Commun. Korean Math. Soc. **35** (2020), No. 2, pp. 481–486
https://doi.org/10.4134/CKMS.c190249
pISSN: 1225-1763 / eISSN: 2234-3024

UNIT GROUPS OF QUOTIENTS OF NUMBER FIELDS

Jerson Caro-Reyes and Guillermo Mantilla-Soler

Abstract. Let K be a number field. Here we give an explicit description of the group $(O_K/I)^*$ for most ideals I. In particular, we give a complete characterization of such group for those ideals I that are coprime to the different ideal $\mathcal{D}_K$.

1. Introduction

Let K be a number field and let $I \lhd O_K$ be a non zero ideal. In this paper we are interested in having an explicit description, as in the case $K = \mathbb{Q}$, of the finite abelian group $(O_K/I)^*$. The structure of such groups is probably known since the time of Hasse but an explicit description as the one we give here seems to be missing from the literature. There are some examples in which such calculations have been carried out, mostly for quadratic and certain cubic fields (see [1], [4]). For instance in [1, Theorems 3.1, 4.1, 4.2, 5.4, 7.1, 7.2] the authors calculate such explicit description for monogenic cubic fields of square free discriminant; it is in fact such paper what motivated us to write this article. The strategy in [1] is to divide the problem in several cases, in terms of possible ramification, and then use the monogenicity and the hypothesis on the discriminant. For each possible ramification the authors obtain the six theorems mentioned above. Here we do not assume any hypothesis on the degree, discriminant or the structure of the ring of integers. Moreover, we write a cohesive result that includes all the cases, except when $p = 3$ ramifies, described in [1]. Our main result is the following:

Theorem (Cf. Theorem 2.6)**.** *Let K be a number field. Let $\mathfrak{P}$ be a prime ideal in O_K lying over a prime p and let e, f be respectively the ramification and residue degrees of $\mathfrak{P}$ over p. Let n be a positive integer and let q,r be the unique non negative integers with $0 \leq r \leq e-1$ such that $n-1 = eq+r$. Suppose that either $p > e+1$, $p = 2$ or that $n \leq 2$. Then,*

$$(O_K/\mathfrak{P}^n)^* \cong \begin{cases} (\mathbb{Z}/p^{q+1}\mathbb{Z})^{rf} \times (\mathbb{Z}/p^q\mathbb{Z})^{(e-r)f} \times \mathbb{Z}/(p^f-1)\mathbb{Z} & \text{if } p \text{ is odd,} \\ \mathrm{Syl}_2((\mathbb{Z}/2^n\mathbb{Z})^*) \times (\mathbb{Z}/2^{n-1}\mathbb{Z})^{f-1} \times \mathbb{Z}/(2^f-1)\mathbb{Z} & \text{if } p = 2 \text{ and } e = 1. \end{cases}$$

Received July 19, 2019; Revised September 26, 2019; Accepted October 14, 2019.
2010 *Mathematics Subject Classification.* Primary 11R04, 11R27.
Key words and phrases. Quotients of number fields, unit groups.

In particular, if $e = 1$

$$(O_K/\mathfrak{P}^n)^* \cong \mathrm{Syl}_p((\mathbb{Z}/p^n\mathbb{Z})^*) \times (\mathbb{Z}/p^{n-1}\mathbb{Z})^{f-1} \times \mathbb{Z}/(p^f-1)\mathbb{Z}.$$

Here by $\mathrm{Syl}_p((\mathbb{Z}/p^n\mathbb{Z})^*)$ *we mean the group*

$$\mathrm{Syl}_p((\mathbb{Z}/p^n\mathbb{Z})^*) := \begin{cases} \mathbb{Z}/p^{n-1}\mathbb{Z} & \text{if } p \text{ is odd or } n = 1, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{(n-2)}\mathbb{Z} & \text{otherwise.} \end{cases}$$

