ERRATUM: NORM RELATIONS AND COMPUTATIONAL PROBLEMS IN NUMBER FIELDS

JEAN-FRANÇOIS BIASSE, CLAUS FIEKER, TOMMY HOFMANN, AND AUREL PAGE

We found an error in Theorem 4.11 of [2]. When constructing the set T used to test for the existence of d-th powers, one should take all prime ideals $\mathfrak{p}$ with $\mathrm{N}(\mathfrak{p}) = 1 \bmod p$ instead of only those satisfying $\mathrm{N}(\mathfrak{p}) = 1 \bmod d$. Here is an explicit counterexample.

Example E.1. Let $K = \mathbb{Q}(\zeta_8)^+$, $d = 4$, $S = \emptyset$ and $\alpha = -1$. We have $L = K(\zeta_4) = \mathbb{Q}(\zeta_8)$, which is a quadratic extension of K, so that the extension L/K is cyclic. Let $\mathfrak{p}$ be a prime of K of degree 1 such that $\mathrm{N}(\mathfrak{p}) = 1 \bmod d$, and let $q = \mathrm{N}(\mathfrak{p})$. We have $q \equiv \pm 1 \bmod 8$, but since $q = 1 \bmod 4$, we get $q = 1 \bmod 8$, so that $\frac{q-1}{2} = 1 \bmod 4$ and therefore -1 is a 4-th power in $K_{\mathfrak{p}}^\times$. All the hypotheses of the original formulation of the theorem are therefore satisfied. However, α is clearly not a d-th power in K.

The mistake in the proof was in the descent step from L to K (note for instance that in Example E.1, α is indeed a d-th power in L), which was only sketched in the published version of the paper. The correct statement of Theorem 4.11 and proof are the following.

Theorem E.2 (Effective Grunwald–Wang)**.** Assume GRH. Let $d = p^r$ with p prime and $r \geq 1$. Let K be a number field of degree n, and $L = K(\zeta_d)$. Let S be a finite set of primes of K, let $M_S = \prod_{\mathfrak{p} \in S} \mathrm{N}(\mathfrak{p})$, and let $S_p = S \cup \{\mathfrak{p} \mid p\}$. Let

$$c_0 = 18d^2 \left(2 \log |\Delta_K| + 6n \log d + \log M_S\right)^2.$$

Let T be the set of prime ideals $\mathfrak{p}$ of K such that

- $\mathfrak{p} \notin S_p$,
- $\mathfrak{p}$ has residue degree 1,
- $\mathrm{N}(\mathfrak{p}) \equiv 1 \bmod p$, and
- $\mathrm{N}(\mathfrak{p}) \leq c_0$.

Let $\alpha \in K^\times$ be such that all valuations of α at primes $\mathfrak{p} \notin S_p$ are divisible by d and such that for every $\mathfrak{p} \in T$, the image of α in $K_{\mathfrak{p}}^\times$ is a d-th power. Then $\alpha \in (L^\times)^d$. If in addition L/K is cyclic, then $\alpha \in (K^\times)^d$.

Proof. Note that the degree of L/K is at most $\varphi(d)$ and the discriminant Δ_L of L satisfies

$$\Delta_L \mid \Delta_K^{\varphi(d)} \Delta_{\mathbb{Q}(\zeta_d)}^n.$$

We first prove that α is a d-th power in L. By contradiction, assume otherwise and let β be a d-th root of α in some extension of L, so that $L(\beta)/L$ is a cyclic extension of degree $d' \neq 1$ dividing d. Let χ be a faithful 1-dimensional character

Date: April 2, 2025.

2010 *Mathematics Subject Classification.* Primary: 11Y16, 20C05, 11R32; Secondary 11R29, 11R04, 11Y40, 11R18, 11R27.

of $\mathrm{Gal}(L(\beta)/L)$, which we see as a ray class group character of L of some conductor $\mathfrak{f}$ by class field theory. Write $\mathfrak{f} = \mathfrak{f}_{\mathrm{tame}}\mathfrak{f}_{\mathrm{wild}}$ where $\mathfrak{f}_{\mathrm{tame}}$ and $\mathfrak{f}_{\mathrm{wild}}$ are coprime and $\mathfrak{f}_{\mathrm{wild}}$ is supported at primes above p. By the assumption on the valuations of α, the extension $L(\beta)/L$ is unramified outside the prime ideals that do not lie above a prime in S_p; indeed, locally at every such prime $\mathfrak{P}$, the extension is generated by a p^i-th root of a unit of $L_{\mathfrak{P}}$ for some $i \le r$. Therefore, by [3, Proposition 2.5] applied to $L(\beta)/L$ and χ, we have

$$\log \mathrm{N}(\mathfrak{f}_{\mathrm{wild}}) \le 2n\varphi(d)(\log p + \log \varphi(d)) \le 4nd \log d.$$

