P-ADIC APPROXIMATION OF ALGEBRAIC INTEGERS AND RESIDUE CLASS RINGS OF RINGS OF INTEGER-VALUED POLYNOMIALS

SOPHIE FRISCH AND FRANZ HALTER-KOCH

Abstract. Let $F\colon K$ be a Galois extension of number fields and Q a prime ideal of $\mathcal{O}_F$ lying over the prime P of $\mathcal{O}_K$. By analyzing the Q-adic closure of $\mathcal{O}_K$ in $\mathcal{O}_F$ we characterize those rings of integers $\mathcal{O}_K$ for which every residue class ring of $\mathrm{Int}(\mathcal{O}_K)$ modulo a non-zero prime ideal is GE_2 (meaning that every unimodular pair can be transformed to $(1,0)$ by a series of elementary transformations).

1. P-adic approximation of algebraic integers

For an algebraic number field K, let $\mathcal{O}_K$ be its ring of integers and $\mathbb{P}_K$ the set of all maximal ideals of $\mathcal{O}_K$. For $P \in \mathbb{P}_K$ we denote by K_P the P-adic completion of K and by $\widehat{O}_P$ its valuation domain.

Let L/K be a finite extension of algebraic number fields, and $P \in \mathbb{P}_K$ and $Q \in \mathbb{P}_L$ such that $Q \supset P$, and suppose that $K_P \subset L_Q$. The greatest intermediate field Z of L/K satisfying $Z_{Q\cap Z} = K_P$ is called the **decomposition field** of Q over K.

If L/K is a Galois extension and $G = \mathrm{Gal}(L/K)$ then the decomposition field Z of Q over K is the fixed field of the decomposition group $G_Q = \{\sigma \in G \mid \sigma Q = Q\}$, the local extension L_Q/K_P is Galois, and the restriction $\tau \mapsto \tau \restriction L$ defines an isomorphism $\mathrm{Gal}(L_Q/K_P) \xrightarrow{\sim} G_Q$ (see [7, §6.1.**3**] or [4, Def. 2.5.3]). We identify: $G_Q = \mathrm{Gal}(L_Q/K_P) \subset G$.

In general, the existence of the decomposition field is provided by the following simple lemma.

Lemma 1.1. *Let L/K be a finite extension of algebraic number fields, $P \in \mathbb{P}_K$ and $Q \in \mathbb{P}_L$ such that $Q \supset P$, and suppose that $K_P \subset L_Q$. Then $K_P \cap L$ is the decomposition field of Q over K.*

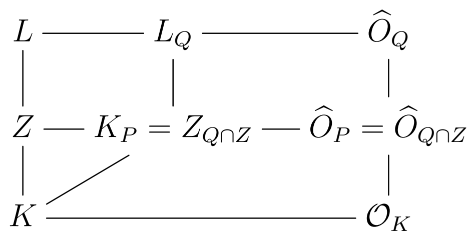
Proof. If M is an intermediate field of L/K such that $M_{Q\cap M} = K_P$, then clearly $M \subset L \cap K_P$, and it suffices to prove that $(L\cap K_P)_{Q\cap(L\cap K_P)} = K_P$. But $K \subset L\cap K_P \subset K_P$, and if we build the topological closure (in the Q-adic topology), we obtain that $K_P \subset (L\cap K_P)_{Q\cap L\cap K_P} \subset K_P$, and thus equality holds. □

Theorem 1.2. *Let L/K be a finite extension of algebraic number fields, $P \in \mathbb{P}_K$, $Q \in \mathbb{P}_L$ such that $Q \supset P$, and let Z be the decomposition field of Q over K.*

Let $Q_Z = Q \cap \mathcal{O}_Z$. Then $\mathcal{O}_{Z,Q_Z}$ is the Q-adic closure of $\mathcal{O}_K$ in L.

