\mu_L$ instead of $U_S(L)$. This approach does introduce new factors into the formula because $\bar{U}(L)^H$ is not necessarily equal to $\bar{U}(L^H)$. More precisely, $c(H) = [\bar{U}(L)^H : \bar{U}(L^H)]$ is the order of the kernel of the map $H^1(H, \mu_L) \rightarrow H^1(H, U_S(L))$, so we know that it is built up from primes dividing both $w(L)$ and $\#G$. For $\mathbf{Z}[G]$ -embeddings $i: X_S \hookrightarrow \bar{U}(L)$ it turns out that the map

$$(4.5) \quad H \mapsto [\bar{U}(L)^H : i(X_S)^H] \frac{w(L^H) n(H)}{h_S(L^H) c(H) l(H)}$$

is factorizable. Thus one recovers [4, §3, Th. 3], where it is assumed that L has odd degree over K and K is totally real, so that $c(H) = n(H) = l(H) = 1$ and $w(L^H) = 2$. Brauer [1] showed that the odd part of $w(L^H)$ is a factorizable \mathbf{Q}^* -valued function of H , and his argument inspired the following lemma (cf. [11, Prop. 4.7]).

(4.6) LEMMA. *Let G be a group, let D be a subgroup of G and let N be a normal subgroup of D of index n such that D/N is cyclic. For every divisor d of n and subgroup H of G , let $m_d(H) \in \mathbf{Z}$ be the number of D -orbits of G/H that split up into exactly d orbits under the action of N . Then $m_d(H)$ is a factorizable \mathbf{Z} -valued function of H .*

Proof. Let $\chi: D \rightarrow \mathbf{C}^*$ be a complex linear character such that $\chi(N) = 1$, and let χ^G be the induced character of G . We claim that $\langle \chi^G, 1_H^G \rangle_G$ is the sum of those $m_d(H)$ for which d is a multiple of the order of χ . Since $\langle \cdot, \cdot \rangle_G$ is a bilinear operation on characters of G (see [16, §7.2]) the integer $\langle \chi^G, 1_H^G \rangle_G$ is a factorizable function of H . We deduce the lemma from the claim by

taking χ of order d and using induction: we start with $n = d$ and then successively remove prime factors from d . It remains to show the claim.

By Frobenius reciprocity one has $\langle \chi^G, 1_H^G \rangle_G = \langle \chi, 1_H^G|_D \rangle_D$, which is equal to the multiplicity of χ in the complex representation $\mathbf{C}[G/H]$ of D . The D -set G/H is D -isomorphic to a disjoint union $\coprod_X D/D_X$, where X runs over the D -orbits of G/H , and each D_X is a subgroup of D . The multiplicity of χ in $\mathbf{C}[D/D_X]$ is either 0 or 1, and it is 1 if and only if $D_X \subset \text{Ker } \chi$. Since $N \subset \text{Ker } \chi$, and D/N is cyclic, it follows that $\langle \chi^G, 1_H^G \rangle_G$ is equal to the number of X for which the order of χ divides $[D : ND_X]$. This index is the number of N -orbits of D/D_X , so the claim follows. \square

If for a prime number p the roots of unity in L of p -power order generate a cyclic extension of K , then one can show with the lemma (with $D = G$) that the p -part of $w(L^H)$ is a factorizable \mathbf{Q}^* -valued function of H . The condition holds for all $p > 2$, so the odd part of $w(L^H)$ is factorizable.

For any prime \mathfrak{p} of K and $d \in \mathbf{Z}$ the number of primes in L^H extending \mathfrak{p} with residue degree d is a \mathbf{Z} -valued factorizable function of H . This follows from the lemma if we take D and N to be the decomposition group and the inertia group of \mathfrak{p} . If \mathfrak{p} has a cyclic decomposition group D then one can also take $N = 1$, and deduce the same statement with “residue degree” replaced by “local degree”.

It follows that the factor $n(H)$ in (4.1) can be replaced by the product of the ramification indices in the extension L/L^H of those primes $\mathfrak{p} \in S(H)$ that extend to a prime of L with non-cyclic decomposition group in L/K . In particular, $n(H)$ is factorizable if S contains no finite ramified primes.

5. APPLICATIONS

Without giving proofs we indicate some concrete applications of the factor equivalence results given in the last two sections.

(5.1) CYCLIC SUBFIELD INTEGER INDEX. Let K be a Galois extension of \mathbf{Q} with abelian Galois group G and ring of integers \mathcal{O}_K . For a $\mathbf{Z}[G]$ -module M let $c_G(M)$ be the index in M of $\sum M^H$, where the sum is taken over those subgroups H of G for which G/H is cyclic. In particular,