Primary units in cyclotomic fields

Chandan Singh Dalawat
Harish-Chandra Research Institute
Chhatnag Road, Jhunsi, Allahabad 211019, India
dalawat@gmail.com

Résumé. Nous étudions les relations mutuelles entre trois notions d’unités $p$-primaires dans le corps cyclotomique local des racines $p$-ième de 1 ($p$ étant un nombre premier impair), spécialement en référence aux unités globales.

Abstract. We investigate the interrelationships among three notions of $p$-primary units in the local cyclotomic field of $p$-th roots of 1 ($p$ being an odd prime number), especially with reference to global units.

Let $p$ be a prime number (including $p = 2$), $K$ a finite extension of $\mathbb{Q}_p$ containing a primitive $p$-th root $\zeta$ of 1, $\mathfrak{o}$ the ring of integers of $K$, and $\mathfrak{p}$ its unique maximal ideal. Denote by $U_n = \text{Ker}(\mathfrak{o}^\times \to (\mathfrak{o}/\mathfrak{p}^n)^\times)$ the filtration by units of various levels, and by $\bar{U}_n$ the image of $U_n$ in $K^\times/K^\times p$.

Recall that a unit $\alpha \in \mathfrak{o}^\times$ is called $p$-primary if the extension $K(\sqrt[p]{\alpha})$ is unramified over $K$. It is known that $\alpha$ is $p$-primary if and only if its image in $K^\times/K^\times p$ lies in the $\mathbb{F}_p$-line $\bar{U}_{e_1}$ [2, prop. 16], where $e_1$ is the ramification index of $K|\mathbb{Q}_p(\zeta)$. This is equivalent to requiring that $\alpha$ be a $p$-th power in $(\mathfrak{o}/\mathfrak{p}^{pe_1})^\times$ [2, prop. 45].

Assume henceforth that $p$ is odd, that $K = \mathbb{Q}_p(\zeta)$, so that $e_1 = 1$, $\mathfrak{o} = \mathbb{Z}_p[\zeta]$, and $\mathfrak{p} = \pi\mathfrak{o}$, where $\pi = 1 - \zeta$. In this case, there are two other notions of “primary” units, which we have called primaire ($\S2$) and primär ($\S4$), in order to distinguish them from the notion of $p$-primary numbers recalled above.

The purpose of this Note is to compare these three notions, with special reference to the global units $\mathbb{Z}[\zeta]^\times$. We will show that for $\alpha \in \mathbb{Z}[\zeta]^\times$, these

MSC 2000 : 11R18, 11S10. Keywords : $p$-primary numbers, nombres primaires, Primärzahlen, cyclotomic fields, corps cyclotomiques, Kreisteilungskörper.
notations are equivalent to being a $p$-th power in $\mathbb{Z}_p[\zeta]^{\times}$ (prop. 3, prop. 6), although they are inequivalent for local units in general.

This allows us to reconcile three different formulations of Kummer’s lemma to the effect that if the odd prime $p$ is regular — if $p$ does not divide the class number of $\mathbb{Q}(\zeta)$ — then certain units $u \in \mathbb{Z}[\zeta]^{\times}$ are $p$-th powers in $\mathbb{Q}(\zeta)^{\times}$. The difference lies in the hypotheses on $u$; in [5, p. 513], $u$ is required to be $p$-primary (at $p$); in [1, p. 377], $u$ is required to be primaire ($\S$2); in [3, p. 288], $u$ is required to be primär ($\S$4).

1. $p$-primary numbers. — Recall that a 1-unit $\alpha \in U_1$ is a $p$-th power if and only if $\alpha \in U_{p+1}$ [2, prop. 30]; $\alpha$ is $p$-primary if and only if $\alpha \in U_p$, and, finally, $\alpha \equiv 1 \pmod{p}$ if and only if $\alpha \in U_{p-1}$.