In the case of quadratic or cubic fields the above theorem does not cover ramified primes lying over 2 and 3. Such cases can be done "by hand" given that there are explicit parametrizations of the ring of integers in such fields; even though the authors in [1] do it only for monogenic fields the same proof of their result for $p = 3$ can be carried out using the of Delone-Faddeev-Gan-Gross-Savin parametrization (see for instance [2, §5]). The remaining missing cases of the above theorem seem hard to describe in a cohesive way. For instance, in the case of cubic fields in which 3 ramifies the structure of the group depends not only on the residue and ramification degrees but also on the residue class of the discriminant modulo 9. At the moment the best we can get, for an explicit description, is for those ideals that contain no ramification. Explicitly:

Theorem (Cf. Theorem 2.7)**.** *Let* K *be a number field and let* I *be a non zero ideal of* O_K*. Let* $I = \mathfrak{P}_1^{n_1} \cdot \ldots \cdot \mathfrak{P}_m^{n_m}$ *be the prime factorization of* I*. Let* p_i *be the rational prime lying under* $\mathfrak{P}_i$ *and let* f_i *be the residue degree of* $\mathfrak{P}_i$ *over* p_i*. If* I *is coprime to the different ideal* $\mathcal{D}_K$*, then*

$$(O_K/I)^* \cong \prod_{i=1}^{m} \left(\mathrm{Syl}_{p_i}((\mathbb{Z}/p_i^{n_i}\mathbb{Z})^*) \times (\mathbb{Z}/p_i^{n_i-1}\mathbb{Z})^{f_i-1} \times \mathbb{Z}/(p_i^{f_i}-1)\mathbb{Z} \right).$$

2. Proofs of results

The calculation of the structure of units in quotients of global fields is done by going over a completion and doing the equivalent calculations over local fields. Here we give proofs of the necessary tools over p-adic fields to obtain our results. As we have mentioned before all of this is elementary however it is missing from the literature (see [1] and its references).

Proposition 2.1. *Let* p *be a prime and let* $\mathcal{K}$ *be a finite field extension of* $\mathbb{Q}_p$*. Let* $\mathcal{B}$ *be the maximal ideal of* $O_{\mathcal{K}}$*, and for any positive integer* m *let* $U^{(m)} = 1 + \mathcal{B}^m$ *be the group of* m*-units. Then, for every positive integer* n

$$(O_{\mathcal{K}}/\mathcal{B}^n)^* \cong U^{(1)}/U^{(n)} \times (O_{\mathcal{K}}/\mathcal{B})^*.$$

Proof. Let $(O_{\mathcal{K}}/\mathcal{B}^n)^* \to (O_{\mathcal{K}}/\mathcal{B})^*$ be the projection map. Since the following sequence is exact

$$1 \longrightarrow U^{(1)}/U^{(n)} \longrightarrow (O_{\mathcal{K}}/\mathcal{B}^n)^* \longrightarrow (O_{\mathcal{K}}/\mathcal{B})^* \longrightarrow 1,$$

the result follows from the fact that $U^{(1)}/U^{(n)}$ is a p-group and that $(O_{\mathcal{K}}/\mathcal{B})^*$ has order coprime to p. □

Theorem 2.2. *Let K be a number field. Let $\mathfrak{P}$ be a prime ideal in O_K lying over a prime p and let e be the ramification degree of $\mathfrak{P}$ over p. Let n be a positive integer. Suppose that either $p > e+1$ or that $n \leq 2$. Then, there is an isomorphism of abelian groups*

$$(O_K/\mathfrak{P}^n)^* \cong O_K/\mathfrak{P}^{n-1} \times (O_K/\mathfrak{P})^*.$$

