Lectures on Euclidean Rings

H.W. Lenstra, Jr.

Bielefeld, Summer 1974

Contents

AMS (MOS) subject classification scheme (1970): 13F10, 12A45, 16A04.

Notation and terminology.

A <u>ring</u> need not be commutative and has a unit element 1 which is different from 0 and which is preserved by ring homomorphisms. The group of units of a ring R is denoted by R^*. A <u>module</u> is a left module, on which 1 acts as the identity. A <u>domain</u> is a commutative ring without zero-divisors. <u>Fields</u> are commutative. By $\underline{Z}$, $\underline{Q}$, $\underline{R}$, $\underline{C}$, $\underline{F}_q$ we mean the ring of integers, the field of rational numbers, the field of real numbers, the field of complex numbers, and the finite field with q elements, respectively. Notations like $\underline{Z}_{\geq 0}$ and $\underline{R}_{>0}$ are self-explaining.

Set - theoretic difference is denoted by −; but $A + B = \{a+b \mid a \in A, b \in B\}$ if A,B are subsets of an additive abelian group, and $a + B = \{a+b \mid b \in B\}$. The cardinality of a set S is denoted by $\# S$. For a real number x we mean by $[x]$ either the greatest integer not exceeding x or a reference to item x of the bibliography. Confusion is unlikely. The end or the absence of a proof is marked by $\square$.

We assume that the reader is acquainted with the elementary properties of well ordered sets and ordinal numbers. The smallest infinite ordinal is denoted by ω, and + denotes ordinary ordinal addition (so $1 + \omega = \omega < \omega + 1$). For Hessenberg addition $\oplus$ we refer to the proof of (1.11).

1. Definitions and elementary properties.

Let R be a ring, M a left R-module and W a well ordered set.

(1.1)Definition. A map φ: $M - \{0\} \to W$ is called an algorithm of type 1 on M if for all $a,b \in M$, $b \neq 0$, there exist $q \in R$ and $c \in M$ such that $a = qb + c$ and either $c = 0$ or $\varphi(c) < \varphi(b)$.

It is often convenient that $\varphi(0)$ have a meaning. There are two natural ways to achieve this.

(1.2) Definition. A map φ: $M \to W$ is called an algorithm of type 2 on M if for all $a,b \in M$, $b \neq 0$, there exist $q \in R$ and $c \in M$ such that $a = qb + c$ and $\varphi(c) < \varphi(b)$.

(1.3) Definition. A map φ: $M \to W$ is called an algorithm of type 3 on M if for all $a,b \in M$ there exist $q \in R$ and $c \in M$ such that $a = qb + c$, and $c = 0$ or $\varphi(c) < \varphi(b)$.

In order to clear up the relation between these three types of algorithms it is useful to introduce the following notion. We call two maps ψ: $S \to W$ and ψ': $S \to W'$ from a set S to well ordered sets W, W' equivalent if there is an isomorphism of ordered sets σ: $\psi[S] \to \psi'[S]$ such that $\psi' = \sigma\psi$. Note that such a σ is necessarily unique. Note also that each map ψ: $S \to W$ is equivalent to a unique ψ' whose image is a beginning segment of the ordinal numbers.

It is clear that a map equivalent to an algorithm of any type is itself an algorithm of the same type. We are only interested in algorithms up to equivalence.

(1.4) Proposition. Let φ_1: $M - \{0\} \to W$ be an algorithm of type 1, and put $W_2 = \{*\} \cup W$ (disjoint). Extend the ordering of W to a well-ordering of W_2 by $* < w$ for all $w \in W$. Then the map φ_2: $M \to W_2$ defined by

$$\varphi_2(m) = \varphi_1(m) \qquad (m \neq 0),$$

$$\varphi_2(0) = *$$

is an algorithm of type 2 on M. Conversely, every algorithm of type 2 on M is, up to equivalence, obtained in this way from an algorithm of type 1.

Proof. It is straightforward to check that φ_2 is an algorithm of type 2. To prove the converse, it clearly suffices to show: if φ is an algorithm of type 2 and $\varphi(b)$ is minimal in $\varphi[M]$, then $b = 0$. But this follows from (1.2), since in the case $b \neq 0$ we would get $\varphi(c) < \varphi(b)$, contradicting the minimality of $\varphi(b)$. □

(1.5) Proposition. Let $\varphi_1 : M - \{0\} \to W$ be an algorithm of type 1, and put $W_3 = W \cup \{*\}$ (disjoint). Extend the ordering of W to a well-ordering of W_3 by $w < *$ for all $w \in W$. Then the map $\varphi_3 : M \to W_3$ defined by

$$\varphi_3(m) = \varphi_1(m) \quad (m \neq 0),$$

$$\varphi_3(0) = *$$

is an algorithm of type 3 on M. Conversely, every algorithm of type 3 is, up to equivalence, obtained in this way from an algorithm of type 1.

Proof. One verifies immediately that φ_3 is an algorithm of type 3. Next let φ be any algorithm of type 3 on M. To prove the last assertion of (1.5) it suffices to show $\varphi(a) < \varphi(0)$ for every $a \in M$, $a \neq 0$. But this is clear from (1.3) with $b = 0$. □

In the sequel we mean by an algorithm an algorithm of type 3, unless the contrary is mentioned. Using (1.4) and (1.5) the reader will have no difficulty in reformulating the various results so as to conform to the other definitions.

Instead of "algorithm" we also say left algorithm. On a right R-module, the notion of a right algorithm is defined similarly: just replace $a = qb + c$ by $a = bq + c$.

A left R-module M is called euclidean if there exist a well ordered set W and an algorithm $\varphi : M \to W$. We call a ring R euclidean or left euclidean if it is euclidean as a left module over itself. Similarly, we call R right euclidean if there is a right algorithm on the right R-module R. Finally, R is two-sided euclidean if there is a map φ from R to a well ordered set which is at the same time a left algorithm and a right algorithm.

(1.6) Theorem. Let M be a euclidean R-module and let $N \subset M$ be a submodule. Then $N = Rx$ for some $x \in N$. More precisely, if φ is an algorithm on M and $x \in N$

satisfies

$$\varphi(x) = \min\{\varphi(y)|y\varepsilon N\}$$

then $N = Rx$.

Proof. Let $x \in N$ satisfy $\varphi(x) = \min\{\varphi(y)|y\varepsilon N\}$. Clearly we have $Rx \subset N$, and the opposite inclusion is proved as follows. For $y \in N$ we can write $y = qx + c$ with $q \in R$, $c \in M$, and $c = 0$ or $\varphi(c) < \varphi(x)$. Then $c = y - qx \in N$ so $\varphi(c) < \varphi(x)$ is excluded by minimality of $\varphi(x)$. Hence $c = 0$ and $y = qx \in Rx$, as required. □

(1.7) Corollary . Every left ideal of a euclidean ring is principal. Every euclidean domain is a principal ideal domain and therefore has unique factorization. Every two-sided ideal $\underline{a}$ of a two-sided euclidean ring R contains an element x such that $\underline{a} = Rx = xR$. □

(1.8) Corollary. Let $\varphi: M \to W$ be an algorithm. For a submodule $N \subset M$ put

$$\hat{\varphi}(N) = \min\{\varphi(y)|y\varepsilon N\}$$

and for $x \in M$ let

$$\varphi_*(x) = \hat{\varphi}(Rx).$$

Then we have

(i) $\hat{\varphi}(N) \leqslant \hat{\varphi}(N')$ for $N' \subset N$, with equality if and only if $N = N'$;

(ii) $\varphi_*(x) \leqslant \varphi(x)$ for all $x \in M$;

(iii) φ_* is an algorithm on M;

(iv) $\varphi_*(x) \leqslant \varphi_*(qx)$ for all $x \in M$ and $q \in R$, with equality if and only if $Rx = Rqx$.

Proof. (i) Clearly $\hat{\varphi}(N) \leqslant \hat{\varphi}(N')$ for $N' \subset N$. If equality holds, then some $x \in N' \subset N$ satisfies $\varphi(x) = \min\{\varphi(y)|y\varepsilon N\}$. By (1.6) this implies $N = Rx \subset N'$ so $N = N'$, as required.

(ii) is obvious.

(iii) Let $b \in M$ and $a \in M - Rb$. Choose $r \in R$ such that $\varphi_*(b) = \varphi(rb)$. Since φ is an algorithm, there exists $c \in a + Rrb$ with $\varphi(c) < \varphi(rb)$. Then $c \in a + Rb$ and $\varphi_*(c) \leqslant \varphi(c) < \varphi(rb) = \varphi_*(b)$, which proves that

φ_* is an algorithm.

(iv) is clear from (i). □

(1.9) Proposition. Let N be a submodule of a euclidean module M. Then both N and M/N are euclidean.

Proof. If φ is an algorithm on M, then $\varphi|N$ is easily proved to be an algorithm on N. An algorithm ψ on M/N is obtained by putting $\psi(x+N) = \min\{\varphi(y)\,|\,y \in x+N\}$ for $x + N \in M/N$. □

(1.10) Corollary. Let R be a euclidean ring and $\underline{a} \subset R$ a two-sided ideal. Then $R/\underline{a}$ is a euclidean ring. □

Subrings of euclidean rings need not be euclidean, e.g. $k[X^2,X^3] \subset k[X]$ where k is a field, or $\underline{Z}[\sqrt{-5}] \subset \underline{Z}[\zeta_{20}]$, where ζ_{20} is a primitive 20-th root of unity.

(1.11) Proposition. Let M_i be a euclidean R_i-module, for i = 1,2. Then $M_1 \times M_2$ is a euclidean $R_1 \times R_2$-module (the action of $R_1 \times R_2$ on $M_1 \times M_2$ being componentwise).

Proof. First we note that a map φ: M → W is an algorithm if and only if for all a,b $\in$ M there exist q $\in$ R and c $\in$ M such that $a = q\cdot b + c$ and $c = b$ or $\varphi(c) < \varphi(b)$ (notice the inessential replacement of "$c = 0$" by "$c = b$").

Secondly, we recall [cf.3] that the "Hessenberg sum" of two ordinals α and β can be defined inductively by

$$\begin{aligned} \alpha \oplus \beta = \min\{\gamma\,|\,&\gamma \text{ is an ordinal},\\ &\gamma > \lambda \oplus \beta \text{ for all } \lambda < \alpha,\\ &\gamma > \alpha \oplus \lambda \text{ for all } \lambda < \beta\}. \end{aligned}$$

This addition is commutative and associative.

Now let φ_i be an algorithm on M_i with ordinal values, for i = 1,2. We claim that an algorithm φ on $M = M_1 \times M_2$ is given by

$$\varphi((m_1,m_2)) = \varphi_1(m_1) \oplus \varphi_2(m_2).$$

To prove this, let $a = (a_1,a_2)$, $b = (b_1,b_2) \in M$. For i = 1,2, choose $q_i \in R_i$,

$c_i \in M_i$ such that $a_i = q_i \cdot b_i + c_i$ and $\varphi_i(c_i) \leqslant \varphi_i(b_i)$, with equality if and only if $c_i = b_i$. Putting $q = (q_1,q_2) \in R = R_1 \times R_2$ we then have $a = qb + c$. Moreover, if at least one of the inequalities $\varphi_1(c_1) \leqslant \varphi_1(b_1)$ and $\varphi_2(c_2) \leqslant \varphi_2(b_2)$ holds <u>strictly</u>, then

$$\varphi(c) = \varphi_1(c_1) \oplus \varphi_2(c_2) < \varphi_1(b_1) \oplus \varphi_2(b_2) = \varphi(b)$$

and if both $\varphi_1(c_1) = \varphi_1(b_1)$ and $\varphi_2(c_2) = \varphi_2(b_2)$ then $c_i = b_i$ for $i = 1,2$ and $c = b$. This proves that φ is an algorithm. □

2. The smallest algorithm.

Let M be a euclidean module, W a well ordered set and Φ a non-empty set of algorithms $\varphi: M \to W$. Then the map $\psi: M \to W$, defined by

$$\psi(x) = \min \{ \varphi(x) \mid \varphi \in \Phi\}$$

is an algorithm on M. To prove this, let $a, b \in M$ and choose $\varphi \in \Phi$ such that $\psi(b) = \varphi(b)$. Since φ is an algorithm, there exist $q \in R$ and $c \in M$ such that $a=qb+c$, and $c=0$ or $\varphi(c) < \varphi(b)$. This implies $c=0$ or $\psi(c) \leqslant \varphi(c) < \varphi(b) = \psi(b)$, as required.

Taking

$$W_M = \{\text{ordinals of cardinality } \leqslant \# M\}$$

we conclude that the map $\theta_M: M \to W_M$ defined by

$$\theta_M(x) = \min \{ \varphi(x) \mid \varphi: M \to W_M \text{ is an algorithm } \}$$

is itself an algorithm, the so-called "smallest algorithm" of M.

(2.1) Proposition. Let $\psi : M \to W_M$ be an algorithm. Then the following three assertions are equivalent:

(a) $\psi = \theta_M$.

(b) $\psi(x) \leqslant \varphi(x)$ for all $x \in M$ and for all algorithms $\varphi : M \to W_M$.

(c) for all $b \in M$ and for all $\lambda \in W_M$ satisfying $\lambda < \psi(b)$, there exists $a \in M - Rb$ such that $\psi(c) \geqslant \lambda$ for every $c \in a + Rb$.

Proof. (a) $\Leftrightarrow$ (b) is clear from the definition of θ_M.
(b) $\Rightarrow$ (c). Assume (b), let $b \in M$ and $\lambda < \psi(b)$. Define $\varphi: M \to W_M$ by

$$\varphi(m) = \psi(m), \quad m \neq b,$$
$$\varphi(b) = \lambda.$$

Then $\varphi(b) < \psi(b)$ so (b) implies that φ is not an algorithm. Therefore there are $a, b' \in M$ with $a \notin Rb'$ such that there is no $c \in a + Rb'$ with $\varphi(c) < \varphi(b')$. In the case $b \neq b'$ this would contradict the assumption that ψ is an algorithm. Hence $b = b'$, and we conclude $\psi(c) = \varphi(c) \geqslant \varphi(b') = \lambda$ for all $c \in a + Rb$, as required.

(c) $\Rightarrow$ (b). Let $\varphi : M \to W_M$ be an algorithm, and $b \in M$. Assuming (c), we prove $\psi(b) \leqslant \varphi(b)$ by induction on $\varphi(b)$. Hence we may assume $\psi(x) \leqslant \varphi(x)$ for all $x \in M$ with $\varphi(x) < \varphi(b)$.

Suppose $\varphi(b) < \psi(b)$; we derive a contradiction. Applying (c) with $\lambda = \varphi(b)$ we find $a \in M - Rb$ such that $\psi(c) \geqslant \varphi(b)$ for all $c \in a + Rb$. In particular, if we choose $c \in a + Rb$ such that $\varphi(c) < \varphi(b)$ then we have $\varphi(c) < \varphi(b) \leqslant \psi(c)$, while the inductive hypothesis asserts $\psi(c) \leqslant \varphi(c)$. Contradiction. □

Using (2.1) (c) one verifies easily that the usual degree is the smallest algorithm (of type 1) on $k[X]$, where k is a field. Compare (4.3).

(2.2) Corollary. If M is euclidean, then $\theta_M(x) \leqslant \theta_M(qx)$ for all $x \in M$, $q \in R$, with equality if and only if $Rx = Rqx$.

Proof. Let $\theta = \theta_M$. From (1.8) (ii,iii) and (2.1) (b) we conclude $\theta_* = \theta$, so (2.2) follows from (1.8) (iv). □

(2.3) Corollary. Let M_i be a euclidean R_i-module with smallest algorithm θ_i, for $i=1,2$. Then the smallest algorithm θ on the $R_1 x R_2$-module $M = M_1 x M_2$ is given by

$$\theta((m_1, m_2)) = \theta_1(m_1) \oplus \theta_2(m_2).$$

Proof. We know from the proof of (1.11) that the map $\psi : M \to W_M$ defined by $\psi((m_1,m_2)) = \theta_1(m_1) \oplus \theta_2(m_2)$ is an algorithm on M. To prove $\psi = \theta$ it suffices to check that (2.1) (c) is satisfied. So let $b = (b_1, b_2) \in M$ and $\lambda < \psi(b) = \theta_1(b_1) \oplus \theta_2(b_2)$ be arbitrary. The definition of the Hessenberg sum implies that for $i=1$ or for $i=2$ there exists an ordinal $\mu_i < \theta_i(b_i)$ such that $\lambda \leqslant \mu_i \oplus \theta_{3-i}(b_{3-i})$. Without loss of generality we may assume $i=1$. Applying (2.1) to M_1 we know that there exists $a_1 \in M_1 - R_1 b_1$ such that $\theta_1(c_1) \geqslant \mu_1$ for all $c_1 \in a_1 + R_1 b_1$. Then the element $a = (a_1, b_2)$ of M is not in $R \cdot b = (R_1 x R_2) \cdot b$, and for each $c = (c_1, c_2) \in a + R \cdot b$ we have $c_2 \in R_2 \cdot b_2$ and therefore

$$\psi(c) = \theta_1(c_1) \oplus \theta_2(c_2) \geqslant \mu_1 \oplus \theta_2(b_2) \geqslant \lambda.$$

This proves that indeed (2.1) (c) is satisfied. □

(2.4) Proposition. Let $\varphi : M \to W_M$ be an algorithm, and let $b \in M$ satisfy $\varphi(b) = \varphi_*(b)$ (cf.(1.8)). Let Ann (b) be the left ideal $\{r \in R \mid r\, b = 0\}$ of R. Then R/Ann (b) is a euclidean R-module, and

$$\varphi(qb) \geqslant \varphi(b) + \theta_{R/\mathrm{Ann}(b)}(q+\mathrm{Ann}(b))$$

for all $q \in R$; here + denotes usual ordinal addition.

Proof. For all $q \in R$ we have $\varphi(qb) \geqslant \varphi(b)$, so we can write

$$\varphi(qb) = \varphi(b) + \mu(q)$$

for some map $\mu : R \to W_M$. Clearly $\mu(q) = \mu(q')$ if $q-q' \in$ Ann (b), so μ induces a map $\lambda : R/\mathrm{Ann}\ (b) \to W_M$. It is easily checked that λ is an algorithm on R/Ann (b), and (2.4) follows quickly. □

(2.5) Corollary. Let R be a euclidean ring without zero-divisors. Then

$$\theta_R(ab) \geqslant \theta_R(b) + \theta_R(a)$$

for all $a,b \in R$, $b \neq 0$.