S. Frisch is supported by the Austrian Science Fund (FWF): P35788.

Proof. Let $\overline{\mathcal{O}_K}$ be the Q-adic closure of $\mathcal{O}_K$ in $\mathcal{O}_L$. By definition, $\overline{\mathcal{O}_K} = \widehat{O}_P \cap L$, and thus we obtain:



$$\overline{\mathcal{O}_K} = \widehat{O}_P \cap L = (K_P \cap \widehat{O}_Q) \cap L = (K_P \cap L) \cap (\widehat{O}_Q \cap L) = Z \cap \mathcal{O}_{L,Q} = \mathcal{O}_{Z,Q_Z}. \qquad \square$$

Corollary 1.3. *Let L/K be a finite Galois extension of algebraic number fields, $P \in \mathbb{P}_K$ and $Q \in \mathbb{P}_L$ such that $Q \supset P$,*

1. *$\mathcal{O}_K$ is dense in $\mathcal{O}_L$ in the Q-adic topology if and only if P splits completely in L.*
2. *$\mathcal{O}_K$ is relatively closed in $\mathcal{O}_L$ in the Q-adic topology if and only if Q is the only maximal ideal of $\mathcal{O}_L$ lying above P.*

Proof. Let Z be the decomposition field of Q over K. Then $r = [Z:K]$ is the number of prime ideals of $\mathcal{O}_L$ lying above P and $\mathcal{O}_Z$ is the Q-adic closure of $\mathcal{O}_K$ in $\mathcal{O}_L$. Consequently,

$$\mathcal{O}_K \text{ is dense in } \mathcal{O}_L \iff \mathcal{O}_Z = \mathcal{O}_L \iff Z = L \iff r = [L:K].$$

$$\mathcal{O}_K \text{ is closed in } \mathcal{O}_L \iff \mathcal{O}_Z = \mathcal{O}_K \iff Z = K \iff r = 1. \qquad \square$$

Theorem 1.4. *Let L/K be a finite extension of algebraic number fields, and let $\mathcal{O}_K^{\#}$ be the intersection of all Q-adic closures of $\mathcal{O}_K$ in L. Then $\mathcal{O}_K^{\#} = \mathcal{O}_K$.*

Proof. Let K' be the intersection of all decomposition fields of Q, where Q ranges through $\mathbb{P}_L$. By Theorem 1.2, $\mathcal{O}_K^{\#} \subseteq K'$. We show that $K' = K$.

Assume first that L/K is Galois and let $G = \mathrm{Gal}(L/K)$. If $P \in \mathbb{P}_K$ is unramified in L and $Q \in \mathbb{P}_L$ such that $Q \supset P$, then $G_Q = \langle F_Q \rangle$ is a cyclic group generated by the Frobenius automorphism F_Q of Q over K. Therefore the fixed field $L^{\langle F_Q \rangle}$ is the decomposition field of Q over K.

For $\sigma \in G$ we denote by $\mathcal{P}(L/K, \sigma)$ the set of all $P \in \mathbb{P}_K$ such that $F_Q = \sigma$ for some $Q \in \mathbb{P}_L$ lying above P. By Chebotarev's density theorem (see [7, Theorem 7.30], [4, Theorem 4.4.6], or [5, Theorem 7.9.2]), the set $\mathcal{P}(L/K, \sigma)$ has positive Dirichlet density. Therefore $\{L^{\langle \sigma \rangle} \mid \sigma \in G\}$ is a subset of the set of all decomposition fields, and hence

$$K \subseteq K' \subseteq \bigcap_{\sigma \in G} L^{\langle \sigma \rangle} = K,$$

which implies $K' = K$.

Now consider any $P \in \mathbb{P}_K$ and some $Q \in \mathbb{P}_L$ lying above P. Let Z be the decomposition field of Q and $Q_Z = Q \cap \mathcal{O}_Z$. Then

$$\mathcal{O}_K^{\#} \subseteq K \cap \mathcal{O}_{Z,Q_Z} = \mathcal{O}_{K,P}.$$

Hence,

$$\mathcal{O}_K \subseteq \mathcal{O}_K^{\#} \subseteq \bigcap_{P \in \mathbb{P}_K} \mathcal{O}_{K,P} = \mathcal{O}_K,$$

so that $\mathcal{O}_K^{\#} = \mathcal{O}_K$.

If L/K is an arbitrary finite extension, let L^*/K be a finite Galois extension such that $L \subset L^*$.

