

Appendix C

APPROXIMATION THEOREMS OVER ALGEBRAIC NUMBER FIELDS

1. Particularly the second part of these lectures was concerned mainly with the approximation of (real, p-adic, g-adic, and g*-adic) numbers by *rational numbers*. In this appendix certain results on the approximation of algebraic numbers by the elements of a fixed algebraic number field, of finite degree over the rational field, will be discussed. Without proofs, we shall state generalisations of the former Approximation Theorems. Detailed proofs would be rather long and involved; but there is no reason to foresee any essential difficulties.

One important special case was already investigated by W. J. LeVeque (Topics in Number Theory, Reading, Mass., 1956, vol. 2, 121-160). He proved the following generalisation of Roth's theorem.

Let K be an algebraic number field of finite degree over the rational field Γ ; let ξ be a real or complex algebraic number not in K; and let $\tau > 2$. There are at most finitely many elements κ of K satisfying

$$|\xi - \kappa| < H(\kappa)^{-\tau}.$$

Here $H(\kappa)$ denotes the *height* of κ , i.e. the maximum of the absolute values of the coefficients of the irreducible primitive equation for κ with rational integral coefficients. LeVeque's proof shows quite clearly which changes, as compared with Roth's proof in the rational case, have to be made for the theory over K.

The reader should also consult the paper by C. J. Parry (Acta mathematica 83, 1950, 1-100). This paper established p-adic generalisations of Siegel's theorem on the approximation of algebraic numbers by other algebraic numbers. Due to the new method by Roth, many of Parry's results can now be improved. Unfortunately, there still are difficulties if one wishes to study the approximation of a given algebraic number by *all algebraic numbers of a bounded degree* that do not necessarily lie in a fixed algebraic number field of finite degree.

2. As was already mentioned in Chapter 1, the rational field Γ has, except for equivalence, only the following valuations,

$$w_0(a), |a|, |a|_p;$$

here p runs over all different primes 2, 3, 5, These valuations are connected by the *basic identity*

$$w_0(a) = |a| \prod_p |a|_p.$$

Further every pseudo-valuation of Γ is equivalent either to a valuation of Γ , or to a pseudo-valuation of one of the two special types

$$\max(|a|_{p_1}^{\lambda_1}, \dots, |a|_{p_r}^{\lambda_r}), \max(|a|, |a|_{p_1}^{\lambda_1}, \dots, |a|_{p_r}^{\lambda_r}).$$

Here p_1, \dots, p_r are finitely many distinct primes, and $\lambda_1, \dots, \lambda_r$ are positive constants that do not affect the equivalence class. Important particular cases are the g -adic and g^* -adic pseudo-valuations

$$|a|_g \text{ and } |a|_{g^*}.$$

Very similar results hold for any algebraic number field K , say of degree n over the rational field Γ . Let

$$K^{(1)}, K^{(2)}, \dots, K^{(n)}$$

be the *conjugate fields* of K , all thought of as imbedded in the complex number field. For any α in K denote by $\alpha^{(i)}$ its conjugate in $K^{(i)}$. As is usual, let the notation be such that the first r_1 conjugate fields

$$K^{(1)}, K^{(2)}, \dots, K^{(r_1)}$$

are real, while the remaining $2r_2$ conjugate fields are arranged in pairs

$$K^{(r_1+i)}, K^{(r_1+r_2+i)} \quad (i = 1, 2, \dots, r_2)$$

of complex conjugate fields. Put

$$g_i = \begin{cases} 1 & \text{if } 1 \leq i \leq r_1, \\ 2 & \text{if } r_1+1 \leq i \leq r_1+r_2, \end{cases}$$