2. Nombres primaires. — Traditionally, a global unit $u \in \mathbb{Z}[\zeta]^{\times}$, or more generally an integer $u \in \mathbb{Z}[\zeta]$ prime to $\pi$, is called “primary” if $u \equiv a \pmod{p}$ for some $a \in \mathbb{Z}$ (prime to $p$), but the definition makes sense for all local units. In order to distinguish it from the notion in $\S$1, we will call a local unit $\alpha \in o^{\times}$ primaire if $\alpha \equiv a \pmod{p}$ for some $a \in \mathbb{Z}_p^{\times}$. Such units form a subgroup of $o^{\times}$ containing $o^{\times p}$ (lemma 1).

We show that if a global unit is primaire, then it is not only $p$-primary in $K = \mathbb{Q}_p(\zeta)$ but even a $p$-th power in $K^{\times}$. (At the other primes $l$ of $\mathbb{Q}(\zeta)$, which are prime to $p$, every global unit $u$ is $p$-primary in the sense that adjoining $\sqrt[l]{u}$ to the local field $\mathbb{Q}(\zeta)_l$ gives an unramified extension thereof, although $u$ need not be a $p$-th power in $\mathbb{Q}(\zeta)_l^{\times}$.)

Not every primaire local unit $\alpha \in o^{\times}$ is $p$-primary. Indeed, we have $(o/\mathfrak{p}o)^{\times p} = F_p^{\times}$ (lemma 1), $\mathfrak{p}o = p^{p-1}$, and, in the notation of [2],

\[
\hat{\alpha} \in (o/\mathfrak{p}o)^{\times p} \iff \hat{\alpha} \in \hat{U}_{p-1}
\]

[2, prop. 45], whereas $\hat{U}_{p} \neq \hat{U}_{p-1}$ [2, prop. 42]. For example, $\alpha = 1 + p$ is $\equiv 1 \pmod{p}$ but $\hat{\alpha} \notin \hat{U}_{p}$, so $1 + p$ is primaire but not $p$-primary.

It might still be true that if a global unit $u \in \mathbb{Z}[\zeta]^{\times}$ is primaire, then it is $p$-primary at every place of $\mathbb{Q}(\zeta)$, but only the place $\mathfrak{p}|p$ really matters. Our aim is to verify that not only is this the case, but in fact $u \in K^{\times p}$, whether $p$ is regular or not (prop. 3). Let us begin with a lemma which has already been invoked.

**Lemma 1.** — With the above notation, $(o/\mathfrak{p}o)^{\times p} = F_p^{\times}$.

This is well-known, see [4, p. 130]. The inclusion $F_p^{\times} \subset (o/\mathfrak{p}o)^{\times p}$ is clear, for $F_p^{\times} = F_p^{\times p}$. To see the converse $(o/\mathfrak{p}o)^{\times p} \subset F_p^{\times}$, note that the $F_p$-space $o/\mathfrak{p}o$ admits the basis $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$. Therefore, for every element
$z = \sum_{i=0}^{p-2} a_i \zeta^i$ of $\mathfrak{o}/\mathfrak{p}\mathfrak{o}$ (with $a_i \in \mathbf{F}_p$), the $p$-th power $z^p = \sum_{i=0}^{p-2} a_i$ is in $\mathbf{F}_p$:

$\left(a_0 + a_1 \zeta + \cdots + a_{p-2} \zeta^{p-2}\right)^p \equiv a_0^p + a_1^p + \cdots + a_{p-2}^p \pmod{p}$

\[ \equiv a_0 + a_1 + \cdots + a_{p-2} \pmod{p}. \]

Recall that $p$ is an odd prime, that $K = \mathbf{Q}_p(\zeta)$, that $\mathfrak{o} = \mathbf{Z}_p[\zeta]$, and that $U_i = \text{Ker}(\mathfrak{o}^\times \to (\mathfrak{o}/\mathfrak{p})^\times)$ for $i > 0$. The local ingredient in Kummer’s lemma amounts to $U_{p-1} \cap N \subset U_p$, where $N = \text{Ker}(N_{K|\mathbf{Q}_p} : K^\times \to \mathbf{Q}_p^\times)$. More precisely,

**Proposition 2.** — If a unit $\alpha \in \mathfrak{o}^\times$ is $\equiv a \pmod{p}$ for some $a \in \mathbf{Z}_p^\times$, and if its absolute norm $N_{K|\mathbf{Q}_p}(\alpha) \equiv 1 \pmod{p\pi}$, then $\alpha$ is $p$-primary.