If $P \in \mathbb{P}_K$, $Q \in \mathbb{P}_L$ and $Q^* \in \mathbb{P}_{L^*}$ are such that $P \subset Q \subset Q^*$, let C_Q be the Q-adic closure of $\mathcal{O}_K$ in L and C_{Q^*} the Q^*-adic closure of $\mathcal{O}_K$ in L^*. Then $C_Q = C_{Q^*} \cap L$. Hence, as the intersection of all Q^*-adic closures already equals $\mathcal{O}_K$, all the more this holds for the intersection of all Q-adic closures. □

2. An application to integer-valued polynomials

For an integral domain D with quotient field D, the "ring of integer-valued polynomials over D" consists of the polynomials with coefficients in K that map elements of D (when substituted for the variable) to elements of D:

$$\mathrm{Int}(D) = \{f \in K[x] \mid f(D) \subseteq D\}.$$

P-adic closure turns out to be useful for describing the image of an element of a number field under the ring of integer-valued polynomials of the ring of algebraic integers in a subfield. (A different description of the same image has been given by McQuillan [6]).

Before showing this, we recall in gory detail, by request of the referee, a standard argument for evaluating $v(f(c))$ when c is an element of a discrete valuation ring D and f a product of monic linear factors in $D[x]$:

Remark 2.1. Consider Legendre's formula for the exponent of a prime p in the prime factorization of $n!$:

$$v_p(1 \cdot 2 \cdot \ldots \cdot n) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

A priori, $v_p(1 \cdot 2 \cdot \ldots \cdot n) = \sum_{j=1}^{n} v_p(j)$, but alternatively we can add up, for $k \geq 1$, the number of those j in $\{1, \ldots, n\}$ that are divisible by p^k, because in that way every j with $v_p(j) = m$ is counted exactly m times.

By the same token, for elements $c, a_1, \ldots, a_n$ in a discrete valuation ring with maximal ideal M, valuation v, and valuation group $e\mathbb{Z}$, $e > 0$,

$$v(\prod_{j=1}^{n}(c - a_j)) = \sum_{j=1}^{n} v(c - a_j) = e \sum_{k \geq 1} \left|\{1 \leq j \leq n \mid a_j \in c + M^k\}\right|.$$

Proposition 2.2. *Let D be a Dedekind domain with finite residue fields, and K its quotient field.*

Let c algebraic over K, $F = K[c]$ and E the integral closure of D in F.

Then, for any maximal ideal Q of E, the image of c under $\mathrm{Int}(D)$ *is contained in E_Q if and only if c is in the Q-adic closure of D in F.*

Proof. Let $P = Q \cap D$, and $PE = Q^e Q_1^{e_1} \ldots Q_{r-1}^{e_{r-1}}$ the prime factorization of P in E. Let v_Q the valuation on F associated to Q, normalized so that its value group is $\mathbb{Z}$, and, consequently, $e\mathbb{Z}$ the value group of its restriction to K, which we write as v_P.

Suppose c is in the Q-adic closure of D in F, and $f \in \mathrm{Int}(D)$. Write $f = g/d$ with $g \in D[x]$ and $d \in D$. Let $m = v_Q(d)$ and let $c' \in D$ such that $v_Q(c - c') \geq m$. Since $v_Q(g(c')) \geq m$ and $g(c') \equiv g(c)$ modulo Q^m, we see $v_Q(g(c)) \geq m$ and hence $f(c) \in E_Q$.

Conversely, suppose that c is not in the Q-adic closure of D in F. Let $m \in \mathbb{N}$ such that $(c + Q^{em}) \cap D = \emptyset$. Let $[D\colon P] = p$ and $a_1, \ldots, a_{p^m}$ a complete system of residues of D modulo P^m. Let $\beta = (1 - p^m)/(1 - p)$, and $d \in K$ such that $v_P(d) = -e\beta$ and $v(d) \geq 0$ for all other essential valuations of D.

Set $g(x) = \prod_{j=1}^{p^m}(x - a_j)$, and $f = dg$. Then, by Remark 2.1, $\min_{r \in D} v_P(g(r)) = e(1 + p + \ldots + p^{(m-1)}) = e\beta$, the minimum being attained by those r with $v_P(r - a_j) = m$ for the unique j such that $r \equiv a_j$ modulo P^m. Also, $f \in D_{P'}[x]$ for all maximal ideals $P' \neq P$ of D, whence $f \in \mathrm{Int}(D)$.