Proof. Apply (2.4) with R=M and $\varphi = \theta_R$. □

We conclude this section with a discussion of the "transfinite construction".

Let M be a module over a ring R, and let W_M be the set of ordinals whose cardinality does not exceed $\# M$. For $\lambda \in W_M$ we define inductively

$$M_\lambda = \{x \in M \mid \text{the natural map } \{0\} \cup \bigcup_{\alpha \in W_M, \alpha<\lambda} M_\alpha \to M/Rx \text{ is surjective}\}.$$

Here the natural map $\{0\} \cup \bigcup_\alpha M_\alpha \to M/Rx$ is the composite of the inclusion in M and the canonical projection $M \to M/Rx$.

We have

$$M_0 = \{x \in M \mid M = Rx\},$$

$$M_\alpha \subset M_\beta \qquad \text{for } \alpha < \beta.$$

If M = R is a commutative ring, then one easily checks

$$R_0 = R^*,$$

$$R_1 = R^* \cup \{x \in R \mid Rx \text{ is a maximal ideal in R, and the map } R^* \to (R/Rx)^* \text{ is surjective}\}.$$

(2.6) Theorem (Motzkin [1], Samuel [2]). The R-module M is euclidean if and only if $\bigcup_{\lambda \in W_M} M_\lambda = M$. If M is euclidean, then its smallest algorithm is given by

$$\theta_M(x) = \min\{\lambda \mid x \in M_\lambda\}.$$

Proof. If $\bigcup_{\lambda \in W_M} M_\lambda = M$ then the function $\psi : M \to W_M$ defined by

$$\psi(x) = \min\{\lambda \mid x \in M_\lambda\} \tag{2.7}$$

is easily proved to be an algorithm; so $\bigcup M_\lambda = M$ implies that M is euclidean. Conversely, suppose M is euclidean and let $\varphi: M \to W_M$ be an algorithm. Using induction on λ it is not hard to prove that

$$\{x \in M \mid \varphi(x) \leqslant \lambda\} \subset M_\lambda \tag{2.8}$$

for $\lambda \in W_M$. Taking the union over λ gives $M \subset \bigcup M_\lambda$ so $M = \bigcup M_\lambda$, as required.

Finally, if M is euclidean then (2.7) and (2.8) imply $\psi(x) \leqslant \varphi(x)$, for all $x \in M$ and all algorithms $\varphi: M \to W_M$. This means $\psi = \theta_M$. □

3. Commutative rings.

In this section R denotes a commutative ring.

(3.1) Proposition. Let M be an R-module. If $M \neq Rx$ for all $x \in M$, then M is not euclidean. If $x \in M$ satisfies $M = Rx$, then M is euclidean if and only if the ring $R/\mathrm{Ann}(x)$ is euclidean.

Proof. Obvious. Note that $R/\mathrm{Ann}(x)$ is a ring since R is commutative. □

By (3.1) we need in the commutative case only consider the situation $M = R$.

A special local ring is a local ring whose maximal ideal $\underline{m}$ is generated by one nilpotent element: $\underline{m} = R\pi$, $\pi^n = 0$. For example, a field is a special local ring.

(3.2) Proposition. Let R be a commutative ring. If R is not a principal ideal ring, then R is not euclidean. If R is a principal ideal ring, then

$$R \cong \prod_{i=1}^{t} R_i$$

for some non-negative integer t, where each R_i is either a principal ideal domain which is no field or a special local ring. In this case R is euclidean if and only if all R_i are euclidean. Finally, if R is euclidean then its smallest algorithm θ is given by

$$\theta(x) = \bigoplus_{i=1}^{t} \theta_i(x_i),$$

for $x = (x_i)_{i=1}^{t} \in \prod_{i=1}^{t} R_i = R$; here $\oplus$ denotes Hessenberg sum and θ_i is the smallest algorithm of R_i.

Proof. The first assertion follows from (1.7). For the decomposition of a principal ideal ring, see [4,Ch. IV, Sec. 15, Th.33]. The rest of (3.2) follows from (1.11), (1.10) and (2.3). □

(3.3) Proposition. Let R be a special local ring with maximal ideal $\underline{m} = R\pi$, and let $n \geq 0$ be minimal with $\pi^n = 0$. Then $R = \dot{\bigcup}_{i=0}^{n} R^* \cdot \pi^i$ (disjoint union), and R is euclidean with smallest algorithm

$$\theta_R(x) = i \quad \text{for} \quad x \in R^* \cdot \pi^i .$$

Proof. Straightforward (use (2.2)). □

By (3.2) and (3.3) the question, whether a commutative ring is euclidean and, if so, how its smallest algorithm looks like, is reduced to the case of a principal ideal domain. It is known that there exist principal ideal domains which are not euclidean ((7.4),(16.7),[5]).

The following proposition sharpens (2.5) in the commutative case.

(3.4) Proposition. Let R be a euclidean domain with smallest algorithm θ. Then $\theta(ab) \geqslant \theta(a) \oplus \theta(b)$ for all $a,b \in R - \{0\}$.

Proof. By induction on $\theta(ab)$. If $\theta(ab) < \theta(a) \oplus \theta(b)$ then, interchanging a and b if necessary, we may assume $\theta(ab) \leqslant \lambda \oplus \theta(b)$ for some $\lambda < \theta(a)$. Choose $r \in R - Ra$ such that $\theta(c) \geqslant \lambda$ for all $c \in r + Ra$ (by (2.1)(c)). Choose $cb \in rb + Rab$ such that $\theta(cb) < \theta(ab)$. Then $c \in r + Ra$ so $\theta(c) \geqslant \lambda$. Now we have

$$\theta(cb) < \theta(ab) \leqslant \lambda \oplus \theta(b)$$

while the inductive hypothesis asserts

$$\theta(cb) \geqslant \theta(c) \oplus \theta(b) \geqslant \lambda \oplus \theta(b).$$

This contradiction proves $\theta(ab) \geqslant \theta(a) \oplus \theta(b)$. □

We remark that for all known R to which (3.4) applies $\theta_R[R-\{0\}]$ consists only of finite ordinals. Since $\oplus$ and + coincide on finite ordinals, this means that no example is known in which (3.4) is actually sharper than (2.5).

Also, for all euclidean domains R for which θ is known there exists $k \in \mathbb{Z}_{\geqslant 0}$ such that

$$\theta(a) + \theta(b) \leqslant \theta(ab) \leqslant \theta(a) + \theta(b) + k$$

for all $a,b \in R - \{0\}$. I do not know how generally this is true.

(3.5) Proposition. Let R be a euclidean domain. Then

$$\theta_R(a) \geqslant \sum_{\underline{m}} \operatorname{ord}_{\underline{m}}(a) \qquad (a \in R, a \neq 0),$$

the sum ranging over the nonzero prime ideals $\underline{m}$ of R. Here $\mathrm{ord}_{\underline{m}}$ denotes the number of factors $\underline{m}$ in Ra.

Proof. Clear from (3.4) or (2.2) since $\theta_R(a) = 0$ only for $a \in R^*$. □

We note that any principal ideal domain R which satisfies the "second stable range condition"

$$R^* \to (R/Ra)^* \text{ is surjective for all } a \in R,$$

is a euclidean ring for which equality holds in (3.5). This includes the case of a semilocal principal ideal domain [2,prop.5]. Also for $R = k[X]$, where k is an algebraically closed field, we have equality in (3.5).

(3.6) Proposition. Let R be a euclidean domain with algorithm φ, and let $S \subset R - \{0\}$ be a multiplicatively closed subset. Then $S^{-1}R$ is euclidean with algorithm

$$\psi(x) = \min\{\varphi(sx) \mid s \in S, sx \in R\}.$$

Proof. [2, prop. 7]. □

4. Unique remainder algorithms.

Let M be a module over a ring R, and let W be a well ordered set. A map $\varphi: M \to W$ is called a unique remainder algorithm (u.r.a.) if for all $a,b \in M$ there exists a unique element $r \in a + R\cdot b$ which satisfies $r = 0$ or $\varphi(r) < \varphi(b)$.

Example: $R = M = k[X]$, with k a skew field, and φ = degree (where $\deg(0) = \omega$).

(4.1) Proposition. An algorithm $\varphi: M \to W$ is u.r.a. if and only if (i) and (ii) hold:

(i) $\forall\, x,y \in M$: $x \neq y \Rightarrow \varphi(x-y) \leqslant \max\{\varphi(x),\varphi(y)\}$,

(ii) $\forall\, x \in M$: $\forall\, q \in R$: $\varphi(x) \leqslant \varphi(qx)$.

Proof. "Only if". (i) Putting $a = x$ and $b = x-y$ we have $x, y \in a + Rb$ so by uniqueness we cannot have both $\varphi(x) < \varphi(b)$ and $\varphi(y) < \varphi(b)$. Hence $\varphi(x) \geqslant \varphi(b)$ or $\varphi(y) \geqslant \varphi(b)$, as required.

(ii) If $\varphi(qx) < \varphi(x)$ then $qx \neq 0$ by §1. But then $r = qx$ and $r = 0$ are two different elements of $0 + Rx$ which both satisfy

$$r = 0 \quad\text{or}\quad \varphi(r) < \varphi(x),$$

contradicting uniqueness.

"If". Suppose (i) and (ii) hold. We have to prove that

$$\begin{aligned} &r \equiv s \bmod Rb,\\ &r = 0 \text{ or } \varphi(r) < \varphi(b),\\ &s = 0 \text{ or } \varphi(s) < \varphi(b)\end{aligned}$$

implies $r = s$. In the case $r = 0$ we have $s \in Rb$, so $\varphi(s) \geqslant \varphi(b)$ by (ii), and $s = 0 = r$. Similarly the case $s = 0$ is treated. If both $\varphi(r) < \varphi(b)$ and $\varphi(s) < \varphi(b)$ then putting $r - s = qb$ we find

$$\max\{\varphi(r),\varphi(s)\} < \varphi(b) \leqslant \varphi(qb) = \varphi(r-s)$$

so (i) implies $r = s$. □

(4.2) Corollary. If φ is u.r.a. on M, then

$$\varphi(x) = \varphi(-x) \qquad \text{for all } x \in M,$$

and

$$\varphi(x+y) = \max\{\varphi(x),\varphi(y)\} \quad \text{if } \varphi(x) \neq \varphi(y),\ x \neq 0 \neq y.$$

Proof. $\varphi(x) = \varphi(-x)$ is clear from (4.1)(ii). Further, if $\varphi(x) > \varphi(y)$ then (i) implies

$$\varphi(y) < \varphi(x) \leqslant \max\{\varphi(x+y),\varphi(y)\}$$

and therefore

$$\varphi(x+y) \geqslant \varphi(x) = \max\{\varphi(x),\varphi(y)\}.$$

The other inequality is clear from (i) and $\varphi(-y) = \varphi(y)$. □

(4.3) Proposition. Let φ be u.r.a. on M such that $\varphi[M]$ is a beginning segment of the ordinal numbers. Then φ is equal to the smallest algorithm θ_M on M. Further, for $b \in M$ and $q \in R$ we have (cf.(2.4))

$$\theta_M(qb) = \theta_M(b) + \theta_{R/\mathrm{Ann}(b)}(q + \mathrm{Ann}(b)).$$

Proof. We check that $\varphi = \psi$ satisfies (2.1)(c). Let $b \in M$ and $\lambda \in W_M$ be such that $\lambda < \varphi(b)$. Choose $a \in M$ with $\varphi(a) = \lambda$. Then $a \notin Rb$, and since the only element r of $a + Rb$ satisfying $\varphi(r) < \varphi(b)$ is given by $r = a$, we have

$$\varphi(r) \geqslant \lambda \qquad \text{for all } r \in a + Rb.$$

This proves (2.1)(c) and we conclude $\varphi = \theta_M$.

Further, let $b \in M$. As in the proof of (2.4) there is an algorithm

$$\lambda\colon R/\mathrm{Ann}(b) \to W_M \text{ such that}$$

$$\theta_M(qb) = \theta_M(b) + \lambda(\bar{q})$$

where $\bar{q} = q + \mathrm{Ann}(b)$. We want to prove $\lambda = \theta_{R/\mathrm{Ann}(b)}$, and this will follow from the above once we know

(i) λ is u.r.a.;
(ii) the image of λ is a beginning segment of the ordinals.

Statement (i) is easily checked. To prove (ii), let $\bar{q} \in R/\mathrm{Ann}(b)$ and $\mu \in W_M$ satisfy $\mu < \lambda(\bar{q})$; we have to find $\bar{r} \in R/\mathrm{Ann}(b)$ such that $\lambda(\bar{r}) = \mu$.

From $\theta_M(b) + \mu < \theta_M(b) + \lambda(\bar{q}) = \theta_M(qb)$ we know that there exists

$c \in M$ such that $\theta_M(c) = \theta_M(b) + \mu$. If c is a multiple rb of b, then $\mu = \lambda(\bar{r})$ and we are done. If c is not in Rb, then $c = rb + d$ with $\theta_M(d) < \theta_M(b)$, and (4.2) implies $\theta_M(c) = \theta_M(rb)$ so again $\mu = \lambda(\bar{r})$. This finishes the proof of (ii). □

Note that (4.3) implies that any two u.r.a.'s on a module M are equivalent. In (4.5) we will see that essentially there are no other algorithms on M.

<u>(4.4) Corollary.</u> Let R be a ring without zero-divisors having a u.r.a. Then $\theta_R(ab) = \theta_R(b) + \theta_R(a)$ for all $a,b \in R$, $b \neq 0$. □

<u>(4.5) Proposition.</u> Let M be a module with u.r.a., and let $\psi\colon M \to W$ be a map, with W well ordered. Then ψ is an algorithm on M if and only if $\psi(a) < \psi(b)$ for all $a,b \in M$ for which $\theta_M(a) < \theta_M(b)$.

<u>Proof.</u> The "if"-part is obvious. "Only if". Suppose ψ is an algorithm, and suppose there are $a,b \in M$ with $\theta_M(a) < \theta_M(b)$ and $\psi(a) \geqslant \psi(b)$. Choose such a,b with $\psi(b)$ smallest possible. From $\theta_M(a) < \theta_M(b)$ we know $a \notin Rb$. Since ψ is an algorithm, there is $r \in a + Rb$ with $\psi(r) < \psi(b)$. Then $r \neq a$, so because θ_M is u.r.a. we have $\theta_M(r) \geqslant \theta_M(b)$. We conclude

$$\theta_M(a) < \theta_M(r), \qquad \psi(a) \geqslant \psi(r)$$

contradicting the minimality of $\psi(b)$ since $\psi(r) < \psi(b)$. □

In the rest of this section we determine all rings R with u.r.a. which are commutative or have no zero-divisors. References: [6,7,8,9,10,11,12,13].

<u>(4.6) Theorem.</u> Let R be a commutative ring. Then R has u.r.a. if and only if $R \cong k[X]$ for some field k, or R is a field, or $R \cong \underline{F}_2 \times \underline{F}_2$.

<u>Proof.</u> The "if"-part is easily checked. "Only if". Let $\theta = \theta_R$ and put $k = \{0\} \cup R^* = \{0\} \cup \{x \in R \mid \theta(x) = 0\}$, cf. (2.6). By (4.1)(i) , the set k is additively closed, so it is a field. Since R is a principal ideal ring, (3.2) tells us that either R is a principal ideal domain but no field, or R is a special local ring, or $R \cong R_1 \times R_2$ for certain nonzero rings R_1, R_2.

Case 1. R is a principal ideal domain but no field. Choose $x \in R - k$ with $\theta(x) = 1$; we claim $R = k[x]$. Suppose, in fact, that there exists $q \in R - k[x]$, and choose such a q with $\theta(q)$ smallest possible. Then $q = a\cdot x + c$ with $a,c \in R$ and $c = 0$ or $\theta(c) < \theta(x) = 1$. Clearly $c \in k$. Also $\theta(a\cdot x) \geqslant \theta(x)$ so from (4.2) we conclude $\theta(q) = \theta(a\cdot x)$. Using commutativity and (4.4) we find $\theta(q) = \theta(ax) = \theta(xa) = \theta(a) + \theta(x) > \theta(a)$. By the minimality of $\theta(q)$ it follows that $a \in k[x]$ and therefore also $q = ax + c \in k[x]$, contradiction. Hence $R = k[x]$, and since R is no field we have $R \cong k[X]$.

Case 2. R is a special local ring. Let $x \in \underline{m}$, then $x = (1+x)-1 \in k + k = k = \{0\} \cup R^*$, but $x \notin R^*$ so $x = 0$, and R is a field.

Case 3. $R = R_1 \times R_2$ with $R_1 \neq 0 \neq R_2$. If $u \in R_1^*$ then $(u,1) - (1,1)$ is in k but not in R^* so $(u,1) = (1,1)$ and $R_1^* = \{1\}$. Similarly $R_2^* = \{1\}$, so $R^* = \{1\}$ and $k = \underline{F}_2$. Let $x = (x_1,x_2) \in R$ satisfy $\theta(x) = 1$. Then $R \neq Rx$, and $k = \underline{F}_2$ surjects onto $R/Rx \cong (R_1/R_1x_1) \times (R_2/R_2x_2)$. Hence $R/Rx \cong \underline{F}_2$ and after re-indexing we may assume $R_1/R_1x_1 \cong \underline{F}_2$ and $R_2 = R_2x_2$. This implies $x_2 \in R^*$ so $x_2 = 1$.