Notice first that we may replace $\alpha$ by $\alpha^{p-1}$: adjoining $\sqrt[3]{\beta}$ or $\sqrt[3]{\beta^{p-1}}$ gives the same extension of $K$, for any $\beta \in K^\times$. We may thus assume that $\alpha \equiv 1 \pmod{p}$, and write $\alpha = 1 + \gamma p$ for some $\gamma \in \mathfrak{o}$, and, as $\mathfrak{o}$ and $\mathbf{Z}_p$ have the same residue field, $\gamma = c + \delta p$ for some $c \in \mathbf{Z}_p$ and $\delta \in \mathfrak{o}$, so that $\alpha = 1 + cp + \delta p \pi$. Now, for every $\sigma \in \text{Gal}(K|\mathbf{Q}_p)$, we have $\sigma(\alpha) = 1 + cp + \sigma(\delta) p \sigma(\pi)$, so that $\sigma(\alpha) \equiv 1 + cp \pmod{p \pi}$, for $\sigma(\pi)$ is also a uniformiser of $K$. Taking the product over all $\sigma$, we get

\[ 1 \equiv N_{K|\mathbf{Q}_p}(\alpha) \equiv (1 + cp)^{p-1} \equiv 1 - cp \pmod{p \pi}. \]

This implies that $cp \equiv 0 \pmod{p \pi}$, and hence $\alpha \equiv 1 \pmod{p \pi}$, showing that $\alpha$ is $p$-primary [2, prop. 16]. This proof is adapted from [6, p. 80].

**Proposition 3.** — If a global unit $u \in \mathbf{Z}[\zeta]^\times$ is primaire, then it is a $p$-th power in $\mathfrak{o}^\times$.

[If $E$ is the image of the global units $\mathbf{Z}[\zeta]^\times$ in the group $\mathfrak{o}^\times = \mathfrak{o}^\times/\mathfrak{o}^{\times p}$ of local units modulo $p$-th powers, and if $(\hat{U}_n)_{n>0}$ denotes the filtration on the latter group, so that $\mathfrak{o}^\times = \hat{U}_1$ and $\hat{U}_{p+1} = \{1\}$, then $E \cap \hat{U}_{p-1} = \{1\}$, although $\hat{U}_{p-1}$ is 2-dimensional over $\mathbf{F}_p$.]

We first need to recall a few facts about global units. Every $u \in \mathbf{Z}[\zeta]^\times$ is (uniquely) of the form $u = \xi w$ for some $p$-th root $\xi$ of 1 and some $w \in \mathbf{Z}[\zeta + \zeta^{-1}]^\times$ “totally real” ([6, p. 3], [4, p. 129]). If moreover $u \equiv a \pmod{\pi^2}$ for some $a \in \mathbf{Z}$, then $u = w$, for $\xi \in U_1$ but $\xi \notin U_2$, unless $\xi = 1$ [6, p. 79]. Hence $N_{\mathbf{Q}(\zeta)|\mathbf{Q}}(u) = N_{\mathbf{Q}(\zeta + \zeta^{-1})|\mathbf{Q}}(u)^2 = 1$, for the norm of a unit is a unit and $\mathbf{Z}^\times \otimes = \{1\}$. Also, $N_{K|\mathbf{Q}_p}(u) = N_{\mathbf{Q}(\zeta)|\mathbf{Q}}(u) = 1$.

Now suppose that $u$ is primaire; in particular, $u \equiv a \pmod{\pi^2}$ for some $a \in \mathbf{Z}$. The above discussion implies that $N_{K|\mathbf{Q}_p}(u) = 1$, and prop. 2 then implies that $u$ is $p$-primary.
But the above discussion also implies that $u$ is in $K^+ = Q_p(\zeta + \zeta^{-1})$. Up to multiplying $u$ by a $p$-th power (such as the multiplicative representative $(a^{-1}) \in \mathfrak{o}^\times$, where $a \in F_p^\times$ is the image of $u$), or replacing $u$ by $w^{p-1}$, we may assume that $u \in U_1$. As for any $p$-primary 1-unit of $K$, we have $u \in U_p$. But if a unit of $K^+$ (such as $u$) is in $U_n$ for some odd $n$ (such as $n = p$), then it is in $U_{n+1}$, because the ramification index of $K|K^+$ is 2. But $U_{p+1} = U_2^p$, so it follows that $u \in K^{x_p}$ [2, prop. 30].