At the same time, $f(c) \notin E_Q$ since $v_Q(g(c)) < e\beta$: To see this, calculate $v_Q(g(c))$ according to Remark 2.1: If $c \notin E_Q$ then already $v_Q(g(c)) < 0$. So, assume $c \in E_Q$. then $v_Q(g(c)) = \sum_{k \geq 1} n_k(c)$, where

$$n_k(c) = |\{1 \leq j \leq p^m \mid v_Q(c - a_j) \geq k\}| = \left|\{1 \leq j \leq p^m \mid a_j \in c + Q^k\}\right|.$$

Now, the intersection of a residue class of Q^k in E with D is either empty or a residue class of $P^{\lceil \frac{k}{e} \rceil}$ in D, and $(c + Q^k) \cap D$ is empty for all $k \geq em$ by assumption.

For $1 \leq s \leq m$, each residue class of P^s is represented among the a_j exactly p^{m-s} times, so that

$$v_Q(g(c)) = \sum_{k=1}^{em-1} n_k(c) = \sum_{s=1}^{m-1} \sum_{r=1}^{e} n_{(s-1)e+r}(c) + \sum_{r=1}^{e-1} n_{(m-1)e+r}(c)$$

implies

$$v_Q(g(c)) \leq \sum_{s=1}^{m-1} \sum_{r=1}^{e} p^{m-s} + \sum_{r=1}^{e-1} 1 = \sum_{s=1}^{m-1} ep^{m-s} + e - 1 = e\beta - 1$$

□

Corollary 2.3. *Let $D = \mathcal{O}_K$ be the ring of integers in a number field K, c algebraic over K, $F = K[c]$, and $E = \mathcal{O}_F$ the integral closure of D in F.*

Then the image of c under $\mathrm{Int}(D)$ *is*

$$\mathrm{Int}(D)[c] = \bigcap_{Q \in \mathcal{P}(c)} E_Q,$$

where $\mathcal{P}(c)$ is the set of those $Q \in \mathrm{Spec}(E)$ such that c is in the Q-adic closure of D.

Proof. Clearly, $D[c] \subseteq \mathrm{Int}(D)[c] \subseteq K[c] = F$. Since $\mathrm{Int}(D)$ is Prüfer, so is $\mathrm{Int}(D)[c]$, as a homomorphic image of a Prüfer domain. In particular, $\mathrm{Int}(D)[c]$ is integrally closed in its quotient field F, and, therefore, contains E. As an overring of the Dedekind ring E, $\mathrm{Int}(D)[c]$ is necessarily an intersection of localizations of E at maximal ideals, and, therefore, equal to the intersection of all E_Q containing it. Proposition 2.2 tells us which ones these are. □

Corollary 2.4. *Let $D = \mathcal{O}_K$ be the ring of integers in a number field K, F a finite extension of K, and $E = \mathcal{O}_F$ the integral closure of D in F. Let $c \in F$.*

Then $\mathrm{Int}(D)[c]$*, the image of* c *under* $\mathrm{Int}(D)$*, is*

$$\mathrm{Int}(D)[c] = \begin{cases} D & \text{if} \quad c \in D \\ \text{a strict overring of } D & \text{if} \quad c \in K \setminus D \\ \text{a strict overring of } E & \text{if} \quad c \in F \setminus K \end{cases}$$

Proof. The first two cases are trivial; the third follows from Theorem 1.4 and Corollary 2.3. □

The relevance of the above corollary is this: it allows us, by applying a result of Vaserstein [9], to conclude that the residue class rings of $\mathrm{Int}(\mathcal{O}_K)$ modulo non-zero prime ideals are GE_2, for those rings of integers $\mathcal{O}_K$ that are themselves GE_2. (We are interested in showing this as residue class rings that are GE_2 can be used as a step towards determining the stable rank of $\mathrm{Int}(\mathcal{O}_K)$.)

Generalized Euclidean rings were introduced by Cohn in a seminal paper [3] in 1966. A commutative ring R is GE_2 if any unimodular pair $(a, b) \in R^2$ (that is, any pair such that $aR+bR = R$) can be transformed to $(1, 0)$ by a series of elementary transformations, where an elementary transformation consists of replacing (a, b) by $(a, b+ra)$ or by $(a+rb, b)$ for some $r \in R$. Likewise, R is called GE_n if every unimodular n-tuple can be transformed to $(1, 0, \ldots, 0)$ by a series of elementary transformations (consisting of adding a scalar multiple of one entry to a different entry), and R is called generalized Euclidean if it is GE_n for all $n > 0$. By the Euclidean algorithm, Euclidean rings are generalized Euclidean.