Now let $y = x-1 = (x_1-1,0)$. Since $\theta(y) = 1$ by (4.2) we have in the same way $\underline{F}_2 \cong R/Ry \cong (R_1/R_1(x_1-1)) \times R_2$. We conclude $R_2 = \underline{F}_2$ and $x_1-1 \in R_1^* = \{-1\}$, so $x_1 = 0$ and $R_1 = R_1/R_1x_1 \cong \underline{F}_2$, as required. □

Let R be a ring, $\rho\colon R \to R$ a ring homomorphism and $\delta\colon R \to R$ a map satisfying $\delta(a+b) = \delta(a) + \delta(b)$ and $\delta(ab) = \rho(a)\delta(b) + \delta(a)b$ (a so-called "ρ-derivation"). Then the skew polynomial ring $R[X;\rho,\delta]$ consists of formal finite sums $\sum_{i\geqslant 0} r_iX^i$, with $r_i \in R$. Addition is performed in the usual componentwise manner, and the multiplication is determined by the multiplication in R and the rules

$$X\cdot X^i = X^{i+1} \qquad (i\geqslant 0)$$

$$X\cdot r = \rho(r)\cdot X + \delta(r) \qquad (r\in R).$$

It is straightforward to prove that this gives a ring. We say that $R[X;\rho,\delta]$ is a J-skew polynomial ring over R if ρ is injective and satisfies Jategaonkar's condition $\rho[R] \subset R^* \cup \{0\}$. If such a ρ exists then clearly R and $R[X;\rho,\delta]$ have no zero-divisors.

(4.7) Proposition. Suppose $S = R[X;\rho,\delta]$ is a J-skew polynomial ring over R, and let R have u.r.a. Then also S has u.r.a., and

$$\theta_S(0) = \omega\cdot\theta_R(0)$$

$$\theta_S(\Sigma_{i=0}^n r_iX^i) = n\cdot\theta_R(0) + \theta_R(r_n), \quad r_i \in R,\ r_n \neq 0,\ n \geqslant 0.$$

Proof. The multiplication is usual multiplication of ordinals ($2\cdot\omega = \omega+\omega$, and $\omega\cdot 2 = \omega$). Notice $\theta_R(0) > \theta_R(r)$ for all $r \in R - \{0\}$, so the term $n\cdot\theta_R(0)$ dominates.

We check that the function θ_S as defined in (4.7) is an algorithm on S. Let $f = \Sigma_{i=0}^n r_iX^i \in S$ with $r_n \neq 0$, and let $g \in S - Sf$. We have to find $h \in g + Sf$ with $\theta_S(h) < \theta_S(f)$. To this end, choose $h \in g + S\cdot f$ with $\theta_S(h)$ minimal. Write $h = \Sigma_{i=0}^m t_iX^i$ with $t_m \neq 0$. We distinguish three cases.

If $m < n$ then $\theta_S(h) < (m+1)\cdot\theta_R(0) \leqslant \theta_S(f)$ and we are done. If $m = n$ then the minimality of $\theta_S(h)$ and the fact that θ_R is an algorithm on R imply $\theta_R(t_m) < \theta_R(r_n)$ so again $\theta_S(h) < \theta_S(f)$. Finally, if $m > n$ then $h_1 = h - t_m\cdot(\rho^{m-n}(r_n))^{-1}\cdot X^{m-n}\cdot f$ satisfies $h_1 \in g + Sf$ and $\theta_S(h_1) < \theta_S(h)$, contradicting minimality of $\theta_S(h)$. We conclude that θ_S is an algorithm on S.

Using (4.1) it is immediate that θ_S is u.r.a., and from (4.3) it follows that θ_S is actually the smallest algorithm on S. □

Let τ be an ordinal number. A ring R is called a J-ring of type τ if there is a chain of subrings R_α, where α ranges over the ordinal numbers $\leqslant \tau$, such that:

(i) $R_0 = R^* \cup \{0\}$;

(ii) $R_{\alpha+1}$ is isomorphic to a J-skew polynomial ring over R_α, for all $\alpha < \tau$;

(iii) $R_\alpha = \bigcup_{\beta<\alpha} R_\beta$ for all limit ordinals $\alpha \leqslant \tau$;

(iv) $R = R_\tau$.

For example, a division ring is a J-ring of type 0, and a polynomial ring in one variable over a field is a J-ring of type 1. For every ordinal τ there do exist J-rings of type τ; for proofs, see [9,12].

The following result is slightly sharper than a theorem of Jategaonkar [10,11].

(4.8) Theorem. Let R be a ring. Then there exists an ordinal τ such that R is a J-ring of type τ if and only if R has a unique remainder algorithm and no zero-divisors.

Proof. The "only if" part is easy from (4.7) by tranfinite induction. Next let R be a ring without zero-divisors with u.r.a. $\theta = \theta_R$. Denote by Λ the collection of ordinals $\lambda \leqslant \theta_R(0)$ satisfying the condition

(4.9) if $\beta < \lambda$ and $\gamma < \lambda$ then $\beta + \gamma < \lambda$, and $\lambda > 0$.

Notice $\theta_R(0) \in \Lambda$ by (4.4). We claim

(4.10) $\lambda \in \Lambda$, $\beta < \lambda \Rightarrow \beta + \lambda = \lambda$.

To prove this, just notice that the unique solution γ of $\beta + \gamma = \lambda$ cannot be $< \lambda$, by (4.9), and clearly cannot be $> \lambda$, so that $\gamma = \lambda$ is the only possibility.

Index the elements of Λ by a beginning segment of the ordinals such that $\lambda_\alpha < \lambda_\beta$ if and only if $\alpha < \beta$. Let τ be determined by $\lambda_\tau = \theta_R(0)$. Define $R_\alpha \subset R$ by

$$R_\alpha = \{r \in R \mid \theta(r) < \lambda_\alpha\} \cup \{0\}, \qquad \alpha \leqslant \tau.$$

From (4.1) (i) and (4.4) it is clear that R_α is a subring of R. To prove (4.8) it suffices to check that (i), (ii), (iii) and (iv) are satisfied.

From (4.4) one easily deduces $R^* = \{r \in R \mid \theta(r) = 0\}$. This implies (i) since $\lambda_0 = 1$. Further (iv) is obvious and (iii) is clear from the easily proved relation

$$\lambda_\alpha = \lim_{\beta<\alpha} \lambda_\beta, \qquad \alpha = (\text{limit ordinal} \leqslant \tau).$$

We are left with (ii).

Choose $x \in R$ with $\theta(x) = \lambda_\alpha$. We claim that $R_{\alpha+1}$ equals $R_\alpha[x] = \{\Sigma_{i=0}^n r_i x^i \mid r_i \in R_\alpha, n \geqslant 0\}$ and that this is a J-skew polynomial ring over R_α.

For $f = \Sigma_{i=0}^{n} r_i x^i \in R_\alpha[x]$ with $r_i \in R_\alpha$ and $r_n \neq 0$ we conclude from (4.4), $\lambda_\alpha \in \Lambda$ and (4.2) that $\theta(f) = n \cdot \lambda_\alpha + \theta(r_n)$. This is smaller than λ_τ, so $f \neq 0$ and every element of $R_\alpha[x]$ has a unique representation as a finite sum $\Sigma r_i x^i$ with $r_i \in R_\alpha$.

Let $r \in R_\alpha$, $r \neq 0$. Since θ is u.r.a., there are unique $\rho(r) \in R$, $\delta(r) \in R$ with $xr = \rho(r)x + \delta(r)$ and either $\delta(r) = 0$ or $\delta(r) < \theta(x) = \lambda_\alpha$. Clearly $\delta(r) \in R_\alpha$, and putting $\delta(0) = 0$ we have a map $\delta\colon R_\alpha \to R_\alpha$. We claim $\rho(r) \in R^* \subset R_\alpha$. In fact, (4.4) and (4.10) imply $\theta(xr) = \theta(r) + \theta(x) = \theta(x)$ so (4.2) gives $\theta(\rho(r)x) = \theta(x)$ which by (4.4) means $\theta(\rho(r)) = 0$. Hence $\rho(r) \in R^* \subset R_0 \subset R_\alpha$. It follows that $R_\alpha[x]$ is a ring.

Putting $\rho(0) = 0$ and using the distributive and associative laws one proves easily that $\rho\colon R_\alpha \to R_0$ is an injective ring homomorphism and that $\delta\colon R_\alpha \to R_\alpha$ is a ρ-derivation. It is clear that $R_\alpha[x]$ is isomorphic to the J-skew polynomial ring $R_\alpha[X;\rho,\delta]$.

To finish the proof of (ii) we must show $R_\alpha[x] = R_{\alpha+1}$. Clearly $\subset$ since $x \in R_{\alpha+1}$. To prove the opposite inclusion we first note that $\lambda = \omega \cdot \lambda_\alpha$ is the smallest ordinal $> \lambda_\alpha$ which satisfies (4.9); hence $\lambda_{\alpha+1} = \omega \cdot \lambda_\alpha$. Now suppose $f \in R_{\alpha+1} - R_\alpha[x]$; we may assume $\theta(f)$ is smallest possible. Write $f = a \cdot x + b$ with $b \in R_\alpha$. As before, $\theta(f) = \theta(x) + \theta(a) = \lambda_\alpha + \theta(a)$, since $a \neq 0$. But $\theta(f) < \lambda_{\alpha+1}$ implies that we can write $\theta(f) = n \cdot \lambda_\alpha + \beta$ with $\beta < \lambda_\alpha$ and $1 \leq n < \omega$. Then $\theta(a) = (n-1)\lambda_\alpha + \beta < n \cdot \lambda_\alpha \leq \theta(f)$ so $a \in R_\alpha[x]$ by the minimality of $\theta(f)$. We conclude $f = ax + b \in R_\alpha[x]$, contradiction. This proves (ii). □

Notice that the type τ and the chain of subrings $(R_\alpha)_{\alpha \leq \tau}$ are uniquely determined by the ring R. In fact, they can be read off from the smallest algorithm as has been done in the above proof.

Finally, we remark that a simple module M over an arbitrary ring R always has u.r.a.

5. Laurent series.

Let R be a ring, and $Q = R\,[[X]]\,[X^{-1}]$ the ring of formal Laurent series with coefficients in R (we let X commute elementwise with R). For

$$f = \sum_{i \geq h} a_i X^i \in Q, \quad a_i \in R, \quad h \in \underline{Z}, \quad a_h \neq 0$$

we put $\psi(f) = a_h$, and $\psi(0) = 0$. So ψ is a function from Q to R.

(5.1) Theorem (Samuel). If R is euclidean then so is Q. More precisely, if φ is an algorithm on R then $\varphi\ \psi$ is an algorithm on Q.

Proof. [2, prop. 8]. □

(5.2) Theorem (F. Dress, [14]). Suppose R has no zero-divisors. Then if Q is euclidean, also R is euclidean. More precisely, if φ is an algorithm on Q, then an algorithm on R is given by

$$\chi\ (r) = \min\ \{\varphi\ (f)\ \mid\ f \in Q,\ \psi\ (f) \in Rr\}.$$

Finally, the smallest algorithm θ_Q on Q is given by $\theta_Q = \theta_R \cdot \psi$.

Proof. We show that χ is an algorithm. Let a, b $\in$ R, a $\notin$ Rb, we look for $s \in a + Rb$ with $\chi(s) < \chi(b)$. Clearly we may assume $b \neq 0$. Choose $f \in Q$ such that $\psi(f) \in Rb$ and such that $\varphi(f)$ is smallest possible. Then $\chi(b) = \varphi(f)$.

Choose $r \in a + Q \cdot f$ with $\varphi(r) < \varphi(f)$ (it is easy to see that $r=0$ cannot happen). We can write

$$r = a+qf = a + \sum_{i \geq h} a_i X^i, \quad a_h \neq 0,$$

where $a_h \in Rb$ since R has no zero-divisors. If $h < 0$ then $\psi(r) = a_h \in Rb$; but this contradicts the choice of f since $\varphi(r) < \varphi(f)$.

Hence we have $h \geq 0$ and $a \equiv \psi(r) \bmod Rb$. Clearly $\chi(\psi(r)) \leq \varphi(r) < \varphi(f) = \chi(b)$ so we can take $s = \psi(r)$. This proves that χ is an algorithm on R.

It follows that

$$\theta_R\ (r) \leqslant \chi\ (r) \qquad (r \in R)$$

so

$$\theta_R\ (\psi(f)) \leqslant \chi\ (\psi(f)) \quad (f \in Q)$$

while the definition of χ implies

$$\chi\ (\psi(f)) \leqslant \varphi\ (f).$$

We conclude $\theta_R\psi\ (f) \leqslant \varphi\ (f)$ for all $f \in Q$ and for all algorithms φ on Q. But $\theta_R\psi$ is itself an algorithm on Q by (5.1), so $\theta_R\psi = \theta_Q$. $\square$

Using (3.2) one easily derives:

(5.3) Corollary. Suppose that R is commutative and that Q is euclidean. Then R is euclidean, and $\theta_Q = (\theta_R \cdot \psi)_*$ (in the notation of (1.8)). $\square$

We note that the construction of Laurent series rings can be repeated transfinitely often. The above results then carry over without difficulty.

6. Matrix rings.

This section contains some results on euclidean matrix rings, without detailed proofs. For a ring R and a positive integer n we denote the ring of n x n matrices over R by M(n,R).

(6.1) Theorem (cf. Brungs, [15]). Let $n \geqslant 1$. If R is left euclidean then so is M(n,R). If R is right euclidean, then so is M(n,R). If R is two-sided euclidean then so is M(n,R).

Proof. Let R be left euclidean and let φ be an algorithm on R assuming ordinal values. Then for every matrix $b \in M(n,R)$ there exists $u \in M(n,R)^*$ such that ub is upper triangular, i.e. $u \cdot b = [d_{ij}]_{1 \leq i,j \leq n}$, with $d_{ij} \in R$, $d_{ij} = 0$ for $i>j$.

Define ψ on M(n,R) by

$$\psi(b) = \min \{ \bigoplus_{i=1}^{n} \varphi(d_{ii}) \mid \text{there exists } u \in M(n,R)^* \text{ such that}$$
$$u \cdot b = [d_{ij}]_{1 \leq i,j < n} \text{ is upper triangular}\},$$

where $\oplus$ denotes Hessenberg sum. We leave it to the reader to verify that ψ is an algorithm on M(n,R), thus proving the first assertion of (6.1). The second one follows immediately. For the proof of the last statement one has to take

$$\psi(b) = \min \{ \bigoplus_{i=1}^{n} \varphi(d_{ii}) \mid \text{there exist } u,\ v \in M(n,R)^* \text{ such that}$$
$$ubv = [d_{ij}]_{1 \leq i,j \leq n} \text{ is upper triangular}\},$$

where φ is a two-sided algorithm on R assuming ordinal values. □

If k is a field then the proof of (6.1) shows that

$$\psi(b) = n - \text{rank}(b)$$

is an algorithm on M(n,k). It is not hard to show that it is the smallest algorithm on M(n,k).

(6.2) Theorem. Let R be a commutative principal ideal ring, and $n \geqslant 2$. Then $M(n,R)$ is two-sided euclidean.

Proof. Using (3.2), (3.3) and (6.1) we reduce to the case R is a principal ideal domain but no field. In that case, let $\ell(d)$ denote the Jordan-Hölder length of the R-module R/Rd, for $d \in R-\{0\}$, and let $\ell(0) = \omega$. So ℓ is a function from R to $W = \{0,1,2,\ldots,\omega\}$.

Well-order W^n by defining $(\alpha_i)_{i=1}^n$ to be smaller than $(\beta_i)_{i=1}^n$ if $\alpha_j < \beta_j$ for $j = \min\{i \,|\, \alpha_i \neq \beta_i\}$. We define a function $\varphi: M(n,R) \to W^n$. For $b \in M(n,R)$ there exist $u,v \in M(n,R)^*$ such that $u\, b\, v$ is a diagonal matrix

$$u\, b\, v = [d_{ij}]_{1\leqslant i,j\leqslant n}, \qquad d_{ij} = 0 \text{ for } i \neq j,$$

which moreover satisfies

$$d_{ii} \equiv 0 \bmod Rd_{jj} \qquad \text{for } 1\leqslant j\leqslant i\leqslant n.$$

Further, the sequence of ideals $(Rd_{ii})_{i=1}^n$ is uniquely determined by b. We define

$$\varphi(b) = (\ell(d_{ii}))_{i=1}^n \in W^n.$$

The proof that φ is an algorithm rests on the following lemma and is left to the reader. □

(6.3) Lemma. Let R be a principal ideal domain, and $a, d \in R$, $d \neq 0$. Let $Ra + Rd = Rb$. Then there exists $t \in R$ such that $Rt + Rd = R$ and $ta \equiv b \bmod Rd$. □

Let R be a principal ideal domain which is no field. For certain R we can determine the smallest algorithm on $M(n,R)$. For $b \in M(n,R)$, put

$$\ell(b) = \bigoplus_{i=1}^{n} \ell(d_{ii})$$

where ℓ, d_{ii} are as in the proof of (6.2). It is not hard to prove (e.g. using (2.2)) that $\psi(b) \geqslant \ell(b)$ for every ordinal-valued algorithm ψ on $M(n,R)$. Hence if ℓ is an algorithm, it is the smallest one. Without proof we mention:

(6.4) Theorem. Let R be a principal ideal domain which is no field, and let $n \geqslant 1$. Then ℓ is an algorithm on $M(n,R)$ if and only if R and n satisfy the following condition:

(6.5) for all $b \in R$, $b \neq 0$ and all $a \in R-Rb$ there exists $r \in a + Rb$ such that $\ell(r) < n \cdot \ell(b)$. □

Examples. Condition (6.5) is satisfied in the following cases:

(a) $n \geqslant 1$ and ℓ is an algorithm on R (cf. § 3), e.g. $R = k[X]$ where k is an algebraically closed field.

(b) $n \geqslant 2$ and R is the ring of integers in an algebraic number field of class number one (by Dirichlet's theorem on primes in arithmetic progressions).

(c) $n \geqslant 2$ and $R = k[X]$ where k is a real closed field.

7. Subrings of global fields.

Let F be a global field, i.e. a finite extension of $\mathbb{Q}$ or a function field in one variable over a finite field, and let S be a finite non-empty set of prime divisors of F, including the set S_∞ of archimedean primes of F. By $\underline{O}_S$ we mean the ring of S-integers of F, i.e.

$\underline{O}_S = \{x \in F \mid |x|_{\underline{p}} \leq 1$ for all primes $\underline{p}$ of F with $\underline{p} \notin S\}$.