Remark. — Prop. 3 allows us to prove Kummer’s lemma in the variant [1, p. 377] along the same lines as in [5, p. 513], thereby avoiding the $p$-adic logarithm or any extraneous global considerations. Namely, if $u \in Z[\zeta]^\times$ is primaire, then it is $p$-primary, even a local $p$-th power (prop. 3), and hence the extension obtained by adjoining $\sqrt[p]{u}$ to $Q(\zeta)$ is cyclic (of degree 1 or $p$) and unramified everywhere. But if $p$ is regular, $Q(\zeta)$ has no everywhere-unramified cyclic degree-$p$ extension, by class field theory (or as a consequence of Hilbert’s Satz 94, as in [5, p. 523]). Hence $u \in Z[\zeta]^{x_p}$.

3. A general observation. — The local argument of prop. 2 can be generalised so as to bring out its essential features. Let $F$ be any finite extension of $Q_p$, allow $p$ to be 2, and let $L|F$ be a totally but tamely ramified extension of degree $e$ (prime to $p$). Let $\pi_F$ and $\pi_L$ be uniformisers of $F$, $L$ respectively. If a unit $\alpha \in \mathfrak{o}_L^\times$ is $\equiv a$ (mod. $\pi_F^e$) for some $a \in \mathfrak{o}_F^\times$ and some $r > 0$, then clearly its relative norm $N_{L|F}(\alpha)$ is $\equiv a^e$ (mod. $\pi_F^e$).

But if we demand that $N_{L|F}(\alpha) \equiv a^e$ (mod. $\pi_F^e \pi_L$), then it follows that $\alpha \equiv a$ (mod. $\pi_F^e \pi_L$), as the following prop. shows.

Proposition 4. — Suppose that $L|F$ is totally ramified of degree $e$ prime to $p$, and let $\alpha \in \mathfrak{o}_L^\times$. If $\alpha \equiv a$ (mod. $\pi_F^e$) and $N_{L|F}(\alpha) \equiv a^e$ (mod. $\pi_F^e \pi_L$) for some $a \in \mathfrak{o}_F^\times$ and some $r > 0$, then $\alpha \equiv a$ (mod. $\pi_F^e \pi_L$).

Write $\alpha = a + b\pi_F^r + \gamma\pi_F^r \pi_L$, where we assume that $b \in \mathfrak{o}_F$ because $L|F$ is totally ramified, and $\gamma \in \mathfrak{o}_L$. For every $F$-conjugate $\sigma(\alpha)$ of $\alpha$, we have $\sigma(\alpha) = a + b\pi_F^r + \sigma(\gamma)\pi_F^r \pi_L$ and, taking the product over the $e$ $F$-embeddings $\sigma$ of $L$ (in some fixed algebraic closure of $F$), we get

$$a^e \equiv N_{L|F}(\alpha) \equiv (a + b\pi_F^r)^e \equiv a^e + ea^{e-1}b\pi_F^r \pmod{\pi_F^e \pi_L}.$$ 

Therefore, working (mod. $\pi_F^e \pi_L$), we have $ea^{e-1}b\pi_F^r \equiv 0$, so $b\pi_F^r \equiv 0$ (as $e$ and $a$ are units in $L$) and hence $\alpha \equiv a$.

Let $U_m$ (resp. $N_m$) be the group of $\alpha \in \mathfrak{o}_L^\times$ such that $\alpha$ (resp. $N_{L|F}(\alpha)$) is $\equiv 1$ (mod. $\pi_F^m$). Taking $a = 1$ in prop. 4, we get

Corollary 5. — When $L|F$ is totally tamely ramified of degree $e$, we have $U_{re} \cap N_{re+1} = U_{re+1}$ for every $r > 0.$
Prop. 2 was essentially the case $F = \mathbb{Q}_p$ ($p$ odd), $L = \mathbb{Q}_p(\zeta)$, $r = 1$. So, from our local perspective, the basic point in Kummer’s lemma in the formulation [1, p. 377] is that this $L|F$ is totally (but tamely) ramified of degree $p - 1$, and that if $u \in \mathbb{Z}[\zeta]^\times$ is primaire, then its norm is 1. Therefore $u$ is $p$-primary at $\pi$ (and also at every other place of $\mathbb{Q}(\zeta)$).

