7. A Remark on Higher Circular l-Units

By Yasutaka IHARA
Research Institute for Mathematical Sciences, Kyoto University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 13, 1992)

1. Let l be a prime number, and $E_l = E(\{0,1,\infty\})$ be the group of higher circular l-units defined and studied in [1] [2] (esp. [1] §2·6). As is shown in [1], elements of E_l are *l-units* in the maximal pro-l extension M_l of $\boldsymbol{Q}(\mu_{l^\infty})$ unramified outside l (μ_{l^∞}: the group of l-powerth roots of 1), and $\boldsymbol{Q}(E_l)$ corresponds to the kernel of the canonical representation of the Galois group $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ in the outer automorphism group of the pro-l fundamental group of $\boldsymbol{P}^1-\{0,1,\infty\}$. The main purpose of this note is to prove the following

Theorem. *For any $\varepsilon \in E_l$ and $\sigma \in \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$, $\varepsilon^{\sigma-1}$ is a unit.*

In other words, if $\varepsilon \in E_l$ and k is any finite Galois extension over $\boldsymbol{Q}$ containing ε, then the fractional ideal $(\varepsilon) = \varepsilon\mathcal{O}_k$ is $\mathrm{Gal}(k/\boldsymbol{Q})$-invariant ($\mathcal{O}_k$: the ring of integers of k).

The above theorem holds trivially when l is a *regular* prime. In fact, in this case, l has a unique extension in M_l and hence every l-unit in M_l has the claimed property. (To see that l has a unique extension in M_l, first observe that it is so in the maximal l-elementary abelian extension of $\boldsymbol{Q}(\mu_l)$ unramified outside l; then apply the Burnside principle "a closed subgroup D of a pro-l group G coincides with G if its image $\bar{D}$ on the Frattini quotient $\bar{G}$ of G coincides with $\bar{G}$" to the decomposition group $D \subset \mathrm{Gal}(M_l/\boldsymbol{Q}(\mu_l))$ of an extension of l.) But when l is *irregular*, l does decompose in M_l; hence not all the l-units of M_l can enjoy the property stated in the theorem.

In [1] (§0·2), we raised two questions (a) (b), which, in the present language, read as

(a) $\boldsymbol{Q}(E_l) = M_l$?

(b) *Is E_l the full group of l-units in $\boldsymbol{Q}(E_l)$*?

The above theorem implies that when l is irregular, E_l cannot be the group of all l-units in M_l, and hence at most one of (a) (b) can have an affirmative answer. In any case, it is an interesting open question to characterize the field $\boldsymbol{Q}(E_l)$ and the group E_l.

2. Proof of the theorem. The proof is quite elementary. Let v denote any extension to $\bar{\boldsymbol{Q}}$ of the normalized additive l-adic valuation ord_l of $\boldsymbol{Q}$ (so, $v(l)=1$).

Lemma 1. *If $a = b^l \in \bar{\boldsymbol{Q}}^\times$ and $v(a-1) < l(l-1)^{-1}$, then $v(b-1) = l^{-1} \times v(a-1)$.*

Proof. Decompose $a-1$ into the product of $b-\zeta^i$ over all $i \pmod l$, ζ

being a primitive l-th root of 1. Then $v(b-\zeta^i)<(l-1)^{-1}$ for at least one i. But since $v(\zeta^i-\zeta^j)=(l-1)^{-1}$ for $j\not\equiv i \pmod l$, we have $v(b-\zeta^j)=v(b-\zeta^i)$ for all j. Therefore, $v(b-\zeta^j)=(1/l)v(a-1)$ for all j. Q.E.D.

The following lemma is crucial for proving the theorem. It is a modification of an estimation previously communicated to the author by G. W. Anderson (letter of October 19, 1987).

Lemma 2. *With the notation of* [1], *let* $S\in\mathcal{S}=\mathcal{S}(\{0,1,\infty\})$, *and assume* $l\neq 2, 3$. *Then*

$$(*)\qquad v(a)<l(l-1)^{-1}$$

for any $a\in S\setminus\{0,\infty\}$.

Proof. By induction on S:

IA: "*Valid for* $T(S)$ *for all* $T\in \mathrm{PGL}_2$ *with* $T(S)\ni 0,1,\infty$"

$\Rightarrow$IC: "*so for* $T'(S^{1/l})$ *for all* $T'\in\mathrm{PGL}_2$ *with* $T'(S^{1/l})\ni 0,1,\infty$".

First, if $S=S_0=\{0,1,\infty\}$, then $T(S)=\{0,1,\infty\}$ and $a=1$; hence $v(a)=0$, and $(*)$ is satisfied.

