Journal of Number Theory 171 (2017) 198–212

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Galois structure on integral valued polynomials

Bahar Heidaryan [a,b], Matteo Longo [a,*], Giulio Peruginelli [a]

[a] *Dipartimento di Matematica, Università di Padova, Via Trieste 63, 35121 Padova, Italy*
[b] *Department of Mathematics, Tarbiat Modares University, 14115-134 Tehran, Iran*

A R T I C L E I N F O

Article history:
Received 4 November 2015
Received in revised form 13 July 2016
Accepted 13 July 2016
Available online 5 September 2016
Communicated by D. Goss

MSC:
13F20
11R32
11S20
11C08

Keywords:
Characteristic ideal
Finite Galois extension
Integer-valued polynomial
Regular basis
Tame ramification
Null ideal

A B S T R A C T

We characterize finite Galois extensions K of the field of rational numbers in terms of the rings $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$, recently introduced by Loper and Werner, consisting of those polynomials which have coefficients in $\mathbf{Q}$ and such that $f(\mathcal{O}_K)$ is contained in $\mathcal{O}_K$. We also address the problem of constructing a basis for $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ as a $\mathbf{Z}$-module.

* Corresponding author.
E-mail addresses: b.heidaryan@modares.ac.ir (B. Heidaryan), mlongo@math.unipd.it (M. Longo), gperugin@math.unipd.it (G. Peruginelli).

http://dx.doi.org/10.1016/j.jnt.2016.07.007

1. Introduction

The main object of this paper is to study the class of rings

$$\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K) := \mathrm{Int}(\mathcal{O}_K) \cap \mathbf{Q}[X]$$

where K varies among the set of finite Galois extensions of $\mathbf{Q}$; here $\mathcal{O}_K$ is the ring of algebraic integers of K and $\mathrm{Int}(\mathcal{O}_K)$ is the ring of polynomials $f \in K[X]$ such that $f(\mathcal{O}_K)$ is contained in $\mathcal{O}_K$.

The rings $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ have been introduced in [LW12] and studied also in [Per14b]. Among other things, the authors of [LW12] proved that $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ is a Prüfer domain. It is immediate to see that $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ is contained in

$$\mathrm{Int}(\mathbf{Z}) = \{f \in \mathbf{Q}[X] \mid f(\mathbf{Z}) \subseteq \mathbf{Z}\},$$

the classical ring of integer-valued polynomials. Moreover, if K is a proper field extension of $\mathbf{Q}$, then $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ is properly contained in $\mathrm{Int}(\mathbf{Z})$: in fact, let $p \in \mathbf{Z}$ be a prime which is not totally split in $\mathcal{O}_K$; then it is not difficult to see that the polynomial

$$f(X) = \frac{X(X-1)\dots(X-(p-1))}{p}$$

is in $\mathrm{Int}(\mathbf{Z})$ but not in $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$. This is an evidence of the fact that, for a finite Galois extension $K/\mathbf{Q}$, the ring $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ is completely determined by the set of primes $p \in \mathbf{Z}$ which are totally split in $\mathcal{O}_K$, and therefore by the field K itself. Our main result is a characterization of finite Galois extensions of $\mathbf{Q}$ in terms of the rings $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$. More precisely, as a corollary of our main result Theorem 2.7, we prove the following:

Theorem 1.1. *Let K and K' be finite Galois extensions of $\mathbf{Q}$. Then $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ is equal to $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K'})$ if and only if $K = K'$.*

The statement is false if we consider finite extensions of $\mathbf{Q}$ which are not Galois. In fact, if $K/\mathbf{Q}$ is a finite non-Galois extension and K' is any conjugate field of K over $\mathbf{Q}$ different from K, then it is easy to see that $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K) = \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K'})$.

A study somehow related to the present paper about the so-called polynomial overrings of $\mathrm{Int}(\mathbf{Z})$, that is, rings R such that $\mathrm{Int}(\mathbf{Z}) \subseteq R \subseteq \mathbf{Q}[X]$, has been recently done in [CP16], in which a complete and thorough classification of such rings has been given: each of them can be realized as the ring of integer-valued polynomials over some closed subset of the profinite completion of $\mathbf{Z}$.

We can reformulate our main result in more abstract terms as follows. Denote by $\mathcal{G}$ the category whose objects are ring of integers $\mathcal{O}_K$ of finite Galois extensions $K/\mathbf{Q}$ with homomorphism given by inclusions, and by $\mathcal{C}$ the category of subrings of $\mathbf{Q}[X]$ in which morphisms are again inclusions. Then the functor

$$\mathrm{Int}_{\mathbf{Q}} : \mathcal{G} \longrightarrow \mathcal{C}$$

which takes an object $\mathcal{O}_K$ of $\mathcal{G}$ to $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ and the inclusion $\mathcal{O}_K \subseteq \mathcal{O}_{K'}$ to the inclusion $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K'}) \subseteq \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$, is a full and faithful contravariant functor (see also Remark 2.8).

We next address the problem of constructing a regular basis of $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ as a $\mathbf{Z}$-module (see Section 2 for the definition of regular basis). In particular, we discuss the value of the p-adic valuation of the leading term of the element of degree n in a regular basis, for each prime number p. We show that this is equivalent to understanding the analogous question for the ring

$$\mathrm{Int}_{\mathbf{Q}_p}(K) := \mathrm{Int}(\mathcal{O}_K) \cap \mathbf{Q}_p[X]$$

for each finite extension $K/\mathbf{Q}_p$, where $\mathrm{Int}(\mathcal{O}_K)$ is the ring of $f \in K[X]$ such that $f(\mathcal{O}_K) \subseteq \mathcal{O}_K$, and $\mathcal{O}_K$ is the valuation ring of K. We completely determine these values in Theorem 3.2, in the case of tame ramification. As a consequence, we obtain the second main result of this paper. To state the theorem, let $K/\mathbf{Q}$ be a Galois extension and, for any prime p of $\mathbf{Z}$, let q_p and e_p be the cardinality of the residue field of any prime ideal of $\mathcal{O}_K$ above p and the ramification index of p in $\mathcal{O}_K$, respectively. We also set

$$w_{q_p}(n) = \sum_{j\geq 1} \left\lfloor \frac{n}{q_p^j} \right\rfloor$$

and define for every integer $n \geq 1$,

$$\omega_p(n) = \omega_{K,p}(n) := \left\lfloor \frac{w_{q_p}(n)}{e_p} \right\rfloor.$$

Theorem 1.2. *Suppose that $K/\mathbf{Q}$ is a Galois extension which is tamely ramified at each prime. Let $\{f_n(X)\}_{n\geq 0}$ be a $\mathbf{Z}$-basis of $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ such that $\deg(f_n) = n$, for each $n \in \mathbf{N}$. Then we can write*

$$f_n(X) = \frac{g_n(X)}{\prod_p p^{\omega_p(n)}}$$

for some monic polynomial $g_n(X)$ in $\mathbf{Z}[X]$, where the product is over all primes p of $\mathbf{Z}$.