In addition, ramification is tame at all primes in S not above p, so we have

$$\mathrm{N}(\mathfrak{f}_{\mathrm{tame}}) \le M_S^d.$$

By [1, Theorem 4], there exists a prime ideal $\mathfrak{P}$ of L that has residue degree 1 (so that $\mathrm{N}(\mathfrak{P}) = 1 \bmod d$), does not lie over primes of S_p, such that $\chi(\mathfrak{P}) \ne 1$ and such that

$$\mathrm{N}(\mathfrak{P}) \le 18 \log^2(\Delta_L^2 \mathrm{N}(\mathfrak{f})) \le 18 \left(2d \log |\Delta_K| + 6nd \log d + d \log M_S\right)^2 = c_0.$$

In particular, the prime ideal $\mathfrak{p} = \mathfrak{P} \cap K$ lies in T, so α is a d-th power in $K_{\mathfrak{p}}^\times$, and *a fortiori* in $L_{\mathfrak{P}}^\times$. This implies that $L(\beta)/L$ is completely split at $\mathfrak{P}$, contradicting the fact that $\chi(\mathfrak{P}) \ne 1$. This proves that $\alpha \in (L^\times)^d$.

Now assume that L/K is cyclic, and let $L' = K(\zeta_p)$. Let $\beta_1, \dots, \beta_d \in L$ be the d-th roots of α, so that we have $L' \subseteq L'(\beta_i) \subseteq L$ for all i. Since L/L' is a cyclic extension of degree a power of p, its intermediate extensions are linearly ordered, so that we may choose our numbering so that $L'(\beta_1) \subseteq L'(\beta_i)$ for all i.

Assume for contradiction that the cyclic extension $L'(\beta_1)/L'$ is nontrivial. Then as above there exists a nontrivial character χ of $\mathrm{Gal}(L'(\beta_1)/L')$ and a prime ideal $\mathfrak{P}$ of L' of degree 1 (so that $\mathrm{N}(\mathfrak{P}) = 1 \bmod p$) such that $\chi(\mathfrak{P}) \ne 1$ and $\mathfrak{p} = \mathfrak{P} \cap K$ lies in T. By hypothesis, α is a d-th power in $K_{\mathfrak{p}}^\times$, so that there exists i such that $\beta_i \in K_{\mathfrak{p}}$; since $L'(\beta_1) \subseteq L'(\beta_i)$, this implies $\beta_1 \in L'_{\mathfrak{P}}$, i.e. $L'(\beta_1)/L'$ is completely split at $\mathfrak{P}$, contradicting $\chi(\mathfrak{P}) \ne 1$. This proves that the extension $L'(\beta_1)/L'$ is trivial, i.e. $\beta_1 \in L'$.

We have $\beta_1^d = \alpha$, so that $\alpha^{[L':K]} = \mathrm{N}_{L'/K}(\alpha) = \mathrm{N}_{L'/K}(\beta_1)^d$, and therefore $\alpha^{[L':K]}$ is a d-th power in K. Since $[L' : K]$ is coprime to d, this implies that α is a d-th power in K, as claimed. $\square$

This does not affect the validity of the rest of the paper.

Acknowledgment. J.-F. Biasse was supported by National Science Foundation grant 183980, National Science Foundation grant 1846166, National Institute of Standards and Technology grant 60NANB17D184, CyberFlorida Collaborative Seed Grant Program and CyberFlorida Capacity Building Program. C. Fieker was supported by Deutsche Forschungsgemeinschaft — Project-ID 286237555 – TRR 195, Project-ID 460135501 - NFDI 29/1 “MaRDI – Mathematische Forschungsdateninitiative” and the state of Rheinland-Pfalz via the Forschungsinitiative and the “SymbTools” project. T. Hofmann was supported by Deutsche Forschungsgemeinschaft — Project-ID 286237555 – TRR 195; and Project-ID 539387714. A. Page was supported by the ANR grant Ciao ANR-19-CE48-0008.

References

[1] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990. 2

[2] Jean-François Biasse, Claus Fieker, Tommy Hofmann, and Aurel Page. Norm relations and computational problems in number fields. *J. Lond. Math. Soc. (2)*, 105(4):2373–2414, 2022. 1

[3] M. R. Murty, V. K. Murty, and N. Saradha. Modular forms and the Chebotarev density theorem. *Amer. J. Math.*, 110(2):253–281, 1988. 2

Department of Mathematics and Statistics, University of South Florida, 4202 East Fowler Ave, CMC342, Tampa, FL 33620-5700, USA
Email address: biasse@usf.edu

Fachbereich Mathematik, Technische Universitat Kaiserslautern, 67663 Kaiserslautern, Germany
Email address: fieker@mathematik.uni-kl.de

Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Strasse 3, 57068 Siegen, Germany
Email address: tommy.hofmann@uni-siegen.de

INRIA, Univ. Bordeaux, CNRS, IMB, UMR 5251, F-33400 Talence, France
Email address: aurel.page@inria.fr