Suitably normalizing the absolute values we have

$$\#(\underline{O}_S/\underline{O}_S x) = \prod_{\underline{p}\notin S} |x|_{\underline{p}}^{-1} = \prod_{\underline{p}\in S} |x|_{\underline{p}}$$

for $x \in \underline{O}_S$, $x \neq 0$. Hence the S-norm $N_S\colon F^* \to \underline{R}_{>0}$, defined by

$$N_S\ (x) = \prod_{\underline{p}\in S} |x|_{\underline{p}}$$

assumes positive integer values on $\underline{O}_S - \{0\}$. We call $\underline{O}_S$ norm-euclidean if N_S is an algorithm (of type 1, see §1) on $\underline{O}_S$.

We are interested in the relationship between the following three assertions:

(7.1) $\underline{O}_S$ is a principal ideal domain;

(7.2) $\underline{O}_S$ is euclidean;

(7.3) $\underline{O}_S$ is norm-euclidean.

Of course, (7.3) implies (7.2) and (7.2) implies (7.1).

Moreover, if $\underline{O}_S$ is euclidean we are interested in its smallest algorithm.

It turns out that the situation much depends on the number of units in $\underline{O}_S$. It is known that $\underline{O}_S^*$ is isomorphic to the direct sum of a finite cyclic group and a free abelian group of rank $\#S-1$. So $\underline{O}_S^*$ is finite if and only if $\#S=1$.

First, let $\underline{O}_S^*$ be finite. Then $N_S = |\ |_{\underline{p}}$ if $S=\{\underline{p}\}$, so N_S is an absolute value on F. All euclidean $\underline{O}_S$ can be determined easily [1,2] and it turns out that they are all norm-euclidean (§8). Since also all $\underline{O}_S$ which are principal ideal domains are known in this case [16, 17], we can form the difference to obtain [18]:

(7.4) Theorem. Let $\underline{O}_S$ be as above. Then $\underline{O}_S$ is a non-euclidean principal ideal domain with only finitely many units if and only if $\underline{O}_S$ is isomorphic to one of the following rings:

$$\underline{Z}\left[\frac{1}{2}(1+\sqrt{-d})\right], \quad d = 19,\ 43,\ 67 \text{ or } 163;$$

$$\underline{F}_2[X,Y] \,/\, (Y^2+Y+X^3+X+1);$$

$$\underline{F}_2[X,Y] \,/\, (Y^2+Y+X^5+X^3+1);$$

$$\underline{F}_3[X,Y] \,/\, (Y^2-X^3+X+1);$$

$$\underline{F}_4[X,Y] \,/\, (Y^2+Y+X^3+\alpha) \qquad \text{where } \alpha \in \underline{F}_4-\underline{F}_2. \qquad \square$$

In the function field case the only euclidean rings $\underline{O}_S$ with $\# S=1$ turn out to be the polynomial rings $\underline{F}_q[X]$. These rings and their algorithms have been discussed in § 4. The number field case will be considered in sections 9-11.

Secondly, consider rings $\underline{O}_S$ with $\underline{O}_S^*$ infinite. It has been proved by Weinberger [19] and Queen [18], modulo certain generalized Riemann hypotheses, that in this case $\underline{O}_S$ is a principal ideal domain if and only if it is euclidean (§ 13). But there exist many principal ideal domains $\underline{O}_S$ which are not norm-euclidean (examples: $\underline{Z}[\sqrt{14}]$, $\underline{F}_3[X,\sqrt{X^4-X^2-1}]$) , so (7.1) and (7.3) are not equivalent.

In the function field case the necessary Riemann hypotheses have been proved [20,21], so there are indeed rings $\underline{O}_S$ satisfying (7.2) but not (7.3). In the number field case however such examples are unknown. Possibly one might find them by using slightly disturbed norm functions as in § 9.

A theorem of O'Meara [22] asserts that for every global field F there exists S such that $\underline{O}_S$ is norm-euclidean. A quantitative version of the number field case of this theorem is proved in section 14. In section 15 we discuss shortly the number fields whose rings of integers (i.e. $\underline{O}_S$ with $S=S_\infty$) are known to be euclidean. The function field case of O'Meara's theorem is included in section 16.

8. Absolute value algorithms.

Let R be a domain with field of fractions F. We consider a function $d: R \to \underline{R}_{\geq 0}$ which satisfies

(8.1) $d(r) = 0 \iff d(r) < 1 \iff r = 0 \qquad (r \in R);$

(8.2) $d(rs) = d(r)\, d(s) \qquad (r,s \in R);$

(8.3) there is a constant C, not depending on r and s, such that

$$d(r+s) \leq C \max\{d(r), d(s)\} \qquad (r,s \in R).$$

So d induces an "absolute value" on F which on R - {0} is ≥ 1. We are interested in when d is an algorithm (of type 2) on R. For this it is clearly necessary that R is euclidean and that d(r) = 1 only for $r \in R^*$. It turns out that these conditions are also sufficient and that, in fact, a complete list of examples can be given.

(8.4) Theorem. Let R be a domain which is no field and let $d: R \to \underline{R}_{\geq 0}$ satisfy (8.1), (8.2), (8.3). Then the following four assertions are equivalent.

(a) d is an algorithm on R (this includes that $d[R] \subset \underline{R}$ is well ordered).

(b) R is euclidean, and $d(r) > 1$ for every non-unit $r \in R - \{0\}$.

(c) R is a Dedekind domain, and there exists $x \in R$ with $d(x) > 1$ such that R^* maps surjectively onto $(R/Rx) - \{0\}$.

(d) Either $R \cong k[X]$ for some field k and $d(f) = c^{\deg(f)}$ for some $c > 1$ and all $f \neq 0$, or R is isomorphic to one of the rings $\underline{Z}$, $\underline{Z}[\sqrt{-e}]$ (e = 1,2), $\underline{Z}[\frac{1}{2}(+\sqrt{-e})]$ (e = 3,7,11), and $d(x) = |x|^c$ for some $c > 0$ and all x.

Proof. (a) $\Rightarrow$ (b) is obvious as noted above; (b) $\Rightarrow$ (c) is clear from (1.7) and (2.6); (d) $\Rightarrow$ (a) is easily checked (cf. section 10). We prove (c) $\Rightarrow$ (d).

We recall the theorem of Artin and Whaples [23, Ch. 12]. Suppose we have a field F and a non-empty set of non-equivalent non-trivial absolute values $|\ |_{\underline{q}}$ on F, where $\underline{q}$ ranges over some index set $\underline{M}$. Put $k = \{x \in F \mid |x|_{\underline{q}} \leq 1 \text{ for all } \underline{q} \in \underline{M}\}$. Clearly k is a subfield of F if and only if all $|\ |_{\underline{q}}$ are non-archimedean. Assume that the following three conditions are satisfied:

(8.5) $\forall x \in F^*$: $|x|_{\underline{q}} = 1$ for all but finitely many $\underline{q} \in \underline{M}$;

(8.6) $\forall x \in F^*$: $\prod_{\underline{q} \in \underline{M}} |x|_{\underline{q}} = 1;$

(8.7) there exists a "reasonable" prime $\underline{q} \in \underline{M}$.

Here $\underline{q} \in \underline{M}$ is called reasonable if it satisfies one of the follwing three conditions: (i) $\underline{q}$ is archimedean; (ii) $\underline{q}$ is discrete with finite residue class field; (iii) $\underline{q}$ is discrete, k is a field and the residue class field of $\underline{q}$ is finite dimensional over k.

In this situation, the theorem of Artin and Whaples asserts: <u>either</u> some $\underline{q} \in \underline{M}$ is archimedean, and then F is a finite extension of $\underline{Q}$, <u>every</u> absolute value of F is equivalent to $|\ |_{\underline{p}}$ for some $\underline{p} \in \underline{M}$, and there is a constant $c > 0$ such that the choice of **the** absolute values is the c-th power of the usual one making the product formula valid;
<u>or</u> k is a field, and then F is finite over k(r) for every $r \in F - k$, <u>every</u> absolute value of F which is trivial on k is equivalent to $|\ |_{\underline{p}}$ for some $\underline{p} \in \underline{M}$, and again the absolute values are as usual except for a positive exponent not depending on $\underline{p}$.

Further we need the following Hahn-Banach-type lemma, the proof of which may be left to the reader.

<u>(8.8) Lemma.</u> Let $H \subset G$ be abelian groups and let $T \subset G$ be an additively closed subset. Suppose $f: H \to \underline{R}$ is a group homomorphism such that $f(t) \geqslant 0$ for all $t \in T \cap H$. Then there exists a group homomorphism $g: G \to \underline{R}$ such that $g|H = f$ and such that $g(t) \geqslant 0$ for all $t \in T$. □

We turn to the proof of (8.4), (c) $\Rightarrow$ (d). Assume (c). Extend d to the field of fractions F of R by multiplicativity. Clearly $d(r) = 1$ for $r \in R^*$ so d induces a group homomorphism $d: H \to \underline{R}_{>0}$, where H is the group of principal fractional R-ideals. Apply lemma (8.8) to G = {all fractional R-ideals}, T = {nonzero ideals of R} and f = log d. Then we find a homomorphism, again denoted by d, from G to $\underline{R}_{>0}$ which satisfies

$$d(\underline{p}) \geqslant 1 \quad \text{for every maximal ideal } \underline{p} \subset R;$$

$$d(a) = \prod_{\underline{p}} d(\underline{p})^{\mathrm{ord}_{\underline{p}}(a)} \quad \text{for all } a \in F^*,$$

where $\underline{p}$ runs over the maximal ideals of R. Now we apply Artin-Whaples with

$$\underline{M} = \{\infty\} \cup \{\underline{p} \mid \underline{p} \subset R \text{ is maximal and } d(\underline{p}) > 1\}$$

$$|a|_{\infty} = d(a)$$

$$|a|_{\underline{p}} = d(\underline{p})^{-\mathrm{ord}_{\underline{p}}(a)}.$$

Clearly, conditions (8.5) and (8.6) are satisfied. We now distinguish two cases.

Case 1. $|\;|_\infty$ is archimedean. Then (8.7) is satisfied, and Artin-Whaples asserts that F is a number field every absolute value of which is equivalent to $|\;|_{\underline{q}}$ for some $\underline{q} \in \underline{M}$. First of all, this implies that F has only one archimedean absolute value, so $F = \underline{Q}$ or $F = \underline{Q}(\sqrt{-e})$ for some squarefree positive integer e. Secondly, all maximal ideals of R must be in $\underline{M}$, so

$$R = \{x \in F \mid |x|_{\underline{q}} \leqslant 1 \text{ for all } q \in \underline{M} - \{\infty\}\}$$

and therefore R is the integral closure of $\underline{Z}$ inside F.

If $F = \underline{Q}$ or $F = \underline{Q}(\sqrt{-1})$ or $F = \underline{Q}(\sqrt{-3})$ we are done. So let $F = \underline{Q}(\sqrt{-e})$, e as above, $e \neq 1$, $e \neq 3$. Then $R^* = \{\underline{+}1\}$ so the element **x** of (8.4)(c) satisfies $\#(R/Rx) \in \{2,3\}$.

If $e \not\equiv -1 \bmod 4$ then $x = a + b\sqrt{-e}$ with $a,b \in \underline{Z}$, and $a^2 + eb^2 = \#(R/R\mathbf{x}) \in \{2,3\}$ clearly implies $e = 2$.

If $e \equiv -1 \bmod 4$ then $2\mathbf{x} = a + b\sqrt{-e}$, with $a,b \in \underline{Z}$, $a \equiv b \bmod 2$, and $a^2 + eb^2 = 4\cdot\#(R/Rx) = 8$ or 12 yields $e \leqslant 12$ so $e = 7$ or $e = 11$.

So in case 1 we indeed have one of the six number rings mentioned in (8.4)(d), and $d = |\;|_\infty$ is the unique archimedean absolute value on F, up to equivalence.

Case2. $|\;|_\infty$ is non-archimedean. Then $k = \{a \in F \mid |a|_{\underline{q}} \leqslant 1 \text{ for all } q \in \underline{M}\}$ is a field containing $R^* \cup \{0\}$. Let **x** be as in (8.4)(c) and let $\underline{r}$ be the ideal R**x** of R. Clearly, (8.4)(c) implies that $\underline{r}$ is maximal and belongs to $\underline{M}$. Let $R_{\underline{r}}$ denote the localization of R at $\underline{r}$. We have $k \subset R_{\underline{r}}$, and since k is a field the two natural maps

$$R^* \cup \{0\} \to k \to R_{\underline{r}}/\underline{r}R_{\underline{r}}$$

are injective. But we also know that

$$R^* \cup \{0\} \to R/Rx \cong R_{\underline{r}}/\underline{r}R_{\underline{r}}$$

is surjective. We conclude that all these maps are bijective, so

$$k = R^* \cup \{0\} \subset R$$

and $k \cong R_{\underline{r}}/\underline{r}R_{\underline{r}}$. Hence the residue class field of $\underline{r}$ has dimension one over k, and condition (8.7) is satisfied.

We conclude that F is finite over $k(x)$, and that every absolute value on F which is trivial on k is equivalent to $|\ |_{\underline{q}}$ for some $q \in \underline{M}$. The divisor of x is

$$(x) = \infty^{-1} \cdot \underline{r}.$$

Since the "zero part" $\underline{r}$ has degree 1 it follows by a well known formula [24, Ch.I,§8,Th.4] that $[F:k(x)] = 1$ so $F = k(x)$. Further $k[x] \subset R$ and equality follows for numerous reasons. Finally, one easily proves $d(f) = d(x)^{\deg(f)}$ for $f \in R - \{0\}$. This proves (8.4). □

Further references: [25,13].

9. Algorithms on $\underline{Z}$.

In this section all algorithms are understood to be of type 1.

(9.1) Theorem. Let W be a well ordered set and $\varphi : \underline{Z} - \{0\} \to W$ a map. Then φ is an algorithm on $\underline{Z}$ if and only if

$$\forall\, r > 0,\ s > 0:\ \min\,\{\varphi\,(r),\ \varphi\,(-s)\} < \min\,\{\varphi\,(r+s),\ \varphi\,(-r-s)\}.$$

Proof. "If". Let $b \in \underline{Z}$, $b \neq 0$, $a \in \underline{Z} - \underline{Z}\cdot b$. Let r be the smallest positive element in the residue class $a + \underline{Z}\cdot b$, and $-s$ the largest negative one. Then $r+s = \pm\, b$ so we have $\min\,\{\varphi\,(r), \varphi\,(-s)\} < \varphi\,(b)$. Hence at least one of $t=r$ and $t=-s$ satisfies $t \in a + \underline{Z}\cdot b$ and $\varphi(t) < \varphi(b)$, and φ is an algorithm.

"Only if". Assume that φ is an algorithm, and consider a triple (r,s,b) of integers such that

(9.2) $\qquad r > 0, \quad s > 0, \quad r+s = |b|.$

To prove (9.1), it suffices to show

(9.3) $\qquad \varphi\,(r) < \varphi\,(b) \quad \text{or} \quad \varphi\,(-s) < \varphi\,(b).$

This is done with induction on $\varphi\,(b)$. So assume that the assertion is true for all triples (r',s',b') as above for which $\varphi\,(b') < \varphi\,(b)$.

If $\varphi\,(-b) < \varphi\,(b)$, the induction hypothesis, applied to the triple $(r,s,-b)$, yields $\varphi\,(r) < \varphi\,(-b)$ or $\varphi\,(-s) < \varphi\,(-b)$, and (9.3) follows. Therefore assume $\varphi\,(-b) \geqslant \varphi\,(b)$, so

(9.4) $\qquad \varphi\,(|b|) \geqslant \varphi\,(b), \qquad \varphi\,(-|b|) \geqslant \varphi\,(b).$

Now choose $d \in r + \underline{Z}\cdot b = -s + \underline{Z}\cdot b$ such that $\varphi\,(d)$ is minimal (note that 0 is not in this residue class, by (9.2)). Since φ is an algorithm, we have

(9.5) $\qquad \varphi\,(d) < \varphi\,(b).$

We distinguish three cases:

(i) $d > |b|$

(ii) $d < -|b|$

(iii) $d \in \{r, -s\}$.

In case (iii), (9.3) follows from (9.5). In each of the cases (i) and (ii) we derive a contradiction.

Case (i). The triple $(r',s',b') = (d-|b|, |b|, d)$ has the properties corresponding to (9.2). By (9.5) we may apply the induction hypothesis, which says

$$\varphi(d-|b|) < \varphi(d) \quad \text{or} \quad \varphi(-|b|) < \varphi(d).$$

But the first possibility is excluded by the minimality assumption on $\varphi(d)$, and the second one by (9.5) and (9.4).

Case (ii). Applying the induction hypothesis to the triple $(r',s',b') = (|b|, -d-|b|, d)$ we get

$$\varphi(|b|) < \varphi(d) \quad \text{or} \quad \varphi(d+|b|) < \varphi(d).$$

The first possibility would contradict (9.5) or (9.4), the second one our choice of d. □

The proof shows that (9.1) can be reformulated as follows:

<u>(9.6)</u> for every algorithm φ on $\underline{Z}$ we have

$$\forall\, b \in \underline{Z}-\{0\}: \forall\, a \in \underline{Z}-\underline{Z}b: \exists\, r \in a+\underline{Z}\cdot b:$$
$$\varphi(r) < \varphi(b) \wedge |r| < |b|.$$

So $|\ |$ plays a dominating role among all algorithms, although it is not the smallest algorithm (cf. § 10). Note that (9.6) also holds if $\underline{Z}$ is replaced by $k[X]$ (for a field k) and $|\ |$ by deg (cf. (4.5)). But the assertion is false if $\underline{Z}$ is replaced by $\underline{Z}[\sqrt{-1}]$. For the five imaginary quadratic number rings mentioned in (8.4) (d) no analogue of (9.1) is known.

From (4.5) and (9.1) it follows that for $R = k[X]$ and for $R = \underline{Z}$ the following statement holds. Let W be any well ordered set and let $\varphi: R-\{0\} \to W$ be a map which is <u>no</u> algorithm. Then there exists a finite subset $E \subset R-\{0\}$ such that there exists no algorithm $\psi: R-\{0\} \to W$ with $\psi\,|\,E = \varphi\,|\,E$. It is not known how generally this is true.