Proof. Let $\mathcal{K}$ be the $\mathfrak{P}$-completion of K and let $\mathcal{B} = \mathfrak{P}O_{\mathcal{K}}$. Since for every non-negative integer m there is a ring isomorphism $O_{\mathcal{K}}/\mathcal{B}^m \cong O_K/\mathfrak{P}^m$ it follows from Proposition 2.1 that

$$(O_K/\mathfrak{P}^n)^* \cong U^{(1)}/U^{(n)} \times (O_K/\mathfrak{P})^*.$$

Hence, the result follows from the facts (see [3, Ch II, Prop 3.10, Prop 5.5]) $U^{(1)}/U^{(2)} \cong O_{\mathcal{K}}/\mathcal{B}$ and that for $p > e+1$ the p-adic logarithm map induces a group isomorphism

$$U^{(1)}/U^{(n)} \cong O_{\mathcal{K}}/\mathcal{B}^{n-1}.$$ □

Proposition 2.3. *Let K be a number field and let $\mathfrak{P}$ be a prime ideal in O_K lying over a prime p and let e and f be the usual. Let m be a non negative integer, let $0 \leq r \leq e-1$ be the residue class of m modulo e and let $q = \frac{m-r}{e}$. Then, there is an isomorphism of abelian groups*

$$O_K/\mathfrak{P}^m \cong (\mathbb{Z}/p^{q+1}\mathbb{Z})^{rf} \times (\mathbb{Z}/p^q\mathbb{Z})^{(e-r)f}.$$

Proof. To simplify things we divide the proof in two cases depending on whether or not $e \geq m$.

(1) Let us suppose first that $e \geq m$. In this case $p \in \mathfrak{P}^m$ hence $O_K/\mathfrak{P}^m$ is a $\mathbb{Z}/p\mathbb{Z}$-module of size p^{mf} in particular $O_K/\mathfrak{P}^m \cong (\mathbb{Z}/p\mathbb{Z})^{mf}$.

(2) Now, let us assume that $e < m$. By the classification theorem of finite abelian groups there are positive integers $a_1 \leq a_2 \leq \cdots \leq a_d$ such that

$$O_K/\mathfrak{P}^m \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_d}\mathbb{Z}.$$

The exponent of the group $O_K/\mathfrak{P}^m$ is p^{a_d} and it can be calculated as follows: a_d is the smallest positive integer such that $p^{a_d}O_K \subseteq \mathfrak{P}^m$. Since locally $p^{a_d}O_K = \mathfrak{P}^{ea_d}$ we have that $a_d = \lceil \frac{m}{e} \rceil$. Let $V_{\mathfrak{P}}$ be the discrete valuation of K induced by $\mathfrak{P}$, where $V_{\mathfrak{P}}(p) = e$. An element $\alpha \in O_K$ is p-torsion in the quotient $O_K/\mathfrak{P}^m$ if and only if $V_{\mathfrak{P}}(p\alpha) \geq m$, i.e., α is p-torsion if and only if $V_{\mathfrak{P}}(\alpha) \geq m-e$. In other words $(O_K/\mathfrak{P}^m)[p] = \mathfrak{P}^{m-e}/\mathfrak{P}^m \cong O_K/\mathfrak{P}^e \cong (\mathbb{Z}/p\mathbb{Z})^{ef}$. Where the last isomorphism is obtained thanks to case 1 of the proof. Hence,

$$d = \dim_{\mathbb{F}_p}((O_K/\mathfrak{P}^m)[p]) = ef.$$

Since $a_d = \lceil \frac{m}{e} \rceil \leq q+1$ the group $O_K/\mathfrak{P}^m$ is a $\mathbb{Z}/p^{q+1}\mathbb{Z}$-module. In particular, as an abelian group, $O_K/\mathfrak{P}^m$ is isomorphic to a direct product of groups of the form $\mathbb{Z}/p^t\mathbb{Z}$ for t at most $q+1$. Let λ and μ respectively be the number of $\mathbb{Z}/p^{q+1}\mathbb{Z}$ copies (resp. $\mathbb{Z}/p^q\mathbb{Z}$ copies) appearing in the decomposition of