The proof of the above theorem is constructive: first, we construct a basis of $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_{K_{\mathfrak{p}}})$, for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above the rational prime p, from knowledge of a local basis of $\mathrm{Int}(\mathcal{O}_{K_{\mathfrak{p}}})$ (here and for the rest of the paper, $K_{\mathfrak{p}}$ denotes the $\mathfrak{p}$-adic completion of K); then, we use the Chinese Remainder Theorem to construct a global basis of $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$.

2. A characterization of Galois extensions

We introduce the following general notation, extending that of the introduction. Let D be an integral domain with quotient field K and let A be a torsion-free D-algebra. Let $B := A \otimes_D K$ be the extended K-algebra; we have canonical embeddings $A \hookrightarrow B$ and $K \hookrightarrow B$. For $a \in A$ and $f \in K[X]$, the value $f(a)$ belongs to B, and the following definition makes sense (see also [PW14]):

$$\mathrm{Int}_K(A) := \{f \in K[X] \mid f(a) \in A, \forall a \in A\}.$$

Clearly, $\mathrm{Int}_K(A)$ is a D-algebra. It is easy to see that $\mathrm{Int}_K(A)$ is contained in the classical ring of integer-valued polynomials $\mathrm{Int}(D) = \{f \in K[X] \mid f(D) \subseteq D\}$ if and only if $A \cap K = D$, and this will be the case henceforth.

A sequence of polynomials $\{f_n(X)\}_{n\in\mathbf{N}} \subset \mathrm{Int}_K(A)$ which forms a basis of $\mathrm{Int}_K(A)$ as a D-module and such that $\deg(f_n) = n$ for each $n \in \mathbf{N}$, is called a *regular basis* of $\mathrm{Int}_K(A)$. We define $\mathfrak{I}_n(\mathrm{Int}_K(A))$ to be the D-module generated by the leading coefficients of all the polynomials $f \in \mathrm{Int}_K(A)$ of degree exactly n; we call these D-modules *characteristic ideals*. For each $n \in \mathbf{N}$, by the above assumption and [CC97, Proposition II.1.1], $\mathfrak{I}_n(\mathrm{Int}_K(A))$ is a fractional ideal of D. Moreover, the set of characteristic ideals forms an ascending sequence:

$$D \subseteq \mathfrak{I}_0(\mathrm{Int}_K(A)) \subseteq \ldots \subseteq \mathfrak{I}_n(\mathrm{Int}_K(A)) \subseteq \mathfrak{I}_{n+1}(\mathrm{Int}_K(A)) \subseteq \ldots \subseteq K.$$

The link between regular bases and characteristic ideals is given by [CC97, Proposition II.1.4], which says that a sequence of polynomials $\{f_n(X)\}_{n\in\mathbf{N}}$ of $\mathrm{Int}_K(A)$ is a regular basis if and only if, for each $n \in \mathbf{N}$, $f_n(X)$ is a polynomial of degree n whose leading coefficient generates $\mathfrak{I}_n(\mathrm{Int}_K(A))$ as a D-module. In particular, note that $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ and $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$ (for $K/\mathbf{Q}$ and $K/\mathbf{Q}_p$ finite field extension) each admits a regular basis.

We fix from here to the end of this section a number field K and denote by $\mathcal{O}_K$ its ring of algebraic integers. For any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we denote $\mathcal{O}_{K,(\mathfrak{p})}$ the localization of $\mathcal{O}_K$ at $\mathfrak{p}$, *i.e.*, the localization at the multiplicative set $\mathcal{O}_K \setminus \mathfrak{p}$. Moreover, for any $\mathbf{Z}$-module M and any prime number p, we denote $M_{(p)}$ the localization at p, *i.e.*, the localization at the multiplicative set $\mathbf{Z} \setminus p\mathbf{Z}$. We also denote by $K_{\mathfrak{p}}$ the completion of K at $\mathfrak{p}$ and by $\mathcal{O}_{K,\mathfrak{p}}$ the valuation ring of $K_{\mathfrak{p}}$.

Proposition 2.1. *We have* $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K) = \bigcap_{\mathfrak{p}} \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})})$ *and*

$$\mathfrak{I}_n(\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)) = \bigcap_{\mathfrak{p}} \mathfrak{I}_n(\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})}))$$

for each $n \in \mathbf{N}$, *where the intersection is over all prime ideals of* $\mathcal{O}_K$.

Proof. We first observe that $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K) = \bigcap_p \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)_{(p)}$; here the intersection is over all primes of $\mathbf{Z}$. Then one observes that $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)_{(p)} = \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(p)})$ (see for example [Wer14]). We conclude that $\mathfrak{I}_n(\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)_{(p)})$ is equal to $\mathfrak{I}_n(\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(p)}))$, showing the second part. Further, $\mathcal{O}_{K,(p)} = \bigcap_{\mathfrak{p}|p} \mathcal{O}_{K,(\mathfrak{p})}$, where $\mathcal{O}_{K,(\mathfrak{p})}$ is the localization of $\mathcal{O}_K$ at $\mathfrak{p}$, and the intersection is over all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ which lie above p. Therefore

$$\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(p)}) = \bigcap_{\mathfrak{p}|p} \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})}) \tag{1}$$

and the result follows. $\square$

Remark 2.2. Note that, if $K/\mathbf{Q}$ is Galois, then $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})})$, for $\mathfrak{p} \mid p$, are all equal because $\mathrm{Gal}(K/\mathbf{Q})$ acts transitively on the set of rings $\{\mathcal{O}_{K,(\mathfrak{p})} : \mathfrak{p} \mid p\}$. Therefore (1) reads as

$$\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(p)}) = \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})})$$

for each $\mathfrak{p} \mid p$. A similar argument has been used in [Per16, Proposition 1.10].