so that

$$r_1 + 2r_2 = \sum_{i=1}^{r_1+r_2} g_i = n.$$

3. First, the Archimedean valuation $|a|$ of Γ has exactly $r_1 + r_2$ distinct continuations

$$|\alpha|_i = |\alpha^{(i)}| \quad (i = 1, 2, \dots, r_1 + r_2)$$

on the field K , and these are likewise Archimedean valuations. Let K_i be the completion of K with respect to $|\alpha|_i$; then K_i is the real or the complex number field according as $1 \leq i \leq r_1$ or $r_1+1 \leq i \leq r_1+r_2$, respectively; and K_i has the degree g_i over the real field P , the completion of Γ with respect to $|a|$. If $N(\alpha)$ denotes the norm over Γ of the element α of K , the different continuations $|\alpha|_i$ of $|a|$ are connected with $N(\alpha)$ by the identity,

$$(1): \quad |N(\alpha)| = \prod_{i=1}^{r_1+r_2} |\alpha|_i^{g_i}.$$

Secondly, let p be any prime, and let $|a|_p$ be the corresponding p -adic valuation of Γ . The principal ideal (p) in K need in general not be a prime ideal. Let

$$(p) = \prod_{j=1}^{\pi(p)} \mathfrak{p}_j^{e(\mathfrak{p}_j)}$$

be its decomposition into a product of prime ideal powers. Here $\pi(p)$ denotes the number of distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_{\pi(p)}$ that divide (p) , and the exponents $e(\mathfrak{p}_j)$ are positive integers. In the usual notation, $e(\mathfrak{p}_j)$ is the *order* of \mathfrak{p}_j , and the positive integer $f(\mathfrak{p}_j)$ defined by

$$N(\mathfrak{p}_j) = p^{f(\mathfrak{p}_j)},$$

is the *degree* of \mathfrak{p}_j ; here $N(\mathfrak{p}_j)$ denotes the ideal norm of \mathfrak{p}_j . We put

$$g(\mathfrak{p}_j) = e(\mathfrak{p}_j)f(\mathfrak{p}_j) \quad (j = 1, 2, \dots, \pi(p)),$$

so that

$$\sum_{j=1}^{\pi(p)} g(\mathfrak{p}_j) = n.$$

There are now $\pi(p)$ distinct continuations of $|a|_p$ on K which we denote by

$$|\alpha|_{\mathfrak{p}_1}, \dots, |\alpha|_{\mathfrak{p}_{\pi(p)}};$$

like $|a|_p$, they are all Non-Archimedean. These valuations may be defined as follows.

If $\alpha = 0$, put

$$|0|_{\mathfrak{p}_j} = 0.$$

Next let $\alpha \neq 0$. There exists then a unique rational integer h_j which may be positive, negative, or zero, such that the fractional ideal

$$\mathfrak{p}_j^{h_j} \cdot (\alpha)$$

is the quotient $\frac{\mathfrak{m}}{\mathfrak{n}}$ of two integral ideals \mathfrak{m} and \mathfrak{n} both of which are relatively prime to \mathfrak{p}_j . In terms of this integer, put

$$|\alpha|_{\mathfrak{p}_j} = p^{\frac{-h_j}{e(\mathfrak{p}_j)}}.$$

The different \mathfrak{p}_j -adic valuations satisfy the identity

$$(2): \quad |N(\alpha)|_p = \prod_{j=1}^{\pi(p)} |\alpha|_{\mathfrak{p}_j}^{g(\mathfrak{p}_j)}.$$

Denote by $K_{\mathfrak{p}_j}$ the completion of K with respect to $|\alpha|_{\mathfrak{p}_j}$; then $K_{\mathfrak{p}_j}$ is an algebraic extension, of the exact degree $g(\mathfrak{p}_j)$, of the p -adic field P_p , the completion of Γ with respect to $|a|_p$. The field $K_{\mathfrak{p}_j}$ is called the *\mathfrak{p}_j -adic field*, and its elements are called *\mathfrak{p}_j -adic numbers*. These \mathfrak{p}_j -adic numbers may be developed in series similar to those for the p -adic numbers, and they have similar properties as the p -adic numbers.

Third, the field K has the trivial valuation $w_0(\alpha)$, and this is the only possible continuation of $w_0(a)$, the trivial valuation of the rational field Γ .