4. Primärzahlen. — In Hilbert’s Zahlbericht, there is a third, closely allied, notion. He defines it only for prime-to-$\pi$ integers in $\mathbb{Z}[\zeta]$, but it makes sense for all local units $\alpha \in \mathfrak{o}^\times$, where $\mathfrak{o} = \mathbb{Z}_p[\zeta]$ (and $p$ is an odd prime). We say that $\alpha$ is primär if

$$\alpha \equiv a \pmod{\pi^2}, \quad N_{K|K^+}(\alpha) \equiv b \pmod{p}, \quad (a, b \in \mathbb{Z}_p^\times),$$

where $K, K^+$ are the completions of $\mathbb{Q}(\zeta), \mathbb{Q}(\zeta + \zeta^{-1})$ at the unique place above $p$. Such units form a subgroup of $\mathfrak{o}^\times$; the name has been chosen to distinguish them from $p$-primary (§1) or primaire (§2) units.

It is clear that if a local unit $\alpha \in \mathfrak{o}^\times$ is primaire, then it is primär, for $\alpha \equiv a \pmod{p}$ implies $\alpha \equiv a \pmod{\pi^2}$ and $N_{K|K^+}(\alpha) \equiv a^2 \pmod{p}$. In particular, every $p$-th power $\alpha \in \mathfrak{o}^{xp}$ is primär (lemma 1).

The converse is of course true for $p = 3$, but false for $p \neq 3$. Indeed, let $\varpi$ be a $(p - 1)$-th root of $-p$ in $K$ [2, prop. 24], so that $\varpi$ is a uniformiser of $K$ and $\sigma_1(\varpi) = -\varpi$, where $\sigma_1$ is the generator of $Gal(K|K^+)$. It is clear that $\alpha = 1 + \varpi^{p-2}$ is primär but not primaire, if $p > 3$.

If a global unit $u \in \mathbb{Z}[\zeta]^\times$ is primär, and if the prime $p$ is regular, then $u \in \mathbb{Z}[\zeta]^{\times p}$ [3, p. 288]. One might therefore suspect that, in general, a primär global unit is $p$-primary (at the prime $\pi$), even if $p$ is irregular. We show that in fact a primär global unit is always a $p$-th power in $K^\times$.

**Proposition 6.** — If a global unit $u \in \mathbb{Z}[\zeta]^\times$ is primär, then $u \in \mathfrak{o}^{xp}$.

[Denoting by $\mathcal{P}$ the image in $\overline{\mathfrak{o}}^\times = \mathfrak{o}^\times/\mathfrak{o}^{xp}$ of the group of primär local units, and by $\overline{E}$ the image of all global units $\mathbb{Z}[\zeta]^\times$, we have $\mathcal{P} \cap \overline{E} = \{1\}$.]

Suppose that $u$ is primär; it is enough to show that $u' = u^{p-1}$ is a $p$-th power in $K^\times$. Since $u' \equiv 1 \pmod{\pi^2}$, we have $u' \in \mathbb{Z}[\zeta + \zeta^{-1}]^\times$, as in the proof of prop. 3, and hence $u' \in K^+$. But then $N_{K|K^+}(u') = u'^2$, and, as $N_{K|K^+}(u') \in U_{p-1}$ by hypothesis, we have $u' \in U_{p-1}$, for $(\ )^{1/2}$ is an automorphism of the $\mathbb{Z}_p$-module $U_{p-1}$.

We have shown that $u'$ is primaire. As it is also a global unit, prop. 3 implies that $u' \in \mathfrak{o}^{xp}$. Hence $u \in \mathfrak{o}^{xp}$.