In order to determine some relations of containments between the rings $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})})$, we introduce the following object: given an extension of commutative rings $R \subseteq S$, we consider the null ideal of S over R, that is, $N_R(S) = \{g \in R[X] \mid g(S) = 0\} \subseteq R[X]$ (for results connected to null ideals see for example [Per14a,PW16,Wer14]).

Proposition 2.3. *Let K be a number field and let $p \in \mathbf{Z}$ be a prime. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal above p with ramification index e and residue class degree f. Then*

$$N_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^e) = ((X^{p^f} - X)^e)$$

Proof. Since $\pi : \mathcal{O}_K/\mathfrak{p}^e \twoheadrightarrow \mathcal{O}_K/\mathfrak{p}^{e-1} \twoheadrightarrow \ldots \twoheadrightarrow \mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f}$ and $\mathbb{F}_p$ embeds in all of these rings (because $\mathfrak{p}^i \cap \mathbf{Z} = p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z}$, for all $i = 1, \ldots, e$) we have

$$\begin{tikzcd}
\mathcal{O}_K/\mathfrak{p}^e \arrow[r, two heads] & \mathcal{O}_K/\mathfrak{p}^{e-1} \arrow[r, two heads] & \ldots \arrow[r, two heads] & \mathcal{O}_K/\mathfrak{p} \\
 & & & \mathbb{F}_p \arrow[u, hook] \arrow[ulll, hook] \arrow[ull, hook]
\end{tikzcd}$$

so, in particular, we have the following chain of containments between these ideals of $\mathbb{F}_p[X]$:

$$N_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^e) \subseteq N_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^{e-1}) \subseteq \ldots \subseteq N_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}).$$

Since $\mathcal{O}_K/\mathfrak{p}$ is a finite field with p^f elements, the ideal $N_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$ is generated by the polynomial $X^{p^f} - X$. The proof proceeds by induction on e. Suppose that $N_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^{e-1})$

is generated by $(X^{p^f}-X)^{e-1}$. It is easy to see that $(X^{p^f}-X)^e$ is contained in $N_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^e)$. Therefore, the latter ideal is generated by a polynomial $g \in \mathbb{F}_p[X]$ which is zero on all the elements of $\mathcal{O}_K/\mathfrak{p}^e$ of the form

$$g(X) = (X^{p^f}-X)^{e-1}h(X) = F_q(X)^{e-1}\prod_{\gamma\in S}(X-\gamma)$$

for some $S \subseteq \mathbb{F}_{p^f} = \mathbb{F}_q$. Suppose that S is strictly contained in $\mathbb{F}_q$ and let $\overline{\gamma} \in \mathbb{F}_q \setminus S$. Without loss of generality, we may assume that $\overline{\gamma} = 0$ (apply the automorphism which takes $X \mapsto X-\gamma$, if necessary; this is an automorphism for $\mathbb{F}_{p^f}$ and $\mathcal{O}_K/\mathfrak{p}^e$).

Let $t \in P/P^e \subset \mathcal{O}_K/\mathfrak{p}^e$ be such that its index of nilpotency is e (that is, $t^e = 0$ but $t^{e-1} \neq 0$). Then $F_q(t)^{e-1} = t^{e-1}\cdot(t^{q-1}-1)^{e-1}$ is not zero in $O_K/\mathfrak{p}^e$, because $t^{q-1}-1$ is a unit of $O_K/\mathfrak{p}^e$ (because $\mathfrak{p}/\mathfrak{p}^e$ is the Jacobson radical of $O_K/\mathfrak{p}^e$).

In the same way, $h(t) = \prod_{\gamma\in S}(t-\gamma)$ is not in the kernel of $\pi : \mathcal{O}_K/\mathfrak{p}^e \twoheadrightarrow \mathcal{O}_K/\mathfrak{p}^{e-1}$, which is $\mathfrak{p}/\mathfrak{p}^e$, because modulo $\mathfrak{p}$, $h(t)$ is not zero ($\pi(h(t)) = h(\pi(t)) = h(0) \neq 0$, because $0 \notin S$). Hence, $h(t)$ is invertible, so that $g(t) = F_q(t)^{e-1}\cdot h(t)$ is not zero, contradiction. □

Proposition 2.4. *Let K, K' be number fields, with prime ideals $\mathfrak{p}, \mathfrak{p}'$ of residual characteristic p, p', respectively, and with ramification index and residue class degree equal to e, f and e', f', respectively. Suppose that*

$$\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K',(\mathfrak{p}')}) \subseteq \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})})$$

Then $\mathfrak{p}\cap\mathbf{Z} = p\mathbf{Z} = \mathfrak{p}'\cap\mathbf{Z}$, $f|f'$ and $e \le e'$. In particular, if the above containment is an equality, we have that $\mathfrak{p}\cap\mathbf{Z} = p\mathbf{Z} = \mathfrak{p}'\cap\mathbf{Z}$, $f = f'$ and $e = e'$.

Proof. Suppose that $\mathfrak{p}\cap\mathbf{Z} = p\mathbf{Z}$ and $\mathfrak{p}'\cap\mathbf{Z} = p'\mathbf{Z}$. Observe that

$$\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})})\cap\mathbf{Q} = (\mathrm{Int}(\mathcal{O}_{K,(\mathfrak{p})})\cap K)\cap\mathbf{Q} = \mathcal{O}_{K,(\mathfrak{p})}\cap\mathbf{Q} = \mathbf{Z}_{(p)}$$

and analogously for $\mathfrak{p}'$ and p'. Therefore

$$\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K',(\mathfrak{p}')})\cap\mathbf{Q} = \mathbf{Z}_{(p')} \subseteq \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})})\cap\mathbf{Q} = \mathbf{Z}_{(p)},$$

so that $p = p'$.

By Proposition 2.3, the containment of the hypothesis implies that

$$\frac{(X^{p^{f'}}-X)^{e'}}{p} \in \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})}). \tag{2}$$

In particular, modulo p, we have

$$(X^{p^{f'}}-X)^{e'} \in N_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^e) = ((X^{p^f}-X)^e),$$

again by Proposition 2.3. It follows that $(X^{p^{f'}}-X)^{e'} \in (X^{p^f}-X)$ and since the latter is a radical ideal (because $X^{p^f}-X$ is a separable polynomial), this means that $X^{p^{f'}}-X$ belongs to $(X^{p^f}-X)$ which is equivalent to $\mathbb{F}_{p^f} \subseteq \mathbb{F}_{p^{f'}}$ which holds if and only if $f|f'$, as claimed.