4. From the basic identity for Γ , and from the product formulae (1) and (2), we find at once that the elements α of K satisfy the *basic identity for K* ,

$$(3): \quad \prod_{i=1}^{r_1+r_2} |\alpha|_i^{g_i} \cdot \prod_{\mathfrak{p}} |\alpha|_{\mathfrak{p}}^{g(\mathfrak{p})} = w_0(\alpha).$$

Here \mathfrak{p} runs over all prime ideals of K , and

$$g(\mathfrak{p}) = e(\mathfrak{p})f(\mathfrak{p})$$

is again the product of the order and the degree of \mathfrak{p} . This identity implies the *basic inequality for K*

$$(4): \quad \prod_{i=1}^{r_1+r_2} |\alpha|_i^{g_i} \cdot \prod_{j=1}^r |\alpha|_{\mathfrak{p}_j}^{g(\mathfrak{p}_j)} \geq 1 \quad \text{if } \alpha \neq 0 \text{ is any integer in } K.$$

Here $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are finitely many prime ideals of K , all distinct. This inequality is of the same importance for the approximation theory over K as was the inequality

$$|a| \prod_{j=1}^r |a|_{p_j} \geq 1 \quad \text{if } a \neq 0 \text{ is a rational integer}$$

for this theory over the rational field.

5. Similarly as for Γ , any finite set of distinct valuations

$$|\alpha|_{i_1}, \dots, |\alpha|_{i_q}, |\alpha|_{\mathfrak{p}_1}, \dots, |\alpha|_{\mathfrak{p}_r}$$

of K is independent, and every pseudo-valuation of K is equivalent to one of the special form

$$\max(|\alpha|_{i_1}, \dots, |\alpha|_{i_q}, |\alpha|_{\mathfrak{p}_1}^{\lambda_1}, \dots, |\alpha|_{\mathfrak{p}_r}^{\lambda_r}).$$

Here $0 \leq q \leq r_1 + r_2$; i_1, \dots, i_q are distinct suffixes $1, 2, \dots, r_1 + r_2$; $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct prime ideals of K ; and $\lambda_1, \dots, \lambda_r$ are positive constants. Actually, the values of the latter do not affect the equivalence class of the pseudo-valuation. One, but not both, of the numbers q and r may vanish, and if then the other number equals 1, the pseudo-valuation becomes equivalent to one of the valuations that were discussed already.

5. Of particular interest are certain Non-Archimedean pseudo-valuations of K which are analogous to the g -adic value $|a|_g$ of Γ and may be defined similarly.

For let \mathfrak{m} be any integral ideal of K that is distinct from both the zero ideal (0) and the unit ideal $\mathfrak{m}=(1)$. Denote by

$$\mathfrak{m} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$$

its factorisation into a product of powers of distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, with exponents e_1, \dots, e_r which are positive integers. Let further $e(\mathfrak{p}_j)$ be the order of \mathfrak{p}_j , and let p_j be the rational prime that is divisible by \mathfrak{p}_j .

Naturally the r rational primes p_1, \dots, p_r need not all be distinct.

The \mathfrak{g} -adic pseudo-valuation $|\alpha|_{\mathfrak{g}}$ of K is now defined by the formula

$$|\alpha|_{\mathfrak{g}} = \max \left(|\alpha|_{\mathfrak{p}_1}^{\frac{e(\mathfrak{p}_1) \log N(\mathfrak{g})}{e_1 \log p_1}}, \dots, |\alpha|_{\mathfrak{p}_r}^{\frac{e(\mathfrak{p}_r) \log N(\mathfrak{g})}{e_r \log p_r}} \right),$$

where $N(\mathfrak{g})$ denotes the ideal norm of \mathfrak{g} . In the special case of the rational field Γ , $|\alpha|_{\mathfrak{g}}$ becomes again the g -adic value $|a|_g$ because $\mathfrak{p}_1 = (p_1), \dots, \mathfrak{p}_r = (p_r)$ now are principal prime ideals, and all the orders $e(\mathfrak{p}_1), \dots, e(\mathfrak{p}_r)$ are unity.