Next we consider <u>multiplicative</u> algorithms. An algorithm $\varphi: R-\{0\} \to W$ is called multiplicative if $W \subset \underline{\mathbb{R}}$ and $\varphi(a\,b) = \varphi(a)\,\varphi(b)$ for all $a,b \in R-\{0\}$ (here R is a domain). One easily proves:

(9.7) Proposition. Let R be a domain, and let $\varphi : R - \{0\} \to \mathbb{R}_{>0}$ be a map with well ordered image such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R - \{0\}$. Extend φ to the field of fractions F of R by multiplicativity and $\varphi(0) = 0$. Then φ is an algorithm on R if and only if for every $x \in F$ there exists $y \in R$ such that $\varphi(x-y) < 1$. $\square$

An example of a multiplicative algorithm on $\mathbb{Z}$ different from the usual absolute value is the following one. Let p be a fixed prime number and $q > p$ a real number. Then the unique function $\varphi : \mathbb{Z} - \{0\} \to \mathbb{R}$ for which

$$\begin{aligned} \varphi(r) &= r \quad \text{for every prime number } r \neq p, \\ \varphi(p) &= q, \\ \varphi(-1) &= 1, \\ \varphi(ab) &= \varphi(a)\varphi(b) \qquad (a,b \in \mathbb{Z}-\{0\}) \end{aligned}$$

is easily checked to be a multiplicative algorithm on $\mathbb{Z}$ (e.g., using (9.1)).

Analogously, one finds "exotic" multiplicative algorithms on $\mathbb{Z}[\sqrt{-1}]$, by taking the usual absolute value and adding extra weight to one prime π; in the case of $\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$ one can even add weight to two primes π_1 and π_2. This is easily derived from (9.7) and the following assertion, which holds for $R = \mathbb{Z}$, $n = 2$, for $R = \mathbb{Z}[\sqrt{-1}]$, $n = 2$, and for $R = \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$, $n = 3$: For every $x \in \mathbb{Q}\cdot R - R$ there exist elements $y_i \in x + R$, $1 \leq i \leq n$, such that

$$|y_i| < 1, \quad \text{for} \quad 1 \leq i \leq n,$$

$$y_i - y_j \in R^*, \quad \text{for} \quad 1 \leq i < j \leq n.$$

If in the case $\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$ one adds extra weight to two primes π_1 and π_2 which do not lie over the same rational prime, then one finds a multiplicative algorithm on $\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$ whose restriction to $\mathbb{Z}$ is not an algorithm on $\mathbb{Z}$.

In the case $R=\underline{Z}$ we prove below that the multiplicative algorithms described above are essentially the only exotic ones. The analogous result for $\underline{Z}[\sqrt{-1}]$ and $\underline{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$ is not known.

(9.8) Theorem. (A.E. Brouwer , H.W. Lenstra jr.) Let $\varphi:\underline{Z}-\{0\} \to W\subset \underline{R}$ be a multiplicative algorithm. Then there exist a prime number p and real numbers $A>0$, $B\geqslant 0$ such that

$$(9.9) \qquad \varphi(a) = |a|^A \cdot a_p^B \qquad \text{for all } a \in \underline{Z}-\{0\}$$

where a_p denotes the largest power of p dividing a. Conversely, if p is prime and $A>0$, $B\geqslant 0$ are real numbers, then the function φ defined by (9.9) is a multiplicative algorithm on $\underline{Z}$. Finally, φ assumes only integral values if and only if $A \in \underline{Z}_{>0}$ and $p^{A+B} \in \underline{Z}$.

Proof. We have already seen that φ is an algorithm if (9.9) holds ($A>0$, $B\geqslant 0$). Further the integrality assertion at the end of the theorem follows by repeatedly forming differences, cf. [Amer. Math. Monthly 80 (1973), pp.170,175]. So it suffices to prove the first assertion of (9.8), and that is done by an argument due to R. Sattler.

For $a \in \underline{Z}-\{0\}$ we clearly have $\varphi(a) = \varphi(-a)$. Hence theorem (9.1) and multiplicativity yield

$$\varphi(a+b) > \min{}'\{\varphi(a), \varphi(b)\}$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

for all $a>0$, $b>0$. It follows that $\varphi(a)>1$ for all $a\geqslant 2$, so if we define $\psi(a)$ by

$$\varphi(a) = a^{\psi(a)}, \qquad a\geqslant 2,$$

then $\psi(a)$ is positive. Let

$$\alpha = \inf \{\psi(a) \mid a\geqslant 2\}.$$

Clearly $\alpha\geqslant 0$. Now there are two cases. Either there is at most one prime p with

$$\psi(p)>\alpha,$$

and in that case we have

$$\varphi(a) = |a|^\alpha \quad \text{(if there is no such p)},$$
$$\varphi(a) = |a|^\alpha \cdot a_p^{\psi(p)-\alpha} \quad (\text{if } \psi(p)>\alpha)$$

for all $a \in \underline{Z} - \{0\}$, which clearly solves the problem. Or there exist two different primes $p \neq q$ such that

(9.10) $\qquad \psi(p) \geqslant \alpha + \varepsilon, \qquad \psi(q) \geqslant \alpha + \varepsilon$

for some $\varepsilon > 0$, and in this case we will deduce

$$\psi(a) \geqslant \alpha + \frac{1}{2}\varepsilon \quad \text{for all } a \geqslant 2$$

which contradicts the definition of α.

So let $p \neq q$ be primes for which (9.10) holds, and let $a \geqslant 2$ be arbitrary. Let $N \in \underline{Z}$, $N > 0$ satisfy $a^N > 3$, and choose integers $r \geqslant 0$ and $s \geqslant 0$ such that

$$p^r < \sqrt{\frac{1}{3}a^N} \leqslant p^{r+1}, \qquad q^s < \sqrt{\frac{1}{3}a^N} \leqslant q^{s+1}.$$

Since p^r and q^s are relatively prime, there are $x,y \in \underline{Z}$ such that $x\cdot p^r + y\cdot q^s = a^N$, and moreover we can achieve that $q^s < x \leqslant 2\cdot q^s$. Then $a^N > 3\cdot p^r\cdot q^s$ implies $y > p^r$. Now we have

$$\begin{aligned}
\varphi(a)^N = \varphi(a^N) &> \min\{\varphi(x p^r), \varphi(y\, q^s)\} = \\
&= \min\{\varphi(p)^r\cdot\varphi(x), \varphi(y)\cdot\varphi(q)^s\} \\
&\geqslant \min\{p^{r(\alpha+\varepsilon)}\cdot x^{\alpha}, y^{\alpha}\cdot q^{s(\alpha+\varepsilon)}\} \\
&\geqslant \min\{p^{r(\alpha+\varepsilon)}\cdot q^{s\alpha}, p^{r\alpha}\cdot q^{s(\alpha+\varepsilon)}\} \\
&\geqslant \min\{\frac{1}{p^{\alpha+\varepsilon}}\cdot\left(\sqrt{\frac{1}{3}a^N}\right)^{\alpha+\varepsilon}\cdot\frac{1}{q^{\alpha}}\left(\sqrt{\frac{1}{3}a^N}\right)^{\alpha}, \ldots\} \\
&\geqslant \frac{1}{(3pq)^{\alpha+\varepsilon}}\cdot a^{N(\alpha+\frac{1}{2}\varepsilon)}.
\end{aligned}$$

Taking N-th roots and letting N tend to infinity we find

$$\varphi(a) \geqslant a^{\alpha + \frac{1}{2}\varepsilon}$$

so $\psi(a) \geqslant \alpha + \frac{1}{2}\varepsilon$, as required. □

10. The smallest algorithms of discrete subrings of $\underline{C}$.

In this section we give an approximative description of the smallest algorithms of the rings $\underline{Z}$, $\underline{Z}[\sqrt{-d}]$ $(d = 1,2)$, $\underline{Z}[\frac{1}{2}(1+\sqrt{-d})]$ $(d = 3,7,11)$.

Let R be one of these rings, and embed R in $K = R \otimes_{\underline{Z}} \underline{R}$. Clearly, K is isomorphic to $\underline{R}$ or $\underline{C}$. By $|\ |$ we denote the usual absolute value on K. We define $c \in \underline{R}$ by

$$c^{-1} = \max_{x \in K} \min_{y \in R} |x-y|.$$

A picture shows

$$R = \underline{Z}, \qquad \underline{Z}[\sqrt{-d}], \qquad \underline{Z}[\tfrac{1}{2}(1+\sqrt{-d})]$$

$$c = 2, \qquad \frac{2}{\sqrt{d+1}}, \qquad \frac{4\sqrt{d}}{d+1},$$

the maxima being attained at $x = \frac{1}{2}$, $x = \frac{1}{2}(1+\sqrt{-d})$ and $x = \frac{d+1}{4d}\sqrt{-d}$, respectively.

In particular, we have $c^{-1} < 1$, and by (9.7) it follows that $|\ |$ is an algorithm (of type 2) on R(note that $|r|^{[K:R]} \in \underline{Z}$ for $r \in R$, so $\{|r|\,|\,r \in R\}$ is well ordered).

(10.1) Theorem. Let R and c be as above, and define $\psi\colon R - \{0\} \to \underline{Z}_{\geq 0}$ by $\psi(x) = \left[{}^{c}\log|x|\right]$. Then ψ is an algorithm (of type 1) on R. Further, if θ denotes the smallest algorithm on R, and k is the smallest integer ≥ 0 for which $c^{k} \geq \frac{1}{c-1}$, then

$$\theta(a) \leq \psi(a) \leq \theta(a) + k$$

for all $a \in R - \{0\}$.

Proof. First we show that ψ is an algorithm. Let $b \in R - \{0\}$ and $a \in R - Rb$; choose $y \in R$ with $|\frac{a}{b} - y| \leq c^{-1}$, then $r = a - yb$ belongs to $a + Rb$ and satisfies $|r| \leq c^{-1} \cdot |b|$ so $\psi(r) < \psi(b)$. Hence ψ is an algorithm, and since it is integer valued it follows that $\psi(x) \geq \theta(x)$ for all $x \neq 0$.

Put $s_n = \sup\{|a|\,|\,a \in R, \theta(a) \leq n\}$. Clearly $s_0 = 1$. Let $a \in R$ satisfy $\theta(a) \leq n$.

Choose $x \in K$ such that $\min_{y \in R}|x-y| = c^{-1}$, and let $b \in R$ be such that $|xa-b| \leqslant c^{-1}$.

Since θ is an algorithm, there exists $r = b - qa \in b + Ra$ such that $r = 0$ or $\theta(r) \leqslant n-1$. Then we have

$$\begin{aligned} s_{n-1} &\geqslant |r| = |(xa-qa) - (xa-b)| \geqslant |x-q|\cdot|a| - |xa-b| \\ &\geqslant c^{-1}\cdot|a| - c^{-1} \end{aligned}$$

so $|a| \leqslant c\cdot s_{n-1} + 1$. Since a is an arbitrary element with $\theta(a) \leqslant n$, we conclude $s_n \leqslant c\cdot s_{n-1} + 1$, and by induction

$$s_n \leqslant \frac{c^{n+1}-1}{c-1} < \frac{1}{c-1}\cdot c^{n+1} \leqslant c^{n+k+1}$$

if $c^k \geqslant \frac{1}{c-1}$. Therefore, if $a \in R - \{0\}$ satisfies $\theta(a) = n$, then $|a| < c^{n+k+1}$ and $\psi(a) \leqslant n+k = \theta(a)+k$, as required. □

(10.2) Corollary. The smallest algorithm of $\underline{Z}$ is given by

$$\theta(a) = \left[{}^2\log|a|\right] \quad (a\neq 0), \qquad \theta(0) = \omega.$$

Proof. Clear from (10.1) since $c = 2$ and $k = 0$. □

In the next section we will give a precise description of the smallest algorithms of $\underline{Z}[\sqrt{-1}]$ and $\underline{Z}[\frac{1}{2}(1+\sqrt{-3})]$. For these rings one has $k = 3$ and $k = 1$, respectively, and it can be checked that $k = \max\{\psi(a)-\theta(a)\,|\,a\in R-\{0\}\}$. For $\underline{Z}[\sqrt{-2}]$, $\underline{Z}[\frac{1}{2}(1+\sqrt{-7})]$ and $\underline{Z}[\frac{1}{2}(1+\sqrt{-11})]$ no precise description of the smallest algorithm is known. We have $k = 13$, 5 and 23, respectively, but doubtless $\max\{\psi(a) - \theta(a)\,|\,a \in R - \{0\}\}$ is smaller. It should not be hard to determine this maximum exactly.

(10.3) Corollary. Let R be as in (10.1). Then there exists a constant $C \in \underline{R}$ such that

$$\theta(a) + \theta(b) \leqslant \theta(ab) \leqslant \theta(a) + \theta(b) + C$$

for all $a,b \in R$, $ab \neq 0$.

Proof. Clear from (10.1) and the corresponding assertion for ψ. $\square$

It may be of interest to remark that the absolute value can be recovered from the smallest algorithm and the value of c by

$$(10.4) \qquad |a| = \lim_{n\to\infty} c^{\theta(a^n)/n} , \quad a \neq 0 .$$

This follows easily from (10.1).

The method used in proving (10.1) can also be employed to determine all quaternion division algebras over $\underline{Q}$ which ramify at ∞ and contain a euclidean order. The result is that up to isomorphism there exist three such orders, namely

$$\underline{Z}[i,j,\tfrac{1}{2}(1+i+j+ij)], \quad i^2 = j^2 = -1, \ ji = -ij,$$

$$\underline{Z}[i,\rho], \quad i^2 = -1, \ \rho^2 = -\rho - 1, \ i\rho = \rho^{-1}i,$$

$$\underline{Z}[\rho,\kappa,\tfrac{1}{\rho-1}(1+\kappa)], \quad \rho^2 = -\rho - 1, \ \kappa^2 = -5, \ \kappa\rho = \rho^{-1}\kappa,$$

each one of which is actually two-sided euclidean. The smallest algorithm can be desribed as in (10.1). It follows that the smallest left algorithm and the smallest right algorithm have bounded difference; it is unknown whether or not they are actually equal (cf.(11.3)).

(10.5) Proposition. Let R, c be as in (10.1), and put

$$r_n = \min\{|a| \,|\, a \in R - \{0\}, \ \theta(a) > n\},$$

$$s_n = \max\{|a| \,|\, a \in R, \ \theta(a) \leqslant n\}.$$

Then $r = \lim_{n\to\infty} r_n c^{-n}$ and $s = \lim_{n\to\infty} s_n c^{-n}$ exist, and $r \leqslant s < \infty$.

Proof. The argument showing that ψ is an algorithm easily generalizes to prove $r_n \geqslant c\cdot r_{n-1}$ for $n \geqslant 1$. Hence $(r_n\cdot c^{-n})_{n\geqslant 0}$ is non-decreasing and therefore has a limit $r \in \underline{R} \cup \{\infty\}$. Further we have seen in the proof of (10.1) that $s_n \leqslant c\cdot s_{n-1} + 1$. Putting $s^*_n = s_n + \frac{1}{c-1}$ we then have $s^*_n \leqslant c\cdot s^*_{n-1}$, so $(s^*_n\cdot c^{-n})_{n\geqslant 0}$ is non-increasing and has a limit $s \in \underline{R}_{\geqslant 0}$. Of course, s is also the limit of $(s_n\cdot c^{-n})_{n\geqslant 0}$. Finally, the definition of s_n implies $\theta([s_n] + 1) > n$, so $r_n \leqslant [s_n] + 1 \leqslant s_n + 1$ and $r \leqslant s$. □

For $R = \underline{Z}$ we have $r = s = 2$. For $R = \underline{Z}[\sqrt{-1}]$ it follows from the results of the next section that $r = \sqrt{2}$ and $s = \sqrt{10}$, while for $\underline{Z}[\frac{1}{2}(1+\sqrt{-3})]$ we have $r = \sqrt{3}$ and $s = \frac{1}{2}\sqrt{21}$ (cf.§11,fig.2). For the other three rings the values of r and s are unknown.

Let again R be as in (10.1), and put

$$a_n = \#\{a \in R \mid a = 0 \text{ or } \theta(a) < n\}, \qquad n \geqslant 0.$$

From (10.5) one easily derives that the sequence $a_n\cdot c^{-n[K:\underline{R}]}$ has a finite limes superior and a positive limes inferior; more precisely,

$$\limsup_{n\to\infty} \; a_n\cdot c^{-n[K:\underline{R}]} \leqslant \frac{2\, s^2\pi}{\sqrt{|\Delta|}\cdot c^2}$$

$$\liminf_{n\to\infty} \; a_n\cdot c^{-n[K:\underline{R}]} \geqslant \frac{2\, r^2\pi}{\sqrt{|\Delta|}\cdot c^2}$$

for $R \neq \underline{Z}$, where Δ denotes the discriminant of R over $\underline{Z}$. Has the sequence actually a limit? For $R = \underline{Z}$, we have

$$a_n = 2\cdot 2^n - 1,$$

and for $R = \underline{Z}[\sqrt{-1}]$ we will see in §11 that

$$a_n = 14\cdot 2^n - 34\cdot 2^m + 4\cdot n + 21 \qquad \text{for } n = 2\cdot m,\ m \geqslant 0\ ,$$

$$a_n = 14\cdot 2^n - 48\cdot 2^m + 4\cdot n + 21 \qquad \text{for } n = 2\cdot m + 1,\ m \geqslant 0\ ,$$

while the same methods yield for $R = \underline{Z}[\frac{1}{2}(1+\sqrt{-3})]$ the formula

$$57\cdot a_n = 333\cdot 3^n - q_n + 114\cdot n + 266, \qquad \text{for } n \geqslant 0\ , \text{ where}$$

$$q_0 = 542,\quad q_1 = 980,\quad q_2 = 1724,\quad q_{n+3} = 2\cdot q_{n+1} + 2\cdot q_n \quad (n \geqslant 0)\ .$$

It follows easily that for these rings the limit actually does exist. Further, for each of these rings the sequence $(a_n)_{n \geqslant 0}$ satisfies a linear recurrence relation. There seems to be no reason to suppose that this also holds for the other three rings. For $R = \underline{Z}[\sqrt{-2}]$ the sequence $(a_n)_{n=0}^{17}$ is given by (1,3,9,17,31,53,85,133,197,293,417,593,849,1193,1661,2291,3139,4299) (the values given in [2] are erroneous).