$O_K/\mathfrak{P}^m$. Since $O_K/\mathfrak{P}^m$ is a $\mathbb{Z}/p^{q+1}\mathbb{Z}$-module, $p^qO_K/\mathfrak{P}^m$ is a $\mathbb{Z}/p\mathbb{Z}$-module, and moreover $\lambda = \dim_{\mathbb{F}_p}(p^qO_K/\mathfrak{P}^m)$. Since $V_{\mathfrak{P}}(p^q) = eq$ and $m = eq + r$, we see that $p^qO_K/\mathfrak{P}^m \cong O_K/\mathfrak{P}^r \cong (\mathbb{Z}/p\mathbb{Z})^{rf}$. Thus, $\lambda = rf$. Since in this case, i.e., $e < m$, q is positive we have that $\#(p^{q-1}O_K/\mathfrak{P}^m) = p^{2\lambda+\mu}$. On the other hand $p^{q-1}O_K/\mathfrak{P}^m \cong O_K/\mathfrak{P}^{e+r}$, hence comparing sizes we get that $f(e+r) = 2\lambda + \mu = 2rf + \mu$ thus $\mu = (e-r)f$. Finally since

$$\#(O_K/\mathfrak{P}^m) = p^{mf} = p^{eqf+rf} = p^{(q+1)rf+q(e-r)f} = p^{(q+1)\lambda+q\mu}$$

we see that there can not be other factors, besides $\mathbb{Z}/p^q\mathbb{Z}$ and $\mathbb{Z}/p^{q+1}\mathbb{Z}$, in the decomposition of $O_K/\mathfrak{P}^m$. In particular there is an isomorphism of abelian groups

$$O_K/\mathfrak{P}^m \cong (\mathbb{Z}/p^{q+1}\mathbb{Z})^{rf} \times (\mathbb{Z}/p^q\mathbb{Z})^{(e-r)f}.$$

Notice that if $e > m$, then $q = 0$ and $r = m$. Moreover, if $e = m$, then $q = 1$ and $r = 0$. Either way the formula obtained in case 2 also applies to case 1. □

Lemma 2.4. *Let p be a prime and let f be a positive integer. Suppose that H is a $\mathbb{Z}_p$-submodule of $\mathbb{Z}_p^f$ such that $\mathbb{Z}_p^f/H \cong (\mathbb{Z}/p\mathbb{Z})^{f-1}$. Then, there is an automorphism ϕ of $\mathbb{Z}_p^f$ such that $\phi(H) = \mathbb{Z}_p \times (p\mathbb{Z}_p)^{f-1}$. In particular, for all non-negative integer m*

$$\mathbb{Z}_p^f/p^mH \cong \mathbb{Z}/p^m\mathbb{Z} \times (\mathbb{Z}/p^{m+1}\mathbb{Z})^{f-1}.$$

Proof. Since $\mathbb{Z}_p^f/H$ is p-torsion we have that $p\mathbb{Z}_p^f \subseteq H$. Moreover, by comparing sizes, $H/p\mathbb{Z}_p^f \cong \mathbb{Z}/p\mathbb{Z}$. Let $t \in H$ be an element in the preimage of 1. In particular, H is the $\mathbb{Z}_p$-module generated by t and $p\mathbb{Z}_p^f$. Let $\alpha_i \in \mathbb{Z}_p$, for $i = 1, \ldots, f$, be the coordinates of t in $\{e_1, \ldots, e_f\}$, the canonical $\mathbb{Z}_p$ basis of $\mathbb{Z}_p^f$. Since t is not in $p\mathbb{Z}_p^f$ there must exist some of $\alpha_i \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Without loss of generality we assume that $\alpha_1 \notin p\mathbb{Z}_p$. It follows that $\mathfrak{B} := \{t, e_2, \ldots, e_f\}$ is also a $\mathbb{Z}_p$-basis of $\mathbb{Z}_p^f$ hence the map induced by $\phi(t) = e_1$ and $\phi(e_i) = e_i$, for $i = 2, \ldots, f$, is a $\mathbb{Z}_p$-automorphism of $\mathbb{Z}_p^f$. By construction $\phi(H) = \mathbb{Z}_p \times (p\mathbb{Z}_p)^{f-1}$. □

Lemma 2.5. *Let K be a number field. Let $\mathfrak{P}$ be a prime ideal in O_K lying over 2. Let e and f be as usual. Suppose that $e = 1$. Then, for every positive integer n*

$$(O_K/\mathfrak{P}^n)^* \cong (\mathbb{Z}/2^n\mathbb{Z})^* \times (\mathbb{Z}/2^{n-1}\mathbb{Z})^{f-1} \times (O_K/\mathfrak{P})^*,$$

where $(\mathbb{Z}/2^n\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ if $n \geq 2$ and trivial otherwise.