(The local ingredient in the above proof says more generally that if $\alpha \in U_{p-1} \cap K^+$ and if $N_{\mathbb{Q}_p|\mathbb{Q}_p}(\alpha) \equiv 1 \pmod{p\pi}$, then $\alpha \in U_{p+1} \subset \mathfrak{o}^{xp}$.)
Indeed, \( \alpha \in U_p \) by prop. 2, and \( U_p \cap K^+ \subset U_{p+1} \), because the ramification index of \( K|K^+ \) is 2 and \( p \) is odd.

5. Summary. — Let us summarise. For local units \( \alpha \in o^\times \), we have

\[
\alpha \in o^{\times p} \implies \alpha \text{ is } p\text{-primary} \implies \alpha \text{ is } \text{primaire} \implies \alpha \text{ is } \text{primär},
\]

and all these implications are strict, except that the last one is an equivalence when \( p = 3 \). But for global units \( \alpha \in \mathbb{Z}[\zeta]^\times \), all three implications are actually equivalences (prop. 3, prop. 6).

Let \( \bar{P} \) be the image in \( \bar{o}^\times = o^\times / o^{\times p} \) of the group of \( \text{primär} \) local units; we have \( \bar{U}_{p-1} \subset \bar{P} \subset \bar{U}_2 \). The above implications can be rewritten as

\[
\{1\} \subset \bar{U}_p \subset \bar{U}_{p-1} \subset \bar{P}
\]

where all three inclusions are strict, except for the last one, which is an equality when \( p = 3 \). Finally, \( \bar{E} \subset \bar{o}^\times \) being the image of the global units \( \mathbb{Z}[\zeta]^\times \), we have \( \bar{E} \cap \bar{P} = \{1\} \) (prop. 6). In short, although the four notions are distinct locally (at \( \pi \)), they are equivalent globally.

(Notice that the \( \mathbb{F}_p \)-dimension of \( \bar{P}/\bar{U}_{p-1} \) grows linearly with \( p \), and equals the number of odd \( a \in [3, p - 2] \) such that \( 2a \geq p - 1 \). Indeed, denoting the set of such \( a \) by \( I \), a basis is provided by the images of \( 1 + \varpi^a \) \( (a \in I) \), where \( \varpi^{p-1} = -p \).)

6. A suggestion. — Starting with Kummer, it is proved at many places that if \( u \in \mathbb{Z}[\zeta]^\times \) is \( p\text{-primary} \) (§1) or \( \text{primaire} \) (§2) or \( \text{primär} \) (§4), and if \( p \) is regular, then \( u \in \mathbb{Z}[\zeta]^{\times p} \). We are advocating that this be done in two steps. The first step, which we have carried out here, is essentially local and says that if \( u \in \mathbb{Z}[\zeta]^\times \) is \( p\text{-primary} \) or \( \text{primaire} \) or merely \( \text{primär} \), then \( u \in \mathbb{Z}_p[\zeta]^{\times p} \); it is valid for all odd primes \( p \), regular or not. The second step, which is global, says of course that if moreover \( p \) is regular, then \( u \in \mathbb{Z}[\zeta]^{\times p} \).

Acknowledgement. The author is grateful to Professor K N Ganesh, director of the Indian Institute of Science Education and Research, Pune, for having gone to great lengths to make a truly enlightening remark on 24/9/2009.

Bibliographic References

[1] Borevich (Z.) & Shafarevich (I.). — Number theory, Academic Press, New York-London, 1966, x+435 pp.
[2] Dalawat (C.). — *Local discriminants, kummerian extensions, and elliptic curves*, Journal of the Ramanujan Mathematical Society, 25 (2010) 1, pp. 25–80. Cf. arXiv:0711.3878v1.

[3] Hilbert (D.). — *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematikervereinigung, 4 (1897), pp. 175–546. = Ges. Abhandlungen I, pp. 63–363.

[4] Kato (K.), Kurokawa (N.) & Saito (T.). — *Number theory 1, Fermat’s dream*, American Mathematical Society, Providence, 2000, xvi+154 pp.

[5] Rosen (M.). — *Remarks on the history of Fermat’s last theorem 1844 to 1984*, in Modular forms and Fermat’s last theorem, Springer, New York, 1997, pp. 505–525.

[6] Washington (L.). — *Introduction to cyclotomic fields*. Springer-Verlag, New York, 1997, xiv+487 pp.