11. The smallest algorithms of $\underline{Z}[i]$ and $\underline{Z}[\rho]$.

In this section all algorithms will be of type 2. For the smallest algorithm θ this means $\theta(0) = 0$.

Let R be a ring without zero-divisors, $R_1 = R^* \cup \{0\}$ and $x \in R$. The subset $\{\Sigma_{i=0}^{n-1} u_i x^i \mid n \in \underline{Z}_{\geq 0}, u_i \in R_1 \text{ for } 0 \leq i < n\}$ of R is denoted by $R_1[x]$. We define $\psi_x : R_1[x] \to \underline{Z}_{\geq 0}$ by

$$\psi_x(r) = \min\{n \in \underline{Z}_{\geq 0} \mid \exists\ u_i \in R_1,\ 0 \leq i < n : r = \Sigma_{i=0}^{n-1} u_i x^i\}.$$

Clearly $\psi_x(r) = 0 \iff r = 0$, and $\psi_x(r) = 1 \iff r \in R^*$.

Examples. Let $R = k[X]$, with k a field, and $x = X$. Then $R_1 = k$ and $R_1[x] = R$. Further $\psi_x(f) = \deg(f) + 1$ for $f \in R - \{0\}$. We know from §4 that ψ_x is the smallest algorithm on R.

Let $R = \underline{Z}$, then $R_1 = \{1,0,-1\}$. For $x = 1$ we have $R_1[x] = \underline{Z}$, and $\psi_1(n) = |n|$. This is an algorithm on $\underline{Z}$, but not the smallest one. For $x = 2$ we also have $R_1[x] = \underline{Z}$, and $\psi_2(n) = [{}^2\log|n|] + 1$ for $n \neq 0$. By (10.2) this is the smallest algorithm (of type 2) on $\underline{Z}$. Also for $x = 3$ we have $R_1[x] = \underline{Z}$, but ψ_3 is no algorithm on $\underline{Z}$.

(11.1) Lemma. Suppose $x \in R - R_1$, and let $a \in R_1[x] - \{0\}$. Then $\psi_x(ax) = \psi_x(a) + 1$. Further $\psi_x(x^n) = n + 1$ for $n \in \underline{Z}_{\geq 0}$.

Proof. Clearly $\psi_x(ax) \leq \psi_x(a) + 1$. If $ax = \Sigma_{i=0}^{n-1} u_i x^i$ with $n = \psi_x(ax)$ and $u_i \in R^* \cup \{0\}$, then $x \notin R^*$ implies $u_0 \notin R^*$ so $u_0 = 0$. Since $x \neq 0$ we find $a = \Sigma_{i=0}^{n-2} u_{i+1} x^i$ so $\psi_x(a) \leq n-1 = \psi_x(ax)-1$. This proves the first assertion. The second one follows by induction on n. □

(11.2) Theorem. Suppose R is euclidean with smallest algorithm $\theta\colon R \to \underline{Z}_{\geqslant 0}$. Let $x \in R - R_1$. Then the following three assertions are equivalent:

(a) $R = R_1[x]$ and ψ_x is an algorithm on R;

(b) $\psi_x(a) \geqslant \theta(a)$ for all $a \in R_1[x]$;

(c) $R = R_1[x]$ and $\psi_x = \theta$.

Proof. (a) $\Rightarrow$ (b) and (c) $\Rightarrow$ (a) are obvious. We prove (b) $\Rightarrow$ (c). Assume (b) and let $a \in R$. With induction on $\theta(a)$ we prove

$$a \in R_1[x] \text{ and } \psi_x(a) = \theta(a).$$

For $\theta(a) = 0$ this is right, so let $\theta(a) = n + 1 \geqslant 1$. Since θ is an algorithm, we have

$$x^n = q \cdot a + r, \text{ with } q,r \in R,\ \theta(r) \leqslant n.$$

The induction hypothesis asserts $r \in R_1[x]$ and $\psi_x(r) \leqslant n$. So we can write $r = \Sigma_{i=0}^{n-1} t_i x^i$ with $t_i \in R_1$. By (11.1) we have $\psi_x(x^n) = n + 1$ so

$$x^n \neq \Sigma_{i=0}^{n-1} t_i x^i$$

$$qa = x^n - \Sigma_{i=0}^{n-1} t_i x^i \neq 0.$$

Using (b) we get

$$\theta(qa) \leqslant \psi_x(qa) \leqslant n+1 = \theta(a)$$

and since $q \cdot a \neq 0$ this implies $q \in R^*$ by (2.2). We conclude

$$a = q^{-1} \cdot x^n - \Sigma_{i=0}^{n-1} q^{-1} \cdot t_i \cdot x^i$$

so $a \in R_1[x]$ and $\psi_x(a) \leqslant n + 1 = \theta(a)$. Equality now follows from (b). □

The condition $x \in R_1$ cannot be missed as is shown by the example $R = \underline{Z}$, $x = 1$.

(11.3) Examples. For $R = k[X]$, $x = X$ and $R = \underline{Z}$, $x = 2$ theorem (11.2) tells us that ψ_x is the smallest algorithm of R, as we knew already.

For $R = \underline{Z}\,[i]$, where $i^2 = -1$, and $x=1+i$ we prove below that ψ_x is an algorithm on R and therefore the smallest one. The same method can be used to show that $\psi_{1-\rho}$ is the smallest algorithm on $\underline{Z}\,[\rho]$, where $\rho = \frac{1}{2}\,(-1+\sqrt{-3})$. It is probable that the smallest algorithm of the ring of integral quaternions $\underline{Z}\,[i,j,\frac{1}{2}(1+i+j+ij)]$ (where $i^2=-1$, $j^2 = -1$, $ji = -ij$) equals ψ_{1+i}, but the proof, which involves four-dimensional pictures, has not yet been carried out. It would follow that on this ring the smallest left algorithm and the smallest right algorithm coincide.

Arbitrarily many examples are obtained by applying the following result transfinitely often. Suppose ψ_x is an algorithm on R, where $x \in R-R_1$, and let $y \in R[[X]]\,[X^{-1}]$ be a nonzero element whose first non-zero coefficient equals x; then ψ_y is an algorithm on $R[[X]]\,[X^{-1}]$. This can be proved by checking (11.2) (b), using (5.1).

Finally we mention the trivial example of a discrete valuation ring R, with x equal to a prime element.

<u>(11.4) Rings which have no algorithm</u> ψ_x. Let R be one of the rings $\underline{Z}\,[\sqrt{-2}]$, $Z\,[\frac{1}{2}(1+\sqrt{-7})]$ and $\underline{Z}\,[\frac{1}{2}(1+\sqrt{-11})]$. We claim that there is no $x \in R$ such that ψ_x is an algorithm on $R=R_1[x]$. To prove this, note first of all that $R=R_1[x]$ would imply $x \notin R_1$. So by (11.2) we would have $\psi_x=\theta$, and (11.1) and (10.4) give $|x| = c$. But $|x|^2 \in \underline{Z}$, while c^2 is one of $\frac{4}{3}, \frac{7}{4}, \frac{11}{9}$ so $c^2 \notin \underline{Z}$, contradiction.

Without proof we mention the following more general result. We call a ring R of <u>finite type</u> over a subring A if there is a finite subset $Y \subset R$ such that A and Y generate R as a ring. Suppose R is a domain which is of finite type over $\underline{Z}$ or over a field, and suppose there exists $x \in R-R_1$ such that ψ_x is an algorithm on $R=R_1[x]$. Then either $R=\underline{Z}$, $x = \pm 2$, or $R=\underline{Z}\,[i]$, $x \in R^*(1+i)$, or $R=\underline{Z}[\rho]$, $x \in R^*(1-\rho)$, or $R=k[x]$ for some subfield k of R, and x is transcendental over k.

Finally, if R is a domain satisfying the second stable range condition (§3) and having an algorithm ψ_x, $x \in R-R_1$, then R is a discrete valuation ring and x is a prime element.

The proofs of these statements basically consist in finding units u such that $x+u$ is neither a prime element nor a unit.

Next we develop a technique for proving a function ψ_x to be an algorithm. Let R be a ring without zero-divisors, and $x \in R-R_1$. By Q we mean the left R-module

$$Q = R[x^{-1}] = \bigcup_{n\geq 0} R\cdot x^{-n}.$$

For commutative R one can consider Q as the ring generated by R and x^{-1} inside the field of fractions of R. For arbitrary R a formal definition is

$$Q = \varinjlim (R_n, f_{n,m})_{n\geq 0,\ m\geq n\geq 0}$$

where

$$R_n = R \qquad \text{for } n\geq 0,$$

$$f_{n,m}: R_n \to R_m \text{ maps } r \text{ to } rx^{m-n}, \text{ for } m\geq n\geq 0.$$

The image of $1 \in R_n$ under the canonical injection $R_n \to Q$ is denoted by x^{-n}, and we consider R as a submodule of Q by $R = R\cdot x^{-0}$; in particular $x^n = x^n \cdot x^{-0}$ for $n\geq 0$. There is a unique R-automorphism $Q \to Q$ mapping x^n to x^{n+1} for all $n \in \mathbb{Z}$. This automorphism and its inverse are written as right multiplications by x and x^{-1}, respectively.

Define $R_1[x,x^{-1}] = \{ \sum_{i=-m}^{n} u_i\cdot x^i \mid n,m \in \mathbb{Z}_{\geq 0},\ u_i \in R_1\} \subset Q$.

Using (11.1) we can extend the mapping $\psi_x : R_1[x] \to \mathbb{Z}_{\geq 0}$ to a mapping $\psi_x : R_1[x,x^{-1}] \to \mathbb{Z}$ by putting $\psi_x(rx^{-n}) = \psi_x(r)-n$ for $r \in R_1[x]-\{0\}$ and $n\geq 0$. Let

$$V = \{v \in R_1[x,x^{-1}] \mid \psi_x(v) \leqslant 0\}$$

$$= \{\Sigma_{i=1}^n u_i x^{-1} \mid n \in \underline{Z}_{\geqslant 0},\ u_i \in R_1\}.$$

The following proposition gives a criterion for ψ_x to be an algorithm in terms of covering properties of the set V, cf. (9.7).

(11.5) Proposition. The following two assertions are equivalent:

(a) $R = R_1[x]$ and ψ_x is an algorithm on R;

(b) there exists an algorithm $\varphi: R \to \underline{Z}_{\geqslant 0}$, and for each $v \in V - \{0\}$ the natural map $V \to Q/Rvx$ is surjective.

Proof. (a) $\Rightarrow$ (b). The existence of φ is clear. Let $v \in V - \{0\}$. For n sufficiently large there exists $a \in R$ with $v = ax^{-n-1}$ and $\psi_x(a) \leqslant n+1$. Since ψ_x is an algorithm, the natural map

$$V\cdot x^n \cap R = \{r \in R \mid \psi_x(r) \leqslant n\} \to R/Ra$$

is surjective. Multiplying by x^{-n} on the right we find that

$$V \cap Rx^{-n} \to Rx^{-n}/Rvx$$

is surjective for n sufficiently large. Taking the union over n one finds that $V \to Q/Rvx$ is surjective, as required.

(b) $\Rightarrow$ (a). Let $\theta: R \to \underline{Z}_{\geqslant 0}$ denote the smallest algorithm on R (of type 2). Let $a \in R_1[x]$, $a \neq 0$, satisfy $\psi_x(a) = n+1$. Then $v = a\cdot x^{-n-1} \in V-\{0\}$ so by (b) the map $V \to Q/Rvx$ is onto. By $Rvx \subset Rx^{-n}$ this easily implies that

$$V \cap Rx^{-n} \to Rx^{-n}/Rvx$$

is onto, and multiplying on the right by x^n one finds that

$$\{r \in R_1[x] \mid \psi_x(r) \leqslant n\} \to R/Ra$$

is surjective. By induction on n and using (2.6) one derives from this $\theta(a) \leqslant n+1$.

Hence we have proved that $\theta(a) \leqslant \psi_x(a)$ for all $a \in R_1[x]-\{0\}$. This implies (a) by (11.2). □

Finally we prove a result which is convenient in determining V. For $W \subset Q$ we define

$$F(W) = \{ (u+w)\, x^{-1} \mid u \in R_1,\ w \in W \}.$$

(11.6) Proposition. Let $S = (Q-R) \cup \{0\}$ and let $T \subset Q$. We have:

(i) $V = \bigcup_{m \geqslant 0} F^m(\{0\}) = \bigcap_{m \geqslant 0} F^m(S)$;

(ii) if $T \subset S$ and $T \subset F(T)$ then $T \subset V$;

(iii) if $0 \in T$ and $F(T) \subset T$ then $V \subset T$;

(iv) if $0 \in T \subset S$ then

$$T = V \Leftrightarrow F(T) = T.$$

Proof. One easily checks

$$F^m(\{0\}) = \{ \Sigma_{i=1}^m u_i x^{-i} \mid u_i \in R_1 \text{ for } 1 \leqslant i \leqslant m \}$$

for $m \geqslant 0$, so

$$V = \bigcup_{m \geqslant 0} F^m(\{0\}).$$

Since

$$W_1 \subset W_2 \Rightarrow F(W_1) \subset F(W_2)$$

$$\{0\} \subset F(\{0\}), \quad F(S) \subset S$$

it follows that

$$\bigcup_{m \geqslant 0} F^m(\{0\}) \subset \bigcap_{m \geqslant 0} F^m(S).$$

To prove the other inclusion, one first proves by induction on m:

(11.7) $F^m(S) = (Q-Rx^{-m}) \cup F^m(\{0\}), \qquad m \geqslant 0.$

Now let $a \in \bigcap_{m \geqslant 0} F^m(S)$. For m sufficiently large we have $a \in Rx^{-m}$, so (11.7) implies $a \in F^m(\{0\}) \subset \bigcup_{m \geqslant 0} F^m(\{0\})$. This proves (i). Statements (ii), (iii), (iv) are immediate consequences. □

<u>(11.8) Example.</u> $R = \underline{Z}$, $x = 2$. Let $T = \{ a \in Q \mid |a| < 1 \}$ where $| \ |$ is the usual absolute value on $Q = \underline{Z}\left[\frac{1}{2}\right] \subset \underline{R}$. One easily checks

$$T = F(T), \quad 0 \in T \subset S,$$

so we have $T = V$. Since $(-|v|, +|v|] \cap Q \subset V$ for $v \in V$, it follows that

$$V \to Q/\underline{Z}2v$$

is surjective for $v \in V - \{0\}$. By (11.5) we conclude that ψ_x is an algorithm on $\underline{Z}$.

<u>(11.9) Example.</u> $R = \underline{Z}[i]$, $x = 1+i$. We consider $Q = R\left[x^{-1}\right] = \underline{Z}\left[i, \frac{1}{2}\right]$ as a subset of the complex plane. If $a_1, \ldots, a_n$ are complex numbers, then $C(a_1, \ldots, a_n)$ denotes the intersection of Q and the convex hull of $\{a_1, \ldots, a_n\}$; further, if $a_1, a_2, \ldots, a_n, a_1$ are the vertices of an n-gon (in that order), then the interior of that n-gon, intersected with Q, is denoted by $I(a_1, \ldots, a_n)$.

Let

$T_1 = I(2+i, 1+2i, -1+2i, -2+i, -2-i, -1-2i, 1-2i, 2-i)$,

cf. fig. 4. One easily checks $F(T_1) \subset T_1$ and $0 \in T_1$, so (11.6) (iii) tells us

$$(11.10) \qquad V \subset T_1.$$

Let T_2 be the intersection of Q and the bounded open region of $\underline{C}$ the boundary of which has been drawn in fig. 3 (note $\{\pm 1, \pm i\} \cap T = \emptyset$). Then $T_2 \subset F(T_2)$ and $T_2 \subset S$ so by (11.6) (ii) we have

$$(11.11) \qquad T_2 \subset V.$$

An impression of how V looks like is given in fig. 1, but we need no information from this picture.

Write $\bar{x} = 1-i$. We are going to prove that for $v \in V$ we have

$$(11.12) \qquad C(0, xv, \bar{x}v, 2v) \subset V \cup (xv+V) \cup (\bar{x}v+V) \cup (2v+V)$$

cf. fig. 5. Since $C(0, xv, \bar{x}v, 2v)$ is a fundamental domain for the lattice $\underline{Z}[i] \cdot xv$, for $v \neq 0$, and since $\bar{x}v$ and $2v$ belong to this lattice, it follows from (11.12) that the natural map

$$V \to Q/\underline{Z}[i] \cdot xv, \qquad v \in V - \{0\},$$

is surjective, so that ψ_x is an algorithm by (11.5).

Proof of (11.12). First we remark:

(11.13) for $v \in V$, $v \in C(x, \bar{x}, -x, -\bar{x})$, assertion (11.12) is true.

This follows simply from $C(v, -v, iv, -iv) \subset V$, cf. fig. 4.

The general case is treated by induction on

$$n(v) = \min \{ n \in \underline{Z}_{\geq 0} \mid x^n v \in R \}.$$

Start of the induction: if $n(v) \leq 1$ then $v \in C(x, \bar{x}, -x, -\bar{x})$ and (11.13) applies.