In the same way, since $X^{p^{f'}}-X$ is a separable polynomial (every irreducible factor appears with multiplicity 1 in the factorization of $X^{p^{f'}}-X$ over $\mathbb{F}_p$), we deduce that $e \leq e'$. □

We recall that, by a result of Gerboud (see [Ger93] and also [CC97, Prop. IV.3.3]) we have

$$\mathrm{Int}(\mathbf{Z}_{(p)}, \mathcal{O}_{K,(\mathfrak{p})}) = \{f \in K[X] \mid f(\mathbf{Z}_{(p)}) \subseteq \mathcal{O}_{K,(\mathfrak{p})}\} = \mathrm{Int}(\mathbf{Z}_{(p)}) \cdot \mathcal{O}_{K,(\mathfrak{p})} \tag{3}$$

Lemma 2.5. *Let K be a number field and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal which lies above a prime $p \in \mathbf{Z}$. Let $e = e(\mathfrak{p}|p)$ and $f = f(\mathfrak{p}|p)$ be the ramification index and residue class degree, respectively. Then the following conditions are equivalent:*

i) $\mathrm{Int}(\mathbf{Z}_{(p)}) \subseteq \mathrm{Int}(\mathcal{O}_{K,(\mathfrak{p})})$.
ii) $\mathrm{Int}(\mathbf{Z}_{(p)}, \mathcal{O}_{K,(\mathfrak{p})}) = \mathrm{Int}(\mathcal{O}_{K,(\mathfrak{p})})$
iii) $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})}) = \mathrm{Int}(\mathbf{Z}_{(p)})$.
iv) $e = f = 1$.

If any of this equivalent conditions holds, then

$$\mathrm{Int}(\mathbf{Z}_{(p)}) \cdot \mathcal{O}_{K,(\mathfrak{p})} = \mathrm{Int}(\mathcal{O}_{K,(\mathfrak{p})}).$$

Proof. Obviously, conditions i) and iii) are equivalent, since $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})})$ is always contained in $\mathrm{Int}(\mathbf{Z}_{(p)})$.

If i) holds, then by (3) above we have $\mathrm{Int}(\mathbf{Z}_{(p)}, \mathcal{O}_{K,(\mathfrak{p})}) \subseteq \mathrm{Int}(\mathcal{O}_{K,(\mathfrak{p})})$, which is condition ii), since we always have the containment $\mathrm{Int}(\mathbf{Z}_{(p)}, \mathcal{O}_{K,(\mathfrak{p})}) \supseteq \mathrm{Int}(\mathcal{O}_{K,(\mathfrak{p})})$. Conversely, if condition ii) holds, then again by (3) above we have $\mathrm{Int}(\mathbf{Z}_{(p)}) \subseteq \mathrm{Int}(\mathcal{O}_{K,(\mathfrak{p})})$.

The equivalence between iii) and iv) follows immediately from Proposition 2.4. □

Corollary 2.6. *Let K be a number field and let $p \in \mathbf{Z}$ be a prime. Then the following conditions are equivalent:*

i) $\mathrm{Int}(\mathbf{Z}_{(p)}) = \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(p)})$.
ii) *p is totally split in $\mathcal{O}_K$.*
iii) $\frac{X^p - X}{p} \in \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$.

Proof. The proof of the equivalence i)⇔ii) follows immediately from (1) and Lemma 2.5. Indeed, if p is totally split in $\mathcal{O}_K$ then, for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p, we have $\mathrm{Int}(\mathbf{Z}_{(p)}) = \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})})$, so that by (1) we have the equality $\mathrm{Int}(\mathbf{Z}_{(p)}) = \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(p)})$.

Conversely, if the last equality holds, then by (1), for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p, we have $\mathrm{Int}(\mathbf{Z}_{(p)}) \subseteq \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K,(\mathfrak{p})}) \subseteq \mathrm{Int}(\mathbf{Z}_{(p)})$, so equality holds throughout and p is totally split in $\mathcal{O}_K$.

We show now that ii)⇒iii). Suppose that p is totally split in $\mathcal{O}_K$, so that, by the Chinese Remainder Theorem we have

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p^n$$

where $n = [K : \mathbf{Q}]$. Hence, $X^p - X$ is zero on $\mathcal{O}_K/p\mathcal{O}_K$, so that $f(X) = \frac{X^p - X}{p}$ is in $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$. Conversely, suppose that $f(X)$ is in $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$. Then $X^p - X$ is zero on $\mathcal{O}_K/p\mathcal{O}_K \cong \prod_{i=1}^g \mathcal{O}_K/\mathfrak{p}_i^{e_i}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ are the prime ideals of O_K above p, with ramification index $e_i = e(\mathfrak{p}_i|p)$ and residue class degree $f_i = f(\mathfrak{p}_i|p)$. Consequently, $X^p - X$ is zero on each factor ring $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$, for $i = 1, \ldots, g$. Let $\overline{\alpha}$ be in the Jacobson ideal of $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$, that is, $\overline{\alpha}$ is in $\mathfrak{p}_i/\mathfrak{p}_i^{e_i}$ (the unique maximal ideal of $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$). Then $1 - \overline{\alpha}^{p-1}$ is a unit in $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$. But by assumption $\overline{\alpha}^p - \overline{\alpha} = \overline{\alpha}(\overline{\alpha}^{p-1} - 1) = 0$, so that $\overline{\alpha} = 0$. Therefore, $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ has trivial Jacobson ideal, which happens precisely when $e_i = 1$. If $f_i > 1$, then $\mathcal{O}_K/\mathfrak{p}_i$ is a proper finite field extension of $\mathbb{F}_p$, so if we take an element $\overline{\gamma}$ of $\mathcal{O}_K/\mathfrak{p}_i \setminus \mathbb{F}_p$, $\overline{\gamma}$ will be a zero of a monic irreducible polynomial $q(X)$ over $\mathbb{F}_p$ of degree strictly larger than 1. Since $X^p - X$ is zero on $\overline{\gamma}$, we would have that $q(X)$ divides $X^p - X$ over $\mathbb{F}_p$, which is clearly not possible because $X^p - X$ splits over $\mathbb{F}_p$. This shows that iii)⇒ii). □

The next result characterizes the finite Galois extensions of $\mathbf{Q}$ in terms of the rings $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$. In particular, we can recover $\mathcal{O}_K$ from $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$, if $K/\mathbf{Q}$ is Galois. Given a subring R of $\mathbf{Q}[X]$, for each $\alpha \in \overline{\mathbf{Z}}$ we consider the following subset of $\mathbf{Q}(\alpha)$:

$$R(\alpha) = \{f(\alpha) \mid f \in R\}$$

Theorem 2.7. *Let $K/\mathbf{Q}$ be a finite extension and let $R_K = \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$. Then*

$$K/\mathbf{Q} \text{ is a Galois extension} \iff \{\alpha \in \overline{\mathbf{Z}} \mid R_K(\alpha) \subset \overline{\mathbf{Z}}\} = \mathcal{O}_K.$$

In particular, if K and K' are two Galois extensions of $\mathbf{Q}$ such that $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ is equal to $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K'})$, then $K = K'$.