There exist elements $\gamma \neq 0$ of K which generate principle ideals of the special form

$$(\gamma) = \mathfrak{g} \frac{\mathfrak{m}}{\mathfrak{n}}$$

where \mathfrak{m} and \mathfrak{n} are integral ideals that are prime to \mathfrak{g} . Therefore

$$|\gamma|_{\mathfrak{p}_j} = p_j^{-e_j/e(\mathfrak{p}_j)} \quad (j = 1, 2, \dots, r)$$

and hence

$$|\gamma|_{\mathfrak{g}} = |\gamma|_{\mathfrak{p}_1}^{\frac{e(\mathfrak{p}_1) \log N(\mathfrak{g})}{e_1 \log p_1}} = \dots = |\gamma|_{\mathfrak{p}_r}^{\frac{e(\mathfrak{p}_r) \log N(\mathfrak{g})}{e_r \log p_r}} = \frac{1}{N(\mathfrak{g})}.$$

It follows then that, similarly as the g -adic value $|a|_g$, the \mathfrak{g} -adic value has the following two properties,

- (I): $|\alpha^n|_{\mathfrak{g}} = (|\alpha|_{\mathfrak{g}})^n$ for all $\alpha \in K$ and all positive integers n ;
- (II): $|\alpha \gamma^n|_{\mathfrak{g}} = |\alpha|_{\mathfrak{g}} (|\gamma|_{\mathfrak{g}})^n$ for all $\alpha \in K$ and all rational integers n .

In the special case when $\mathfrak{g} = \mathfrak{p}^e$ is the power of a single prime ideal,

$$|\alpha|_{\mathfrak{g}} = |\alpha|_{\mathfrak{p}}^{\frac{e(\mathfrak{p})e f(\mathfrak{p}) \log p}{e \log p}} = |\alpha|_{\mathfrak{p}}^{g(\mathfrak{p})},$$

and so $|\alpha|_{\mathfrak{g}}$ is now equivalent to the \mathfrak{p} -adic valuation $|\alpha|_{\mathfrak{p}}$.

6. The completion of K with respect to $|\alpha|_{\mathfrak{g}}$, $K_{\mathfrak{g}}$ say, is called the \mathfrak{g} -adic ring, and its elements are called \mathfrak{g} -adic numbers. Let similarly $K_{\mathfrak{p}_1}, \dots, K_{\mathfrak{p}_r}$ be the completions of K with respect to $|\alpha|_{\mathfrak{p}_1}, \dots, |\alpha|_{\mathfrak{p}_r}$, so that they are the \mathfrak{p}_1 -adic, ..., \mathfrak{p}_r -adic fields, respectively, which we have already considered. Just as in the g -adic case, there is a one-to-one correspondence

$$A \leftrightarrow (\alpha_1, \dots, \alpha_r)$$

between the elements A of $K_{\mathfrak{g}}$ and the sets $(\alpha_1, \dots, \alpha_r)$ of one element α_r in $K_{\mathfrak{p}_r}$, respectively. This correspondence is again preserved under addition, subtraction, and multiplication; and whenever division is possible, it is also preserved under division.

7. In order to formulate the assertions in a convenient form, the following notation will be used.

First, we put $|\alpha|^* = \min(|\alpha|, 1)$,

$$|\alpha|_i^* = \min(|\alpha|_i, 1) \quad (i = 1, 2, \dots, r_1 + r_2),$$

$$|\alpha|_{\mathfrak{p}}^* = \min(|\alpha|_{\mathfrak{p}}, 1),$$

$$|\alpha|_{\mathfrak{g}}^* = \min(|\alpha|_{\mathfrak{g}}, 1).$$

Secondly, let q be any integer satisfying

$$0 \leq q \leq r_1 + r_2.$$

Then denote by i_1, \dots, i_q any system of q distinct suffixes $1, 2, \dots, r_1 + r_2$ arranged such that

$$1 \leq i_1 < i_2 < \dots < i_q \leq r_1 + r_2;$$

for $q=0$ the system is empty.