Induction step. By (11.13), (11.10) and reasons of symmetry we may assume

$$v \in C(i,\ 1+i,\ 1\frac{1}{2} + 1\frac{1}{2}i,\ 1 + 2i,\ 2i),$$

cf. fig. 4. A lemma which we formulate and prove below asserts that we can write

$$v = \frac{1}{2} x\ (1+w), \quad \text{with } w \in V, \quad n(w) = n(v)-1.$$

Applying the inductive hypothesis to w we find

$$C(0,\ xw,\ \bar{x}w,\ 2w) \subset V \cup (xw + V) \cup (\bar{x}w + V) \cup (2w + V).$$

After the transformation $z \mapsto \frac{1}{2}\ x(1+z)$ $(z \in Q)$ this means that the dotted square in fig. 5:

$$C(\frac{1}{2} x,\ \frac{1}{2} x\ (1+xw),\ \frac{1}{2} x\ (1+\bar{x}w),\ \frac{1}{2} x\ (1+2w))$$

$$= C(\frac{1}{2} x,\ xv + \frac{1}{2} \bar{x},\ \bar{x}v - \frac{1}{2} \bar{x},\ 2v - \frac{1}{2} x)$$

is contained in the set

$$\frac{1}{2} x\ (1+V) \cup (xv + \frac{1}{2} x\ (-i+V)) \cup (\bar{x}v + \frac{1}{2} x\ (i+V)) \cup (2v + \frac{1}{2} x\ (-1+V))$$

which in turn by $F(V) = V$ is contained in

$$V \cup (xv + V) \cup (\bar{x}v + V) \cup (2v + V).$$

In order to finish the induction step it now suffices to show that the "large" square $C(0,\ xv,\ \bar{x}v,\ 2v)$ minus the dotted one is also contained in $V \cup (xv + V) \cup (\bar{x}v + V) \cup (2v + V)$. For reasons of symmetry this follows if we prove (cf. fig. 5)

(11.14) $I\ (0,\ \bar{x}v,\ \bar{x}v - \frac{1}{2} \bar{x},\ \frac{1}{2} x) \cup C(0,\ \bar{x}v) \subset V \cup (\bar{x}v + V).$

Suppose (11.14) is false. Then there is an element a in the left hand side of (11.14) such that $a \notin V$ and $a - \bar{x}v \notin V$. Putting $b = \bar{x}v - a$ this means:

(11.15) there exist $a, b \in I\ (0, \frac{1}{2}\bar{x}, \bar{x}v - \frac{1}{2}x, \bar{x}v, \bar{x}v - \frac{1}{2}\bar{x}, \frac{1}{2}x)$

such that $a \notin V$, $b \notin V$ and $a+b = \bar{x}v = 1 + w$.

From (11.15) we derive a contradiction. Note that (11.15) is symmetric in a and b.

First we consider the case $v \in C\ (\frac{1}{2} + i, 1+i, 1\frac{1}{2} + 1\frac{1}{2}i, 1+2i, \frac{1}{2} +2i)$, cf. fig. 6. Then both a and b are contained in

$$I\ (0, \frac{1}{2} - \frac{1}{2}i, 2\frac{1}{2} - \frac{1}{2}i, 3, 3+i, 2+2i).$$

We have $\mathrm{Re}\ (a+b) = \mathrm{Re}\ (\bar{x}v) < 3$ (Re = real part), so we may assume $\mathrm{Re}\ (a) < \frac{3}{2}$. Then

$$a \in I\ (0, \frac{1}{2} - \frac{1}{2}i, 1\frac{1}{2} - \frac{1}{2}i, 1\frac{1}{2} + 1\frac{1}{2}i),$$

so from $a \notin V$ and (11.11) we conclude $a = 1$ (cf. fig. 3). But then $b = w$ which contradicts $b \notin V$.

Secondly we consider the case $v \in C(i, \frac{1}{2} + i, \frac{1}{2} + 2i, 2i)$, cf. fig. 7.

Then

$$a, b \in I\ (0, \frac{1}{2} - \frac{1}{2}i, 2\frac{1}{2} + 1\frac{1}{2}i, 1\frac{1}{2} + 2\frac{1}{2}i, \frac{1}{2} + 1\frac{1}{2}i, \frac{1}{2} + \frac{1}{2}i).$$

We have $\mathrm{Re}\ (\bar{x}a + \bar{x}b) = \mathrm{Re}\ (-2iv) < 4$ so we may assume $\mathrm{Re}\ (\bar{x}a) < 2$. Then

$$a \in I\ (0, \frac{1}{2} - \frac{1}{2}i, 1\frac{1}{2} + \frac{1}{2}i, \frac{1}{2} + 1\frac{1}{2}i, \frac{1}{2} + \frac{1}{2}i).$$

But this set is by (11.11) and fig. 3 entirely contained in V, so $a \in V$, contradiction.

This finishes the induction step and the proof of (11.12), except that the following lemma is still to be proved.

(11.16) Lemma. Suppose $v \in V \cap C(i, 1+i, 1\frac{1}{2} + 1\frac{1}{2}i, 1+2i, 2i)$. Then there exists $w \in V$ such that $v = \frac{1}{2}x(1+w)$ and $n(w) = n(v)-1$.

Proof. Let $n = n(v)$, then we can write $v = \Sigma_{j=1}^{n} u_j x^{-j}$ with $u_j \in R_1$ and $u_n \in R^*$. Repeated use of $x^{-m} = -i\cdot x^{-m} + x^{-(m-1)}$ shows that we may assume $u_j \in R^*$ for $1 \leqslant j \leqslant n$.

Then we have $v \in x^{-1}.\ (R^* + V) = \frac{1}{2}\, x\cdot(R^* + V)$ (since $\frac{1}{2}\, x = i\cdot x^{-1}$), so $v \in \frac{1}{2}\, x\cdot(\varepsilon + V)$ for some $\varepsilon \in R^*$. We distinguish four cases: $\varepsilon = -i$, $\varepsilon =-1$, $\varepsilon = i$ and $\varepsilon = 1$.

If $\varepsilon = -i$, then $v \in \frac{1}{2}\, x(-i + V) \subset \frac{1}{2}\, x(-i + T_1)$ by (11.10), but $\frac{1}{2}\, x(-i + T_1)$ has empty intersection with the pentagon $C\ (i,\ 1+i,\ 1\frac{1}{2} + 1\frac{1}{2}\, i,\ 1 + 2i,\ 2i)$, contradiction.

For $\varepsilon = -1$ we derive exactly the same contradiction.

For $\varepsilon = i$ we have $v \in \frac{1}{2}\, x(i + V) \subset \frac{1}{2}\, x(i + T_1)$ and taking the intersection with the pentagon we find

$$v \in C(i,\ 1+i,\ 2i) - C(1+i,\ 2i).$$

If $v \notin C(i, 2i)$ then fig. 3 easily yields $v \in \frac{1}{2}\, x(1 + T_2)$ which by (11.11) is part of $\frac{1}{2}\, x(1 + V)$, so we can take $\varepsilon = 1$; and if $v \in C(i, 2i)$ then $v = -\bar{v} \in -\frac{1}{2}\, \bar{x}\ (-i + V) = \frac{1}{2}\, x\ (1 + V)$ which also reduces to the case $\varepsilon = 1$.

The conclusion is that we are always in the fourth case $\varepsilon = 1$, so $v = \frac{1}{2}\, x(1 + w)$ for some $w \in V$. It is immediate that $n(w) = n(v)-1$. □

(11.17) Example. $R = \underline{Z}\ [\rho]$, $\rho^2 = -\rho-1$, $x=1-\rho$. In this case V is slightly more complicated (cf. fig. 2). But by methods completely analogous to those employed for $\underline{Z}\ [i]$ one can show that condition (11.5) (b) is satisfied. We conclude that ψ_x is an algorithm on R.

Let again $R = \underline{Z}\ [i]$. We conclude this section with an outline of the computation of

$$a_n = \# R_n$$

where

$$R_n = \{\, a \in R \mid \psi_{1+i}(a) \leqslant n \,\}$$

$$= \{\, \Sigma_{j=0}^{n-1}\ u_j \cdot (1+i)^j \mid u_j \in R_1 = R^* \cup \{0\} \text{ for } 0 \leqslant j \leqslant n-1 \}.$$

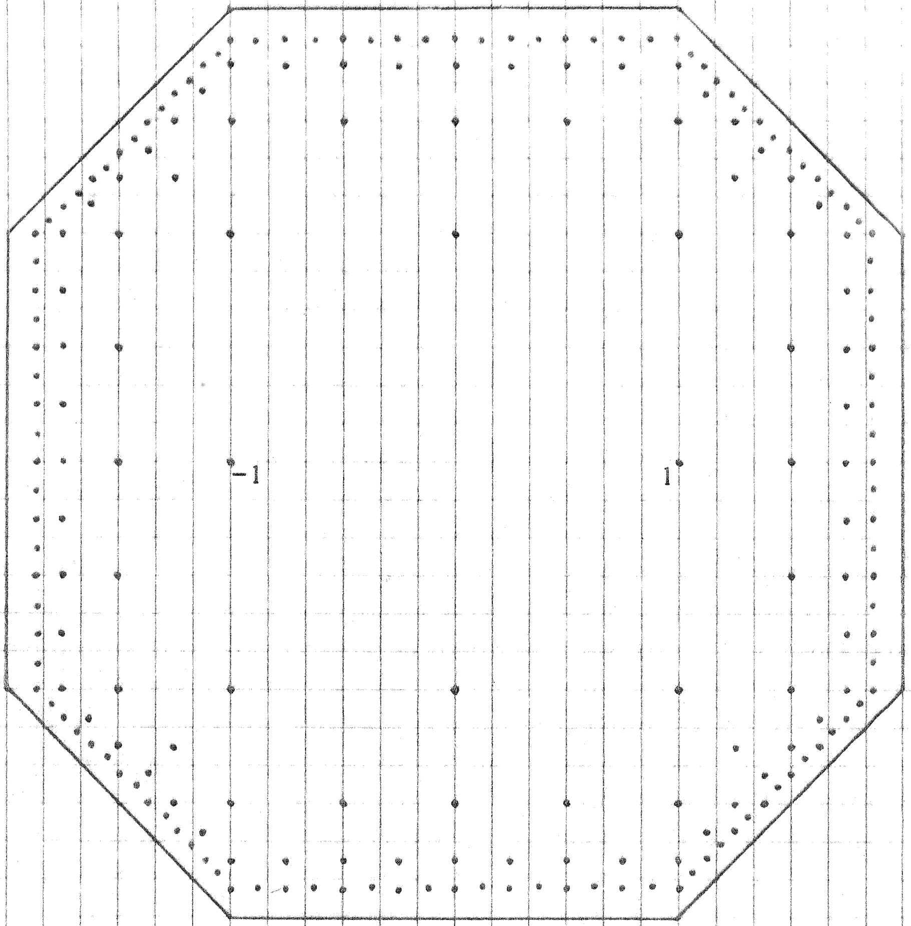

Fig. 1

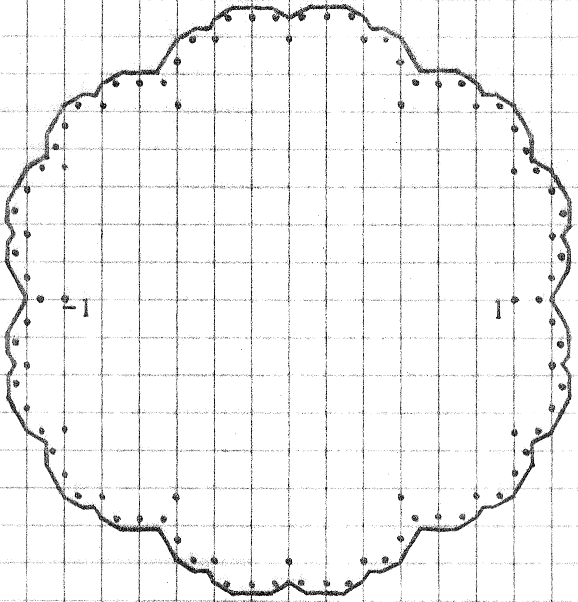

Fig. 2

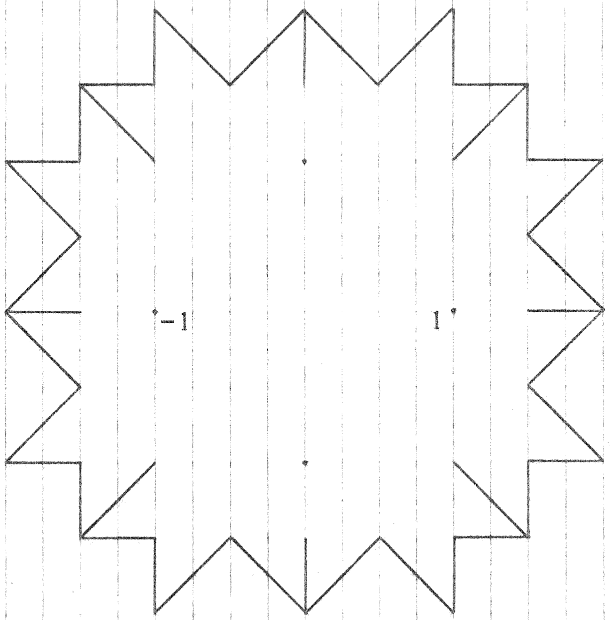

Fig. 3

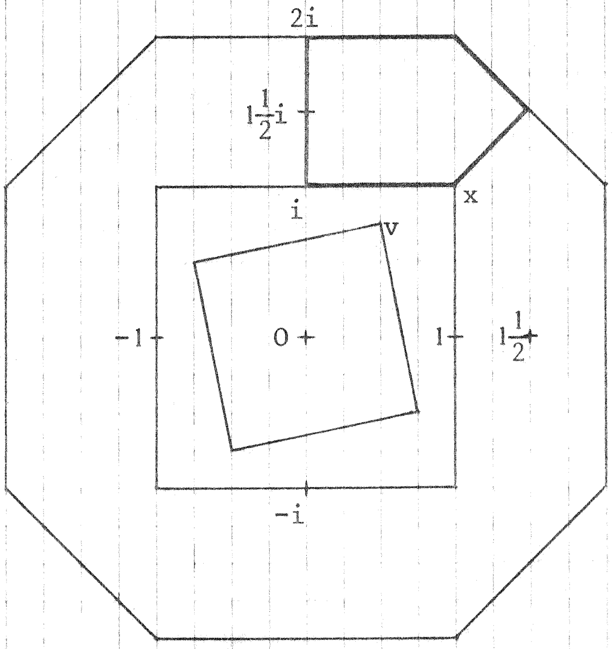

Fig. 4

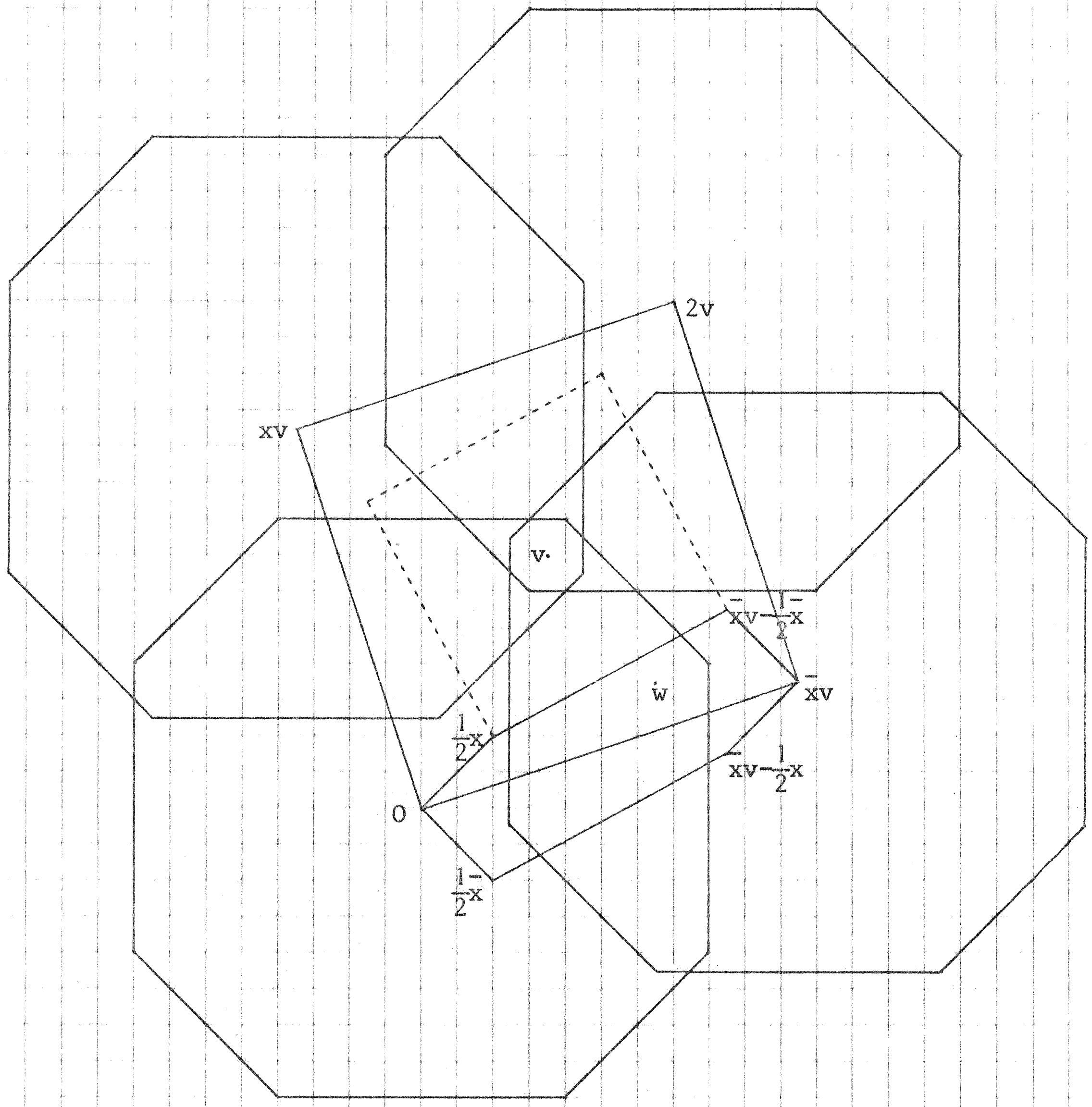
2v
xv
v
$\bar{x}v-\frac{1}{2}\bar{x}$
w
$\bar{x}v$
$\frac{1}{2}x$
$\bar{x}v-\frac{1}{2}x$
O
$\frac{1}{2}\bar{x}$