Note that the condition $R_K(\alpha) \subset \overline{\mathbf{Z}}$ is equivalent to $R_K(\alpha) \subseteq \mathcal{O}_{\mathbf{Q}(\alpha)}$.

Proof. The second statement about K and K' follows immediately from the first.

For the first statement, let $R_K = \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ and suppose that

$$\{\alpha \in \overline{\mathbf{Z}} \mid R_K(\alpha) \subset \overline{\mathbf{Z}}\} = \mathcal{O}_K.$$

It is easily seen that the left-hand side is invariant under the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Hence, $\mathcal{O}_K$ contains the ring of integers of all the conjugates of K over $\mathbf{Q}$, so $K/\mathbf{Q}$ is Galois.

Conversely, suppose that $K/\mathbf{Q}$ is a Galois extension. It is clear that we have the containment $\{\alpha \in \overline{\mathbf{Z}} \mid R_K(\alpha) \subset \overline{\mathbf{Z}}\} \supseteq \mathcal{O}_K$. Conversely, let $\alpha \in \overline{\mathbf{Z}}$, $\alpha \notin \mathcal{O}_K$. We have to show that there exists $f \in \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ such that $f(\alpha) \notin \overline{\mathbf{Z}}$. Let $K_\alpha = \mathbf{Q}(\alpha)$ and let N_α be the Galois closure of K_α over $\mathbf{Q}$ (the compositum inside $\overline{\mathbf{Q}}$ of all the conjugates over $\mathbf{Q}$ of K_α). We have that $\alpha \notin K \Leftrightarrow K_\alpha \not\subset K \Leftrightarrow N_\alpha \not\subset K$, where the last equivalence holds because by assumption $K/\mathbf{Q}$ is Galois.

By Tchebotarev's Density Theorem, a Galois extension K of $\mathbf{Q}$ is completely determined by the set of primes $S(K/\mathbf{Q})$ which are totally split in K (see [Neu99, Chapter VII, Corollary 13.10]). Hence, the condition $N_\alpha \not\subset K$ is equivalent to $S(K/\mathbf{Q}) \not\subset S(N_\alpha/\mathbf{Q})$, that is, the set of primes $p \in \mathbf{Z}$ which are totally split in K is not contained in the set of primes which are totally split in N_α. Let $p \in \mathbf{Z}$ be such a prime and suppose also that

- p is ramified neither in K nor in N_α.
- p does not divide $[\mathcal{O}_{K_\alpha} : \mathbf{Z}[\alpha]]$

The above primes are always finite in number and since the above set is infinite, by removing the latter primes we still get a non-empty set. By Corollary 2.6, $f(X) = \frac{X^p - X}{p}$ is in $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ but not in $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{N_\alpha})$. Recall that a prime $p \in \mathbf{Z}$ splits completely in the normal closure N_α of K_α (over $\mathbf{Q}$) if and only if it splits completely in K_α ([Mar77, Chap. 4, Corollary of Theorem 31]). Hence, there exists some prime ideal $\mathfrak{p}$ of $\mathcal{O}_{K_\alpha}$ above p which has inertia degree strictly greater than 1. Since p does not divide $[\mathcal{O}_{K_\alpha} : \mathbf{Z}[\alpha]]$, it follows by Dedekind-Kummer's Theorem (see [Neu99, Chapter I, Proposition 8.3]) that the factorization in $\mathbb{F}_p[X]$ of the residue modulo p of the minimal polynomial $p_\alpha(X)$ of α over $\mathbf{Z}$ has at least one irreducible polynomial over $\mathbb{F}_p$ whose degree is strictly greater than 1; this factor corresponds to a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{K_\alpha}$ above p which is not inert, that is $\mathcal{O}_{K_\alpha}/\mathfrak{p} \supsetneq \mathbb{F}_p$. In particular, this means that modulo $\mathfrak{p}$, α is not in $\mathbb{F}_p$, and so it is not annihilated by $\overline{g}(X) = X^p - X$ (equivalently, modulo $\mathfrak{p}$, α is a zero of an irreducible polynomial over $\mathbb{F}_p$ of degree strictly greater than 1). This implies that $f(\alpha)$ is not integral over $\mathbf{Z}$. □

Remark 2.8. We also offer a shorter proof of the second statement in Theorem 2.7 based on the following claim: let K, K' be two finite Galois extensions over $\mathbf{Q}$. Then

$$\mathcal{O}_K \subseteq \mathcal{O}_{K'} \Longleftrightarrow \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K'}) \subseteq \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$$

We prove the implication ($\Leftarrow$), the other being obvious (and it is true even without the Galois assumption). Suppose then that $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_{K'}) \subseteq \mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ and let $p \in \mathbf{Z}$ be a prime which is totally split in $\mathcal{O}_{K'}$. Then by Corollary 2.6 we have

$$\mathrm{Int}(\mathbf{Z}_{(p)}) = \mathrm{Int}_{\mathbf{Q}}(O_{K',(p)}) \subseteq \mathrm{Int}_{\mathbf{Q}}(O_{K,(p)}).$$

Since in any case $\mathrm{Int}_{\mathbf{Q}}(O_{K,(p)})$ is contained in $\mathrm{Int}(\mathbf{Z}_{(p)})$, the containment in the above equation is an equality, so that again by Corollary 2.6 we have that p is totally split in K, too. This shows that the set of primes $p \in \mathbf{Z}$ which are totally split in $\mathcal{O}_{K'}$ is contained in the set of primes which are totally split in $\mathcal{O}_K$. Therefore, by [Neu99, Chap. VII, Prop. 13.9] it follows that $K \subseteq K' \Leftrightarrow \mathcal{O}_K \subseteq \mathcal{O}_{K'}$.