Third, $\mathfrak{g}, \mathfrak{g}', \mathfrak{g}''$ are three integral ideals distinct from (0) and $\mathfrak{s} = (1)$ which are relatively prime in pairs.

Fourth, r, r', r'' are three non-negative integers, and

$$\mathfrak{p}_1, \dots, \mathfrak{p}_r; \mathfrak{p}_{r+1}, \dots, \mathfrak{p}_{r+r'}; \mathfrak{p}_{r+r'+1}, \dots, \mathfrak{p}_{r+r'+r''}$$

are $r+r'+r''$ distinct prime ideals of K . It is not excluded that one or more of r, r', r'' are zero.

Fifth, $\rho_{i_1}, \dots, \rho_{i_q}, \sigma$ are non-negative constants, and λ, μ are constants satisfying

$$0 \leq \lambda \leq 1, \quad 0 \leq \mu \leq 1.$$

Sixth, $c_{i_1}, \dots, c_{i_q}, c, c', c'', C_{i_1}, \dots, C_{i_q}, C, C', C''$ are positive constants.

8. The conjectured generalisations of the former Approximation Theorems can now be formulated. There are three such assertions, and each has two equivalent forms, just as in the former theorems.

Assertion (1,I): Let $\xi_{(i_1)}, \dots, \xi_{(i_q)}, \xi_1, \dots, \xi_r$ be algebraic numbers, all distinct from zero and such that

$$\xi_{(i_1)} \in K_{i_1}, \dots, \xi_{(i_q)} \in K_{i_q}; \quad \xi_1 \in K_{\mathfrak{p}_1}, \dots, \xi_r \in K_{\mathfrak{p}_r}.$$

Further let Ξ be the \mathfrak{g} -adic number defined by

$$\Xi \leftrightarrow (\xi_1, \dots, \xi_r).$$

Assume that there exist infinitely many elements $\kappa \neq 0$ of K , all distinct, satisfying the inequalities

$$|\xi_{(i_Q)} - \kappa^{(i_Q)}|^* \leq c_{i_Q} H(\kappa)^{-\rho_{i_Q}} \quad (Q = 1, 2, \dots, q),$$

$$|\Xi - \kappa|_{\mathfrak{g}}^* \leq c H(\kappa)^{-\sigma},$$

$$|\kappa|_{\mathfrak{g}}^* \leq c' H(\kappa)^{\lambda-1}, \quad \left| \frac{1}{\kappa} \right|_{\mathfrak{g}}^* \leq c'' H(\kappa)^{\mu-1}.$$

Then

$$\sum_{Q=1}^q g_{1Q} \rho_{1Q} + \sigma \leq \lambda + \mu .$$

Assertion (1,II): Let $F(x)$ be a polynomial with coefficients in K which does not vanish for $x=0$ and has no multiple factors. Assume there exists an infinite sequence of distinct elements $\kappa \neq 0$ of K satisfying the inequalities

$$\begin{aligned} |F(\kappa)|_{i_Q}^* &\leq C_{i_Q} H(\kappa)^{-\rho_{1Q}} \quad (Q = 1, 2, \dots, q), \\ |F(\kappa)|_{\mathfrak{g}}^* &\leq C H(\kappa)^{-\sigma}, \\ |\kappa|_{\mathfrak{g}}^* &\leq C' H(\kappa)^{\lambda-1}, \quad \left| \frac{1}{\kappa} \right|_{\mathfrak{g}}^* \leq C'' H(\kappa)^{\mu-1}. \end{aligned}$$

Then

$$\sum_{Q=1}^q g_{1Q} \rho_{1Q} + \sigma \leq \lambda + \mu .$$

Remark: LeVeque's theorem is the special case $q=1, \sigma=0, \lambda=\mu=1$ of the Assertion (1,I).