Vaserstein showed for the ring of integers $\mathcal{O}_K$ in a number field K that firstly, every strict overring of $\mathcal{O}_K$ is GE_2, and, secondly, when K is not imaginary quadratic then $\mathcal{O}_K$ itself is GE_2.

Cohn [3] had already shown that in an imaginary quadratic number field K, the ring of integers $\mathcal{O}_K$ is not GE_2 unless it is actually Euclidean. Since the Euclidean imaginary quadratic $\mathcal{O}_K$ are known, we have in the results of Cohn [3] and Vaserstein [9] a complete classification of those rings of integers in number fields (and their overrings) that are GE_2.

Corollary 2.5. *Let* K *be one of those number fields for which* $\mathcal{O}_K$ *is* GE_2*. Then* $\mathrm{Int}(\mathcal{O}_K)/P$ *is* GE_2 *for every non-zero prime ideal* P *of* $\mathrm{Int}(\mathcal{O}_K)$*.*

In particular, $\mathrm{Int}(\mathcal{O}_K)/P$ *is* GE_2 *for every non-zero prime ideal* P *of* $\mathrm{Int}(\mathcal{O}_K)$ *whenever* $\mathcal{O}_K$ *is Euclidean or* K *not imaginary quadratic.*

Proof. If P is maximal then $\mathrm{Int}(\mathcal{O}_K)/P$ is a field, and hence Euclidean. Any non-zero non-maximal prime ideal of $\mathrm{Int}(\mathcal{O}_K)$ is of the form $\mathrm{Int}(\mathcal{O}_K) \cap f(x)K[x]$ for an irreducible polynomial $f \in K[x]$. Let c be a root of f in the splitting field of f over K. Clearly then $\mathrm{Int}(\mathcal{O}_K)/P$ is isomorphic to the image of c under $\mathrm{Int}(\mathcal{O}_K)$, which is GE_2 by Corollary 2.4 and the hypothesis. □

Acknowledgment: The surviving author wishes to thank the referee for graciously correcting some inaccuracies due to Prof. Halter-Koch's sudden death in the drafting stage of the paper, before proofreading.

References

[1] H. Bass, *Libération des modules projectifs sur certains anneaux de polynômes*, in Séminaire Bourbaki, 26e année (1973/1974), Exp. No. 448, Springer, Berlin, 1975, 228–354. Lecture Notes in Math., Vol. 431.

[2] S. Bourbaki, *Vol. 1973/1974, 26e année: Exposés Nos. 436–452*, Lecture Notes in Mathematics, Vol. 431, Springer, Berlin-New York, 1975.

[3] P. M. Cohn, *On the structure of the* GL_2 *of a ring*, Inst. Hautes Études Sci. Publ. Math. (1966), 5–53.

[4] F. Halter-Koch, *An Invitation to Algebraic Numbers and Algebraic Functions*, CRC Press, Boca Raton, 2020.

[5] F. Halter-Koch, *Class Field Theory and L-Functions*, CRC Press, Boca Raton, 2022.

[6] D. McQuillan, *Split primes and integer-valued polynomials*, J. Number Theory 43 (1993), 216–219.

[7] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 1992. English translation, see [8].

[8] J. Neukirch, *Algebraic number theory*, vol. 322 of Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer, Berlin, 1999. English translation of [7].

[9] L. N. Vaseršteĭn, *The group* SL_2 *over Dedekind rings of arithmetic type*, Mat. Sb. (N.S.) 89(131) (1972), 313–322, 351.

[10] L. N. Vaseršteĭn and A. A. Suslin, *Serre's problem on projective modules over polynomial rings, and algebraic* K*-theory*, Izv. Akad. Nauk SSSR Ser. Mat. 40 (1976), 993–1054, 1199.

Institut für Analysis und Zahlentheorie, Graz University of Technology, Kopernikusgasse 24, 8010 Graz, Austria

Email address: frisch@math.tugraz.at

Institut für Mathematik und wissenschaftliches Rechnen, University of Graz, Heinrichstrasse 36, 8010 Graz, Austria