Note that the above statement shows in particular that the functor $\mathrm{Int}_{\mathbf{Q}} : \mathcal{G} \to \mathcal{C}$ is full, as we claimed in the Introduction.

3. Characteristic ideals

Proposition 2.1 reduces the study of characteristic ideals of $\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)$ to the study of characteristic ideals in the local case. We will address a description of these ideals and apply the local results to the global context.

3.1. Local case

Fix a finite field extension $K/\mathbf{Q}_p$ having residue class degree f and ramification degree e. Denote by v_p the p-adic valuation of $\mathbf{Q}_p$, normalized such that $v_p(p) = 1$. Let:

$$w_p(n) := v_p(n!) = \sum_{j \geq 1} \left\lfloor \frac{n}{p^j} \right\rfloor$$

and, if $q = p^f$ is the cardinality of the residue field of K, put

$$w_q(n) := \sum_{j \geq 1} \left\lfloor \frac{n}{q^j} \right\rfloor .$$

The following equality follows from [CC97, Corollary II.2.9]:

$$-v_p\left(\mathfrak{I}_n\left(\mathrm{Int}(\mathbf{Z}_p)\right)\right) = w_p(n)$$

and, similarly, we have:

$$-v_\pi\left(\mathfrak{I}_n\left(\mathrm{Int}(\mathcal{O}_K)\right)\right) = w_q(n) \tag{4}$$

where π is a uniformizer of K and v_π the associated valuation.

We define finally

$$w_{\mathcal{O}_K}^{\mathbf{Q}_p}(n) := -v_p\left(\mathfrak{I}_n\left(\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)\right)\right).$$

The following equality holds because of the next lemma, noticing that $\lceil -\frac{n}{e} \rceil = -\lfloor \frac{n}{e} \rfloor$:

$$\mathfrak{I}_n(\mathrm{Int}(\mathcal{O}_K)) \cap \mathbf{Q}_p = p^{-\lfloor \frac{w_q(n)}{e} \rfloor} \mathbf{Z}_p$$

and since $\mathfrak{I}_n(\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)) \subseteq \mathfrak{I}_n(\mathrm{Int}(\mathcal{O}_K)) \cap \mathbf{Q}_p$, for every $n \in \mathbf{N}$ we have:

$$w_{\mathcal{O}_K}^{\mathbf{Q}_p}(n) \leq \left\lfloor \frac{w_q(n)}{e} \right\rfloor. \tag{5}$$

Lemma 3.1. *Let $n \in \mathbf{Z}$ and $e = e(\mathfrak{p}|p)$, where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_K$. Then*

$$\mathfrak{p}^n \cap \mathbf{Q}_p = p^{\lceil \frac{n}{e} \rceil}\mathbf{Z}_p.$$

Proof. ($\supseteq$). Clearly, $p^{\lceil \frac{n}{e} \rceil} \in \mathfrak{p}^n \Leftrightarrow v_{\mathfrak{p}}(p^{\lceil \frac{n}{e} \rceil}) = e \cdot \lceil \frac{n}{e} \rceil \geq n$, which is true, so the containment follows, since clearly $\mathfrak{p}^n \cap \mathbf{Q}_p$ is a $\mathbf{Z}_p$-module.

($\subseteq$). Let $\alpha \in \mathfrak{p}^n \cap \mathbf{Q}_p$, say $\alpha = p^m u$, where $u \in \mathbf{Z}_p^*$ and $m = v_p(\alpha)$. Then $v_{\mathfrak{p}}(\alpha) = me$ which has to be greater than or equal to n. Therefore, $m \geq \lceil \frac{n}{e} \rceil$, so $\alpha \in p^{\lceil \frac{n}{e} \rceil}\mathbf{Z}_p$. $\square$

The main result of this section shows the opposite inequality in (5) in the case of tame ramification for a finite Galois extension. By the above remarks, this corresponds to say that $\mathfrak{I}_n(\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)) = \mathfrak{I}_n(\mathrm{Int}(\mathcal{O}_K)) \cap \mathbf{Q}_p$, for each $n \in \mathbf{N}$. We show in Example 3.6 that these two conditions, namely, Galois and tame ramification, cannot be relaxed.

Theorem 3.2. *Let $K/\mathbf{Q}_p$ be a finite tamely ramified Galois extension, with ramification index e and residue field of cardinality q. Then for all $n \in \mathbf{N}$ we have*

$$w_{\mathcal{O}_K}^{\mathbf{Q}_p}(n) = \left\lfloor \frac{w_q(n)}{e} \right\rfloor.$$

In particular, $w_{\mathcal{O}_K}^{\mathbf{Q}_p}(n)$ only depends on n, q and e.

Proof. By (5) it is sufficient to show that $d = p^{-\lfloor \frac{w_q(n)}{e} \rfloor}$ is in $\mathfrak{I}_n(\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K))$.

We observe that if $f(X) = \sum_{i=0}^{n} a_i X^i$ belongs to $\mathrm{Int}(\mathcal{O}_K)$, then

$$f^\sigma(X) := \sum_{i=0}^{n} \sigma(a_i) X^i$$

belongs to $\mathrm{Int}(\mathcal{O}_K)$ for all $\sigma \in G = \mathrm{Gal}(K/\mathbf{Q}_p)$ (here we use crucially the assumption that $K/\mathbf{Q}_p$ is Galois). As a consequence, if we denote $\mathrm{tr} = \mathrm{tr}_{K/\mathbf{Q}_p} : K \to \mathbf{Q}_p$ the trace homomorphism, we see that

$$\mathrm{Tr}(f)(X) := \sum_{\sigma \in G} f^\sigma(X) = \sum_{i=0}^{n} \mathrm{tr}(a_i) X^i$$

belongs to $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$, if $f \in \mathrm{Int}(\mathcal{O}_K)$. Therefore, the trace homomorphism between the function fields $\mathrm{Tr} : K(X) \to \mathbf{Q}_p(X)$ restricts to $\mathrm{Tr} : \mathrm{Int}(\mathcal{O}_K) \to \mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$.