9. The next assertions can be put in a rather simpler form, but are somewhat stronger.

Assertion (2,I): Let $\xi_{(1)} \neq 0, \dots, \xi_{(r_1)} \neq 0$ be real algebraic numbers; let $\xi_{(r_1+1)} \neq 0, \dots, \xi_{(r_1+r_2)} \neq 0$ be complex algebraic numbers; and let $\xi_j \neq 0$, for $j=1, 2, \dots, r$, be a \mathfrak{p}_j -adic algebraic number. Assume there exists an infinite sequence of distinct elements $\kappa \neq 0$ of K such that

$$\prod_{i=1}^{r_1+r_2} |\xi_{(i)}^{-\kappa}|^* g_{1i} \prod_{j=1}^r |\xi_j^{-\kappa}|_{\mathfrak{p}_j}^* g(\mathfrak{p}_j)^{r+r'+r''} \left| \frac{1}{\kappa} \right|_{\mathfrak{p}_j}^* g(\mathfrak{p}_j) \leq c H(\kappa)^{-\tau} .$$

Then

$$\tau \leq 2 .$$

Assertion (2,II): Let $F_{(1)}(x), \dots, F_{(r_1+r_2)}(x), F_1(x), \dots, F_r(x)$ be arbitrary equal or distinct polynomials with coefficients in K that do not vanish for $x=0$ and have no multiple factors. Assume there exists an infinite sequence of distinct elements $\kappa \neq 0$ of K satisfying

$$\prod_{i=1}^{r_1+r_2} |F_{(i)}(\kappa)|_i^* g_{1i} \prod_{j=1}^r |F_j(\kappa)|_{\mathfrak{p}_j}^* g(\mathfrak{p}_j)^{r+r'} \left| \frac{1}{\kappa} \right|_{\mathfrak{p}_j}^* g(\mathfrak{p}_j) \leq C H(\kappa)^{-\tau} .$$

Then

$$\tau \leq 2 .$$

10. The results stated so far refer to solutions $\kappa \neq 0$ which are arbitrary elements of K . They have analogues in which $\kappa \neq 0$ is restricted to *integers* in K , and then stronger assertions can be made. It will suffice to state the analogues to the two assertions (2,I) and (2,II).

Assertion (3,I): Let $\xi_{(1)} \neq 0, \dots, \xi_{(r_1)} \neq 0$ be real algebraic numbers; let $\xi_{(r_1+1)} \neq 0, \dots, \xi_{(r_1+r_2)} \neq 0$ be complex algebraic numbers; and let $\xi_j \neq 0$, for $j=1, 2, \dots, r$, be a p_j -adic algebraic number. Assume there exists an infinite sequence of distinct integers $\kappa \neq 0$ in K for which

$$\prod_{i=1}^{r_1+r_2} |\xi_{(i)} - \kappa|_1^{*g_i} \cdot \prod_{j=1}^r |\xi_j - \kappa|_{p_j}^{*g(p_j)} \cdot \prod_{j=r+1}^{r+r'} |\kappa|_{p_j}^{*g(p_j)} \leq c H(\kappa)^{-\tau}.$$

Then

$$\tau \leq 1.$$

Assertion (3,II): Let $F_{(1)}(x), \dots, F_{(r_1+r_2)}(x), F_1(x), \dots, F_r(x)$ be arbitrary equal or distinct polynomials with coefficients in K that do not vanish for $x=0$ and have no multiple factors. Assume there exists an infinite sequence of distinct integers $\kappa \neq 0$ in K for which

$$\prod_{i=1}^{r_1+r_2} |F_{(i)}(\kappa)|_1^{*g_i} \cdot \prod_{j=1}^r |F_j(\kappa)|_{p_j}^{*g(p_j)} \cdot \prod_{j=r+1}^{r+r'} |\kappa|_{p_j}^{*g(p_j)} \leq C H(\kappa)^{-\tau}$$

Then

$$\tau \leq 1.$$

10. In Chapter 9 we gave a number of applications of the Approximation Theorem over the rational field. It is obvious that similar applications can be made of the last assertions.