Proof. We may assume that $n \geq 2$. Arguing similarly to the proof of Theorem 2.2 it is enough to show that

$$U^{(1)}/U^{(n)} \cong (\mathbb{Z}/2^n\mathbb{Z})^* \times (\mathbb{Z}/2^{n-1}\mathbb{Z})^{f-1}.$$

Let m be an integer such that $2 \leq m \leq n$. Let $\mathcal{K}$ be the $\mathfrak{P}$-completion of K and let $\mathcal{B} = \mathfrak{P}O_{\mathcal{K}}$. As in the proof of Theorem 2.2, using the 2-adic logarithm

(see [3, Ch II, Prop 5.5])

$$U^{(m)} \cong \mathcal{B}^m \cong \mathbb{Z}_2^f \text{ and } U^{(m)}/U^{(n)} \cong O_K/\mathfrak{P}^{n-m} \cong (\mathbb{Z}/2^{n-m}\mathbb{Z})^f.$$

The last isomorphism is obtained thanks to Proposition 2.3. In particular,

$$U^{(m)}/\left(U^{(m)}\right)^2 \cong \mathbb{Z}_2^f/2\mathbb{Z}_2^f \cong (\mathbb{Z}/2\mathbb{Z})^f \text{ and } U^{(m)}/U^{(m+1)} \cong (\mathbb{Z}/2\mathbb{Z})^f.$$

Since $\left(U^{(m)}\right)^2 \subseteq U^{(m+1)}$ it follows from the above that $\left(U^{(m)}\right)^2 = U^{(m+1)}$. In particular, $U^{(n)} = \left(U^{(2)}\right)^{2^{(n-2)}}$. Since $\mathcal{K}/\mathbb{Q}_2$ is unramified the torsion subgroup of $U^{(1)}$ is ± 1 hence $U^{(1)} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^f$ (see [3, Ch. II, proof of Prop 5.7]). Since $U^{(2)}$ is torsion free, using the projection map onto the second component $U^{(1)} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^f$, we get $U^{(2)} \cong H \lhd \mathbb{Z}_2^f$. Thus,

$$U^{(1)}/U^{(n)} = U^{(1)}/\left(U^{(2)}\right)^{2^{(n-2)}} \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}_2^f)/2^{(n-2)}H.$$

By [3, Ch. II, Prop 3.10] and Proposition 2.3, $U^{(1)}/U^{(2)} \cong O_K/\mathfrak{P} \cong (\mathbb{Z}/2\mathbb{Z})^f$. In particular, $\mathbb{Z}_2^f/H \cong (\mathbb{Z}/2\mathbb{Z})^{f-1}$. It follows from Lemma 2.4 that

$$\mathbb{Z}_2^f/2^{n-2}H \cong \mathbb{Z}/2^{n-2}\mathbb{Z} \times (\mathbb{Z}/2^{n-1}\mathbb{Z})^{f-1}.$$

Therefore

$$U^{(1)}/U^{(n)} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \times (\mathbb{Z}/2^{n-1}\mathbb{Z})^{f-1}. \qquad \square$$

Theorem 2.6. *Let K be a number field. Let $\mathfrak{P}$ be a prime ideal in O_K lying over a prime p and let e, f be respectively the ramification and residue degrees of $\mathfrak{P}$ over p. Let n be a positive integer and let q, r be the unique non negative integers such that $n-1 = eq + r$ and $0 \le r \le e-1$. Suppose that either $p > e+1$, $p = 2$ or that $n \le 2$. Then,*

$$(O_K/\mathfrak{P}^n)^* \cong \begin{cases} (\mathbb{Z}/p^{q+1}\mathbb{Z})^{rf} \times (\mathbb{Z}/p^q\mathbb{Z})^{(e-r)f} \times \mathbb{Z}/(p^f-1)\mathbb{Z} & \text{if } p \text{ is odd,} \\ (\mathbb{Z}/2^n\mathbb{Z})^* \times (\mathbb{Z}/2^{n-1}\mathbb{Z})^{f-1} \times \mathbb{Z}/(2^f-1)\mathbb{Z} & \text{if } p = 2 \text{ and } e = 1. \end{cases}$$