Since $p \nmid e$, the trace homomorphism tr is surjective (the converse is also true, see [Nar04, Chapter 5, Corollary, p. 227]). Fix $\alpha \in \mathcal{O}_K$ such that $\mathrm{tr}(\alpha) = 1$ and consider the element $c = d\alpha \in K$. In particular, since the trace is a $\mathbf{Q}_p$-homomorphism, we have $\mathrm{tr}(c) = d$. Note that the v_π-value of c is greater than or equal to $-e\lfloor \frac{w_q(n)}{e} \rfloor \geq -w_q(n)$. By (4), c is in $\mathfrak{I}_n(\mathrm{Int}(\mathcal{O}_K))$, so there exists $f \in \mathrm{Int}(\mathcal{O}_K)$ of degree n whose leading coefficient is equal to c. Therefore, $\mathrm{Tr}(f)$ is a polynomial of degree n in $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$ with leading coefficient equal to d, as we wanted to show. □

Remark 3.3. We remark that, from the fact that $\mathrm{tr} = \mathrm{tr}_{K/\mathbf{Q}_p} : \mathcal{O}_K \to \mathbf{Z}_p$ is surjective (because the extension is tame), the proof of Theorem 3.2 also shows that the restriction of the trace homomorphism $\mathrm{Tr} : \mathrm{Int}(\mathcal{O}_K) \to \mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$ is surjective. In fact, for each $n \in \mathbf{N}$, the n-th element of a regular basis of $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$, whose leading coefficient has p-adic value $-\left\lfloor \frac{w_q(n)}{e} \right\rfloor$ by the above theorem, is the image via the trace homomorphism of a polynomial of $\mathrm{Int}(\mathcal{O}_K)$.

Obviously, if Tr is surjective, it is easily seen that tr is surjective, because $\mathbf{Z}_p$ is contained in $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$. Finally, we have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Int}(\mathcal{O}_K) & \xrightarrow{\mathrm{Tr}} & \mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K) \\ \uparrow & & \uparrow \\ \mathcal{O}_K & \xrightarrow{\mathrm{tr}} & \mathbf{Z}_p \end{array}$$

The next corollary shows that Theorem 2.7 is false in the local case.

Corollary 3.4. *Let K_1, K_2 be two finite tamely ramified Galois extensions of $\mathbf{Q}_p$. Then $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_{K_1}) = \mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_{K_2})$ if and only if K_1 and K_2 have the same ramification index and residue field degree.*

Proof. Suppose that K_1 and K_2 have the same ramification index and residue field degree. In particular, the functions $w_{\mathcal{O}_{K_i}}^{\mathbf{Q}_p}(n)$, for $i = 1, 2$, are the same, by Theorem 3.2. Hence, by definition, the set of characteristic ideals of the rings $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_{K_i})$, $i = 1, 2$, coincide, so these rings have a common regular bases, and therefore they are equal.

Conversely, if the $\mathrm{Int}_{\mathbf{Q}_p}$-rings are equal, a straightforward adaptation of Proposition 2.4 to the present setting shows that the ramification indexes and residue field degrees of K_1 and K_2 are the same. Note that this part of the proof holds also without the tameness assumption. □

Remark 3.5. In the case $K/\mathbf{Q}_p$ is a finite unramified extension (so, in particular, a Galois extension), we can given an explicit basis of $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$. Let $q = p^f$ be the cardinality of the residue field of $\mathcal{O}_K$. By Theorem 3.2, for all $n \in \mathbf{N}$ we have $w_{\mathcal{O}_K}^{\mathbf{Q}_p}(n) = w_q(n)$. Let

$$f(X) := \frac{X^q - X}{p}$$

which clearly belongs to $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$. For $k \in \mathbf{N}$, we denote by $f^{\circ k}(X)$ the composition of f with itself k times, namely $f^{\circ k}(X) = f \circ \ldots \circ f(X)$. If $k = 0$ we put $f^0(X) := X$. For each positive integer $n \in \mathbf{N}$, we consider its q-adic expansion:

$$n = n_0 + n_1 q + \ldots + n_r q^r$$

where $n_i \in \{0, \ldots, q-1\}$ for all $i = 0, \ldots, r$. We define

$$f_n(X) := \prod_{i=0}^{r} (f^{\circ i}(X))^{n_i}$$

Notice that $f_n(X) = X^n$ for $n = 0, \ldots, q-1$ and $f_q(X) = f(X)$. Moreover, f_n belongs to $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$ and has degree n, for every $n \in \mathbf{N}$. It is easy to prove by induction that $\mathrm{lc}(f^{\circ i}) = p^{-a_i}$, where $a_i = 1 + q + \ldots + q^{i-1} = w_q(q^i!)$. By the same proof of [CC97, Chap. 2, Prop. II.2.12] one can show that $\mathrm{lc}(f_n) = p^{-w_q(n)}$ for every $n \in \mathbf{N}$, so, finally, the family of polynomials $\{f_n(X)\}_{n\in\mathbf{N}}$ is a regular basis of $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$.

Example 3.6. In the next two examples we show the assumptions in Theorem 3.2 cannot be dropped.

(1) If $K/\mathbf{Q}_p$ is not a Galois extension, then the restriction of the trace homomorphism to $\mathrm{Int}(\mathcal{O}_K)$ may give a polynomial in $\mathbf{Q}_p(X)$ which is not in $\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)$. For example, let $K = \mathbf{Q}_2(\sqrt[3]{2})$, whose ring of integers is $\mathcal{O}_K = \mathbf{Z}_2[\sqrt[3]{2}]$. Then the polynomial

$$f(X) = \frac{X(X-1)(X-\sqrt[3]{2})(X-(1+\sqrt[3]{2}))}{2}$$

is in $\mathrm{Int}(\mathcal{O}_K)$ but its trace over $\mathbf{Q}_2(X)$ is equal to $g(X) = \frac{3X^2(X-1)^2}{2}$, which is not integer-valued over $\mathcal{O}_K$, since $g(\sqrt[3]{2}) \notin \mathcal{O}_K$. One can show by an explicit computation that in this example the equality $w_{\mathcal{O}_K}^{\mathbf{Q}_p}(n) = \left\lfloor \frac{w_q(n)}{e} \right\rfloor$ does not hold for $n = 4$. Indeed, the first four elements of a $\mathcal{O}_K$-basis of $\mathrm{Int}(\mathcal{O}_K)$ are

$$f_1(X) = X; \quad f_2(X) = \frac{X(X-1)}{\sqrt[3]{2}}; \quad f_3(X) = \frac{X(X-1)(X-\sqrt[3]{2})}{\sqrt[3]{2}};$$
$$f_4(X) = \frac{X(X-1)(X-\sqrt[3]{2})(X-(1+\sqrt[3]{2}))}{2};$$

and considering all possible $\mathcal{O}_K$-combinations of these elements which lie in $\mathbf{Q}_2[X]$ (recall that $\mathrm{Int}_{\mathbf{Q}_2}(\mathcal{O}_K) = \mathbf{Q}_2[X] \cap \mathrm{Int}(\mathcal{O}_K)$), we see that there is no element in $\mathrm{Int}_{\mathbf{Q}_2}(\mathcal{O}_K)$ of degree 4 whose leading coefficient has valuation $-1 = -\left\lfloor \frac{w_2(4)}{3} \right\rfloor$.