Now let S satisfy the above induction assumption IA, and let $T'(S^{1/l})$ be any PGL_2-transform of $S^{1/l}$ containing $0, 1, \infty$. Take any $c\in T'(S^{1/l})$, $c\neq 0,\infty$. Then T', c are of the form:

$$T'(t)=\frac{b_2-b_3}{b_2-b_1}\cdot\frac{t-b_1}{t-b_3},\qquad c=\frac{b_2-b_3}{b_2-b_1}\cdot\frac{b_4-b_1}{b_4-b_3},$$

where $a_i=b_i^l\in S$ $(i=1,\cdots,4)$. (When one of the b_i is ∞, the two factors, such as $t-b_i$, b_i-b_j, involving this b_i should be cancelled out.) First, assume that a_i are distinct and finite. Then by using IA for $T_j(S)$, where $T_j(t)=1-a_j^{-1}t$, we obtain

$$v(1-a_j^{-1}a_i)<l(l-1)^{-1}\quad (i\neq j);$$

hence

$$(**)\qquad v(1-b_j^{-1}b_i)=l^{-1}\cdot v(1-a_j^{-1}a_i)$$

by Lemma 1. Therefore, $v(b_j-b_i)=l^{-1}v(a_j-a_i)$ for $i\neq j$. Therefore, we obtain the desired inequality IC:

$$v(c)=\frac{1}{l}v\left(\frac{a_2-a_3}{a_2-a_1}\cdot\frac{a_4-a_1}{a_4-a_3}\right)<(l-1)^{-1}<l(l-1)^{-1},$$

by using IA for

$$T(t)=\frac{a_2-a_3}{a_2-a_1}\cdot\frac{t-a_1}{t-a_3}.$$

When $a_1=a_4$, $a_2=a_3$, and are finite, the estimation of $v(c)$ will become the "worst". In this case,

$$c=\frac{b_2}{b_2-b_1}\,\frac{b_4}{b_4-b_3}(1-\zeta)(1-\zeta')$$

$(\zeta,\zeta'\in\mu_l\setminus\{1\})$. First, note that the above equality $(**)$ remains valid for $i, j=1, 2$ of this case. This gives

$$v(b_2(b_2-b_1)^{-1})=l^{-1}v(a_2(a_2-a_1)^{-1}).$$

But $a_2(a_2-a_1)^{-1}=T(0)\in T(S)$, for $T(t)=(t-a_2)(a_1-a_2)^{-1}$; hence $v(a_2(a_2-a_1)^{-1})<l(l-1)^{-1}$ by IA. Therefore, $v(b_2(b_2-b_1)^{-1})<(l-1)^{-1}$. Similarly,

$v(b_4(b_4-b_3)^{-1})<(l-1)^{-1}$. Therefore, $v(c)<4(l-1)^{-1}<l(l-1)^{-1}$, as $l\geq 5$.

The other cases are simpler and will be omitted. Q.E.D.

Lemma 3. *Assume $l\neq 2,3$. If $S\in\mathcal{S}$, $a, a'\in S\backslash\{\infty\}$ and $a\neq a'$, then $(a-a')^{\sigma-1}$ is a unit.*

Proof. Induction on S;

"valid for S" $\Rightarrow$ "valid for $T(S)$, $S^{1/l}$".

(i) For $T(S)$. This is trivial, as the difference of two distinct elements of $T(S)$ can be expressed as the ratio of two elements each of which is a product of at most 3 elements of the form $s-s'(s, s'\in S\backslash(\infty))$.

(ii) For $S^{1/l}$: Take $a, a'\in S$, and b, b', with $b^l=a$, $b'^l=a'$, $b\neq b'$. Consider the element $(b-b')^{\sigma-1}$. If $a=a'$, then $a\neq 0$, and hence $a^{\sigma-1}=(a-0)^{\sigma-1}$ is a unit by the induction assumption. Hence $b^{\sigma-1}$ is also a unit (being an l-th root of $a^{\sigma-1}$). Moreover, $(1-\zeta)^{\sigma-1}$ is a unit for any $\zeta\in\mu_l\backslash\{1\}$. Therefore, $(b-b')^{\sigma-1}$ is a unit in this case.

Now suppose that $a\neq a'$, $a'\neq 0$. Put $\beta=bb'^{-1}$ and $\alpha=\beta^l=aa'^{-1}$. Then $(\alpha-1)^{\sigma-1}=(a-a')^{\sigma-1}/a'^{\sigma-1}$ is a unit by the induction assumption. In particular, $v(\alpha^\sigma-1)=v(\alpha-1)$. By Lemma 2 applied to $1-\alpha\in T(S)(T(t)=1-a'^{-1}t)$, we obtain $v(\alpha-1)<l(l-1)^{-1}$. Thus, Lemma 1 gives

$$v(\beta-1)=v(\beta^\sigma-1)=\frac{1}{l}v(\alpha-1).$$

Therefore, $v((\beta-1)^{\sigma-1})=0$ for any extension v of ord_l. Since $\beta-1\in E_l$ is an l-unit ([1] Prop. 2·5·1.), this implies that $(\beta-1)^{\sigma-1}$ is a unit. Since $b'^{\sigma-1}$ is also a unit (being an l-th root of $a'^{\sigma-1}$ which is a unit by the induction assumption), $(b-b')^{\sigma-1}$ is unit. Q.E.D.

Now, to prove the theorem we may assume l irregular, in particular $l>3$. By Lemma 3 applied to the case $a'=0$, we see that $a^{\sigma-1}$ is a unit for all $a\in S\backslash\{0,\infty\}$. Since E_l is generated by $S\backslash\{0,\infty\}$ $(S\in\mathcal{S})$, the theorem follows.

Acknowledgment. The author wishes to thank Greg W. Anderson for his generosity to have allowed me to use a modification of his earlier estimation as a crucial lemma (§2, Lemma 2).

References

[1] Anderson, G. and Ihara, Y.: Pro-l branched coverings of $\boldsymbol{P}^1$ and higher circular l-units. Ann. of Math., **128**, 271–293 (1988).

[2] ——: Part 2. International J. of Math., 1, 119–148 (1990).