In particular, if $e = 1$,

$$(O_K/\mathfrak{P}^n)^* \cong \mathrm{Syl}_p((\mathbb{Z}/p^n\mathbb{Z})^*) \times (\mathbb{Z}/p^{n-1}\mathbb{Z})^{f-1} \times \mathbb{Z}/(p^f-1)\mathbb{Z}.$$

Proof. Let us suppose first that p is odd. Thanks to Theorem 2.2 we have that

$$(O_K/\mathfrak{P}^n)^* \cong O_K/\mathfrak{P}^{n-1} \times (O_K/\mathfrak{P})^*.$$

Since $\mathfrak{P}$ is maximal, the group $(O_K/\mathfrak{P})^*$ is cyclic and has order $p^f - 1$. The structure of the group $O_K/\mathfrak{P}^{n-1}$ is given by Proposition 2.3. For the last part notice that if $e = 1$, then $r = 0$ and $q = n-1$ hence, in such case, $(O_K/\mathfrak{P}^n)^* \cong (\mathbb{Z}/p^{n-1}\mathbb{Z})^f \times \mathbb{Z}/(p^f-1)\mathbb{Z}$ from which the last part follows. The case $p = 2$ is done in Lemma 2.5. $\square$

As an immediate consequence of the above we deduce:

Theorem 2.7. *Let K be number field and let I be a non zero ideal of O_K. Let $I = \mathfrak{P}_1^{n_1} \cdot \ldots \cdot \mathfrak{P}_m^{n_m}$ be the prime factorization of I. Let p_i be the rational prime lying under $\mathfrak{P}_i$ and let f_i be the residue degree of $\mathfrak{P}_i$ over p_i. If I is coprime to the different ideal $\mathcal{D}_K$, then*

$$(O_K/I)^* \cong \prod_{i=1}^{m} \left(\mathrm{Syl}_{p_i}((\mathbb{Z}/p_i^{n_i}\mathbb{Z})^*) \times (\mathbb{Z}/p_i^{n_i-1}\mathbb{Z})^{f_i-1} \times \mathbb{Z}/(p_i^{f_i}-1)\mathbb{Z} \right).$$

Proof. This follows from the Chinese reminder theorem and the last part of Theorem 2.6. □

Acknowledgments. We would like to thank the referee for the careful reading of the paper, and for their helpful comments.

References

[1] A. Harnchoowong and P. Ponrod, *Unit groups of quotient rings of integers in some cubic fields*, Commun. Korean Math. Soc. **32** (2017), no. 4, 789–803. https://doi.org/10.4134/CKMS.c160254

[2] G. Mantilla-Soler, *Integral trace forms associated to cubic extensions*, Algebra Number Theory **4** (2010), no. 6, 681–699. https://doi.org/10.2140/ant.2010.4.681

[3] J. Neukirch, *Algebraic Number Theory*, translated from the 1992 German original and with a note by Norbert Schappacher, Grundlehren der Mathematischen Wissenschaften, **322**, Springer-Verlag, Berlin, 1999. https://doi.org/10.1007/978-3-662-03983-0

[4] A. Ranum, *The group of classes of congruent quadratic integers with respect to a composite ideal modulus*, Trans. Amer. Math. Soc. **11** (1910), no. 2, 172–198. https://doi.org/10.2307/1988676

Jerson Caro-Reyes
Department of Mathematics
Universidad Católica de Chile
Santiago, Chile
Email address: jersoncaro459@gmail.com

Guillermo Mantilla-Soler
Department of Mathematics
Konrad Lorenz University
Bogotá, Colombia
Email address: gmantelia@gmail.com