(2) We now discuss the tameness assumption. Consider the case of $K = \mathbf{Q}_2(i)$ with $i^2 = -1$ and let $\{f_n(X) : n \geq 0\}$ be a regular basis of $\mathrm{Int}(\mathcal{O}_K)$ obtained by means of compositions and products of the Fermat polynomial $\frac{X^2-X}{1+i}$ (in the same way as in the Remark 3.5; see [CC97, Chapter II, p. 32]). We set $G(X) = X^2 - X$. One can check that

$$f_6 + if_4 = -\frac{G^3}{4} + \frac{G^2}{2} - \frac{G}{2}$$

and

$$f_{10} + 2f_8 - 2if_6 + (1-2i)f_4 = \frac{G^5}{16} + \frac{G^3}{8} - \frac{G^2}{4} + G$$

belong to $\mathrm{Int}_{\mathbf{Q}_2}(\mathcal{O}_K)$ and their leading coefficients have valuation equal, respectively, to $-\left\lfloor \frac{w_2(6)}{2} \right\rfloor = -2$ and $-\left\lfloor \frac{w_2(10)}{2} \right\rfloor = -4$; one can also check that

$$-v_2\left(\mathfrak{I}_n\left(\mathrm{Int}_{\mathbf{Q}_2}(\mathcal{O}_K)\right)\right) = \left\lfloor \frac{w_2(n)}{2} \right\rfloor$$

for all $n \leq 11$. On the other hand, writing down a basis of $\mathrm{Int}(\mathcal{O}_K)$ up to degree 12, and considering all possible $\mathcal{O}_K$-combinations of these elements which lie in $\mathbf{Q}_2[X]$, we see that

$$-v_2\left(\mathfrak{I}_{12}\left(\mathrm{Int}_{\mathbf{Q}_2}(\mathcal{O}_K)\right)\right) = \left\lfloor \frac{w_2(12)}{2} \right\rfloor - 1.$$

It might be interesting to describe the values taken by $v_p\left(\mathfrak{I}_n\left(\mathrm{Int}_{\mathbf{Q}_p}(\mathcal{O}_K)\right)\right)$ in the case of wild ramification.

3.2. Global case

Let $K/\mathbf{Q}$ be a finite Galois extension with absolute discriminant D and degree d over $\mathbf{Q}$. For each rational prime p, denote by f_p the residue class degree and e_p its ramification degree in O_K. As usual, we say that $K/\mathbf{Q}$ is tamely ramified if, for every prime $p \in \mathbf{Z}$, $p \nmid e_p$. Let $q_p = p^{f_p}$ be the cardinality of the residue field of K_p. The following is a reformulation of Theorem 1.2 in the Introduction:

Theorem 3.7. *Let $K/\mathbf{Q}$ be a tamely ramified Galois extension. Then*

$$\mathfrak{I}_n(\mathrm{Int}_{\mathbf{Q}}(\mathcal{O}_K)) = \left(\prod_p p^{-\left\lfloor \frac{w_{q_p}(n)}{e_p} \right\rfloor}\right)$$

as fractional ideals of $\mathbf{Z}$, where the product is over the set of all primes $p \in \mathbf{Z}$.

Proof. Note that for a fixed n we have $w_q(n) = 0$ for almost all prime powers q, and therefore the above product is well defined. The result follows immediately combining Proposition 2.1 and Theorem 3.2. □

Acknowledgments

The authors wish to thank the referee for carefully reading the paper.

The first author is partially supported by PRAT 2013 "Arithmetic of Varieties over Number Fields". The second author is partially supported by PRIN 2010/11 "Arithmetic Algebraic Geometry and Number Theory" and PRAT 2013 "Arithmetic of Varieties over Number Fields". The third author has been supported by grant "Bando Giovani Studiosi 2013", Project title "Integer-valued polynomials over algebras" Prot. GRIC13X60S of the University of Padova.

References

[CC97] P.-J. Cahen, J.-L. Chabert, Integer-Valued Polynomials, Math. Surveys Monogr., vol. 48, American Mathematical Society, Providence, RI, 1997.

[CP16] J.-L. Chabert, G. Peruginelli, Polynomial overrings of Int($\mathbf{Z}$), J. Commut. Algebra 8 (1) (2016) 1–28.

[Ger93] G. Gerboud, Substituabilité d'un anneau de Dedekind, C. R. Acad. Sci. Paris Sér. I Math. 317 (1) (1993) 29–32.

[LW12] K.A. Loper, N.J. Werner, Generalized rings of integer-valued polynomials, J. Number Theory 132 (11) (2012) 2481–2490.

[Mar77] D.A. Marcus, Number Fields, Universitext, Springer-Verlag, New York–Heidelberg, 1977.

[Nar04] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, third ed., Springer Monogr. Math., Springer-Verlag, Berlin, 2004.

[Neu99] J. Neukirch, Algebraic Number Theory, Grundlehren Math. Wiss., vol. 322, Springer-Verlag, Berlin, 1999.

[Per14a] G. Peruginelli, Integer-valued polynomials over matrices and divided differences, Monatsh. Math. 173 (4) (2014) 559–571.

[Per14b] G. Peruginelli, Integral-valued polynomials over sets of algebraic integers of bounded degree, J. Number Theory 137 (2014) 241–255.

[Per16] G. Peruginelli, The ring of polynomials integral-valued over a finite set of integral elements, J. Commut. Algebra 8 (1) (2016) 113–141.

[PW14] G. Peruginelli, Nicholas J. Werner, Integral closure of rings of integer-valued polynomials on algebras, in: Commutative Algebra, Springer, New York, 2014, pp. 293–305.

[PW16] G. Peruginelli, Nicholas J. Werner, Properly integral polynomials over the ring of integer-valued polynomials on a matrix ring, J. Algebra 460 (2016) 320–339.

[Wer14] N.J. Werner, Int-decomposable algebras, J. Pure Appl. Algebra 218 (10) (2014) 1806–1819.