Fig. 5

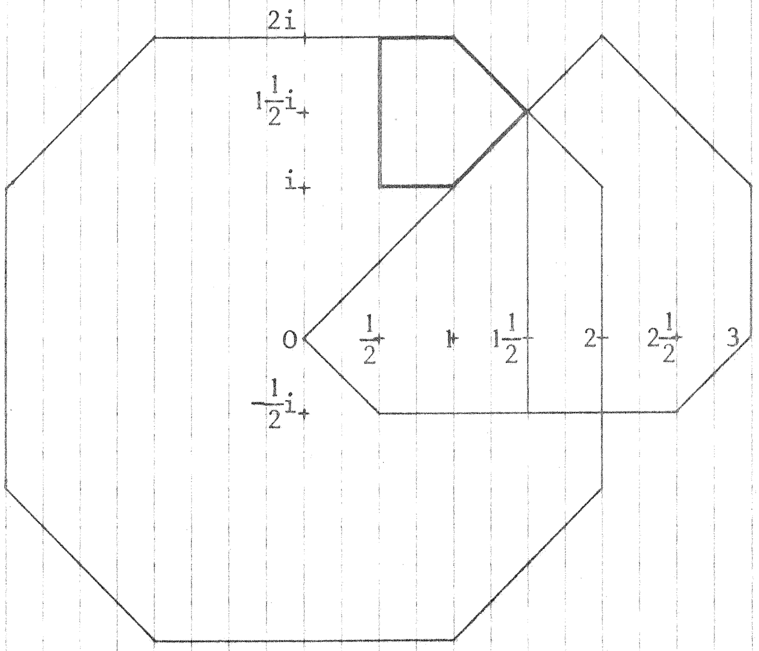
2i
$1\frac{1}{2}i$
i
0
$\frac{1}{2}$
1
$1\frac{1}{2}$
2
$2\frac{1}{2}$
3
$-\frac{1}{2}i$

Fig. 6

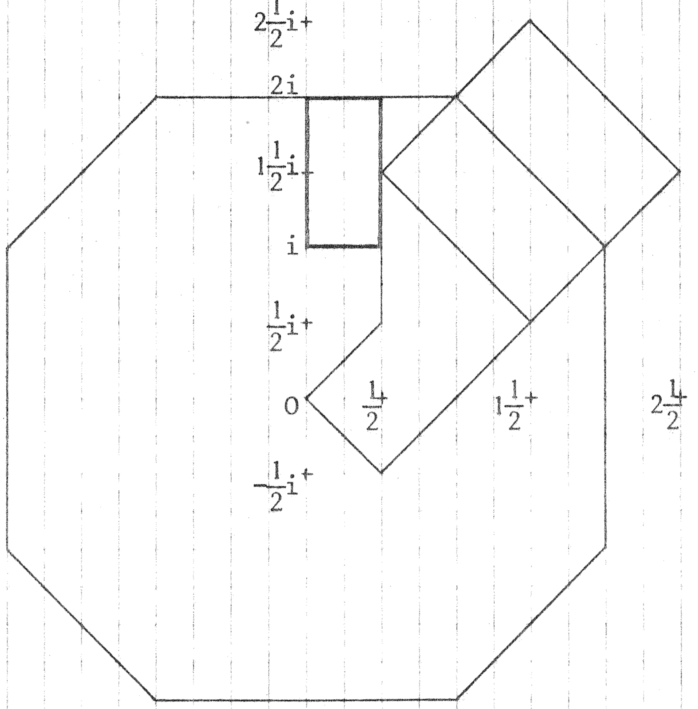
$2\frac{1}{2}i$
2i
$1\frac{1}{2}i$
i
$\frac{1}{2}i$
0
$\frac{1}{2}$
$1\frac{1}{2}$
$2\frac{1}{2}$
$-\frac{1}{2}i$

Fig. 7

The injective map $R_{n-1} \to R_n$ mapping a to $a\cdot(1+i)$ has as its image precisely the elements $\Sigma_{j=0}^{n-1} u_j\cdot(1+i)^j$ with $u_0 = 0$. Hence if we put

$$b_n = a_n - a_{n-1}, \qquad \text{where } a_{-1} = 0,$$

then

$$b_n = \# B_n \qquad (n\geqslant 0)$$

where

$$B_0 = \{0\}$$

$$B_n = \{ \Sigma_{j=0}^{n-1} u_j\cdot(1+i)^j \mid u_j \in R_1 \text{ for } 1 \leqslant j \leqslant n-1, \text{ and } u_0 \in R^*\}.$$

We will compute b_n by considering the area of a suitable region in $\underline{C}$. For $W \subset \underline{C}$, put $F(W) = \{ (u+w)\cdot(1+i)^{-1} \mid u \in R_1, w \in W \}$ as before. Let $U \subset \underline{C}$ be the square $\{ \alpha + \beta i \mid \alpha, \beta \in \underline{R}, |\alpha|+|\beta| \leqslant 1 \}$. By induction on n one proves

$$F^n(U) = \bigcup_{r \in B_n} (x^{-n} \cdot r + x^{-n} \cdot U)$$

where the union is "disjoint" in the sense that the intersections have measure zero. If μ denotes the usual measure on $\underline{C}$, then $\mu(U) = 2$, so

$$\mu(F^n(U)) = 2^{1-n}\cdot b_n$$

and

$$b_n = 2^{n-1}\cdot\mu(F^n(U)).$$

Drawing pictures of the first few $F^n(U)$ one discovers that it is not hard to give an explicit description of $F^n(U)$ for all n and a formula for its area. But this method would be difficult to imitate for $\underline{Z}[\rho]$. Below we describe a method which needs much less information about the sets $F^n(U)$ and has the advantage of being applicable to $\underline{Z}[\rho]$. The details are left to the reader.

(a) $F^n(U)$ is simply connected, and its boundary can be broken up in a certain number, say f_n, of straight line segments, each one of which has length $\sqrt{2}^{1-n}$. The angle between two consecutive line segments, measured inside $F^n(U)$, equals oneof $\frac{1}{2}\pi$, π, $\frac{3}{2}\pi$. Let this happen c_n, d_n and e_n times, respectively. Clearly, $c_n + d_n + e_n = f_n$.

(b) If t is one of those f_n line segments, then there exists a unique triangle, <u>not</u> lying inside $F^n(U)$, which has t as one of its edges and whose other two edges each have length $\sqrt{2}^{-n}$. Let this triangle, together with its interior, be denoted by Δ_t. Note that $\mu(\Delta_t) = 2^{-n-1}$.

(c) $F^{n+1}(U)$ arises from $F^n(U)$ by adjunction of all triangles Δ_t:

(11.18) $F^{n+1}(U) = \left(\bigcup_t \Delta_t\right) \cup F^n(U)$,

and this union is disjoint modulo sets of measure zero. Therefore

$$\mu(F^{n+1}(U)) = \mu(F^n(U)) + f_n \cdot 2^{-n-1}$$

and

$$\begin{aligned} b_{n+1} &= 2 \cdot b_n + \frac{1}{2} f_n \\ &= 2 \cdot b_n + \frac{1}{2} (c_n + d_n + e_n). \end{aligned}$$

(d) One can use (11.18) to describe the boundary of $F^{n+1}(U)$ in terms of the boundary of $F^n(U)$. This yields

$$\begin{aligned} c_{n+1} &= f_n - 2 \cdot e_n = c_n + d_n - e_n \\ d_{n+1} &= c_n + e_n \\ e_{n+1} &= d_n. \end{aligned}$$

The conclusion is

$$\begin{pmatrix} b_{n+1} \\ c_{n+1} \\ d_{n+1} \\ e_{n+1} \end{pmatrix} = \begin{pmatrix} 2 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 1 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} b_n \\ c_n \\ d_n \\ e_n \end{pmatrix}, \qquad n \geqslant 0,$$

and we also have $b_0 = 1$, $c_0 = 4$, $d_0 = e_0 = 0$. By standard techniques of linear algebra one finds

$$b_n = 7 \cdot 2^n - (5 + \frac{7}{2}\sqrt{2}) \cdot \sqrt{2}^n - (5 - \frac{7}{2}\sqrt{2}) \cdot (-\sqrt{2})^n + 4$$

and it follows easily that

$$a_n = 14\cdot 2^n - (17+12\cdot\sqrt{2})\ \sqrt{2}^n - (17-12\sqrt{2})\cdot(-\sqrt{2})^n + 4\cdot n + 21$$

which is equivalent to the formula mentioned in section 10.

12. Artin's conjecture.

In this section we discuss a generalized version of Artin's conjecture, which will be needed in §13.

Let F be a global field, E/F a finite Galois extension with group G, and $C \subset G$ a conjugacy class. Further we fix an element $t \in F^*$ which is no root of unity. If $\underline{p}$ is a finite (i.e. non-archimedean) prime of F we say that t is a primitive root (p.r.) mod $\underline{p}$ if $\mathrm{ord}_{\underline{p}}(t) = 0$ and the image of t in the residue class field $\bar{F}_{\underline{p}}$ of $\underline{p}$ generates $\bar{F}^*_{\underline{p}}$. Here $\mathrm{ord}_{\underline{p}}$ denotes the normalized exponential valuation induced by $\underline{p}$. We are interested in the set

$$\begin{aligned} M_{t,C} = \{\underline{p} \mid \underline{p} & \text{ is a finite prime of } F, \\ & t \text{ is a primitive root mod } \underline{p}, \\ & \text{and } (\underline{p},E/F) = C\} \end{aligned}$$

where $(\underline{p},E/F)$ is the Artin symbol.

If m is a squarefree positive integer not divisible by $\mathrm{char}(F)$, we put $L_m = F(\zeta_m, \sqrt[m]{t})$, where ζ_m denotes a primitive m-th root of unity. Clearly L_m/F is Galois, and $L_m \cdot L_{m'} = L_{m \cdot m'}$ for $(m,m') = 1$.

(12.1) Lemma. Let $\underline{p}$ be a finite prime of F with $\mathrm{ord}_{\underline{p}}(t) = 0$, and if F is a number field assume $\mathrm{ord}_{\underline{p}}(2.\Delta_{F/\underline{Q}}) = 0$, where $\Delta_{F/\underline{Q}}$ denotes the discriminant of F over $\underline{Q}$. Then t is a p.r. mod $\underline{p}$ if and only if for all prime numbers $\ell \neq \mathrm{char}(F)$ we have $(\underline{p},L_\ell/F) \neq \mathrm{id}$ (we understand $(\underline{p},L_\ell/F) \neq \mathrm{id}$ also to be valid if $\underline{p}$ ramifies in L_ℓ; id is the identity element of $\mathrm{Gal}(L_\ell/F)$).

Proof. "If": if t is no p.r. mod $\underline{p}$, then for some prime number ℓ dividing $\# \bar{F}^*_{\underline{p}}$ we have $(t \bmod \underline{p}) \in \bar{F}^{*\ell}_{\underline{p}}$. But since $\mathrm{ord}_{\underline{p}}(\ell) = 0 = \mathrm{ord}_{\underline{p}}(t)$ this exactly means that $\underline{p}$ splits completely in L_ℓ, contradiction.

"Only if". Let t be p.r. mod $\underline{p}$, and let $\ell \neq \mathrm{char}(F)$ be a prime number. If $\mathrm{ord}_{\underline{p}}(\ell \cdot 1) > 0$ then F is a number field and the condition $\underline{p} \nmid 2 \cdot \Delta_{F/\underline{Q}}$ implies that $\underline{p}$ ramifies in L_ℓ by the presence of the ℓ-th roots of unity in L_ℓ. If $\mathrm{ord}_{\underline{p}}(\ell \cdot 1) = 0$ and $(\underline{p},L_\ell/F) = \mathrm{id}$, then $\bar{F}_{\underline{p}}$ contains the ℓ-th roots of unity and an ℓ-th root of (t mod $\underline{p}$), so t cannot be p.r. mod $\underline{p}$, contradiction. $\square$

Note that some condition on $\underline{p}$ is necessary: -7 is p.r. mod 2, but 2 splits in $\underline{Q}(\sqrt{-7})$.

We conclude that $M_{t,C}$ differs only by a finite set from

$$\{\underline{p} \mid (\underline{p},E/F) = C \text{ and } (\underline{p},L_\ell/F) \neq \text{id for all primes } \ell \neq \text{char}(F)\}.$$

The determination of the Dirichlet density would be easy if $(\underline{p},L_\ell/F) \neq \text{id}$ would be required for only finitely many primes:

(12.2) Lemma. Let m be a squarefree positive integer not divisible by char(F). Then the set

$$\{\underline{p} \text{ prime} \mid (\underline{p},E/F) = C \text{ and } (\underline{p},L_\ell/F) \neq \text{id for all primes } \ell \mid m\}$$

has a Dirichlet density which is given by

$$\frac{1}{[L_m\cdot E:F]} \cdot \#\{\sigma \in \text{Gal}(L_m\cdot E/F) \mid (\sigma|E) \in C, \text{ and}$$
$$\sigma \notin \text{Gal}(L_m\cdot E/L_\ell) \text{ for all primes } \ell \mid m\}.$$

If we define, for $d \mid m$:

$$f(d) = \#(C \cap \text{Gal}(E/E \cap L_d)) \begin{cases} = \# C \text{ if } C \subset \text{Gal}(E/E \cap L_d) \\ = 0 \text{ else,} \end{cases}$$

then this density can also be expressed by

$$\sum_{d|m} \frac{\mu(d)\cdot f(d)}{[L_d\cdot E:\ F]}$$

where μ denotes the Moebius function. If the density is 0, then the set is finite.

Proof. The first expression for the Dirichlet density is immediate from Tchebotarev's theorem [26]. The second formula is immediate from the principle of in- and exclusion and the remark that the number of elements $\sigma \in \text{Gal}(L_m\cdot E/F)$ for which $(\sigma/E) \in C$ and $\sigma \in \text{Gal}(L_m\cdot E/L_{\ell_1}) \cap \ldots \cap \text{Gal}(L_m\cdot E/L_{\ell_s})$ precisely equals

$f(\ell_1 \ldots \ell_s) \cdot [L_m \cdot E : L_{\ell_1 \ldots \ell_s} \cdot E]$; here $\ell_1, \ldots, \ell_s$ are different primes dividing m.

If the density is 0 then all $\underline{p}$ in the set must ramify in $L_m \cdot E$ so then the set is finite. □

Letting m tend to infinity we arrive at a generalized form of Artin's conjecture [27,Preface]:

(12.3) Hypothesis. The set $M_{t,C}$ has a Dirichlet density which equals

$$\lim_{m} \sum_{d|m} \frac{\mu(d) \cdot f(d)}{[L_d \cdot E : F]}$$

the limit being taken over all squarefree m not divisible by char(F), ordered by divisibility. Here f(d) is as defined in (12.2).

The evidence for this hypothesis is as follows. For F a function field and E = F, C = {id}, Bilharz [28] proved (12.3) modulo the Riemann hypothesis for function fields. This hypothesis was shown to be correct by A. Weil [20,cf.21]. From what Bilharz actually proves [28,p.485] it is not hard to derive the more general result (12.3) in the function field case, cf. [18]. We conclude that (12.3) is a theorem in the function field case.

In the number field case (12.3) easily reduces to the case E is abelian over F, cf. [26,pp.169-170]. For E abelian over F, Weinberger [19,formula(6.2)] proves (12.3), with natural density instead of Dirichlet density, modulo the generalized Riemann hypothesis, making use of ideas of Hooley [29] (the assumption of Weinberger that t is a fundamental unit is doubtless irrelevant). We conclude that in the number field case (12.3) is a consequence of the generalized Riemann hypothesis.

Further references: [30,31,32,33,64].

We are interested in whether or not the density of $M_{t,C}$ is zero.

(12.4) Theorem. Assume (12.3). Then the following four assertions are equivalent (t and C are fixed):

(a) $M_{t,C}$ is an infinite set;

(b) the density of $M_{t,C}$ is positive;

(c) for every squarefree $m > 0$, $m \not\equiv 0 \bmod \mathrm{char}(F)$, there exists $\sigma \in \mathrm{Gal}(L_m \cdot E/F)$ such that

$(\sigma|E) \in C$,

$(\sigma|L_\ell) \neq \mathrm{id}$ for all primes $\ell|m$;

(d) let h be the product of those prime numbers $\ell \neq \mathrm{char}(F)$ for which $t \in F^{*\ell}$, and let n be the product of those prime numbers $\ell \neq \mathrm{char}(F)$ for which $L_\ell \subset E(\zeta_h)$; then there exists $\sigma \in \mathrm{Gal}(E(\zeta_h)/F)$ such that

$(\sigma|E) \in C$,

$(\sigma|L_\ell) \neq \mathrm{id}$ for all primes $\ell|n$.

Note that h and n in (d) are well-defined, since there are only finitely many primes ℓ with $t \in F^{*\ell}$, or $t \in E(\zeta_h)^{*\ell}$, respectively. Notice also that h divides n.

Proof of (12.4). (b) $\Rightarrow$ (a) and (c) $\Rightarrow$ (d) are obvious. Further (a) $\Rightarrow$ (c) is clear from (12.1) and (12.2). We prove (c) $\Rightarrow$ (b) and (d) $\Rightarrow$ (c) below.

(12.5) Lemma. Suppose F is a number field, and let T be the product of those prime numbers ℓ which satisfy one of the following conditions:

ℓ divides $2.\Delta_{E/\underline{Q}}$;

there is a finite prime $\underline{\ell}$ of F with $\mathrm{ord}_{\underline{\ell}}(\ell) > 0$ and $\mathrm{ord}_{\underline{\ell}}(t) \neq 0$;

$t \in F^{*\ell}$.

Then for every prime number q not dividing T we have

(i) $[L_q:F] = q(q-1)$;

(ii) if d is any squarefree number not divisible by q, then the fields L_q and $L_d \cdot E$ are linearly disjoint over F.

Proof of (12.5). (i) $[L_q:F]$ is divisible by q since $t \notin F^{*q}$, and $[F(\zeta_q):F] = q-1$ since $q \nmid \Delta_{E/\underline{Q}}$. Hence $[L_q:F] = q(q-1)$.

(ii) Since L_q/F is Galois it suffices to prove $L_q \cap L_d \cdot E = F$.

Let $M = L_q \cap L_d \cdot E$. Clearly, M/F is a solvable Galois extension, so if $M \neq F$ then there is an abelian subextension $F \subsetneq M' \subset M$. From $M' \subset L_d \cdot E$ we see that M'/F is only ramified at primes lying over prime numbers dividing d.T. Hence M'/F is unramified at primes lying over q.

But from $M' \subset L_q$ and M'/F abelian it follows that $M' \subset F(\zeta_q)$ (here we use (i) and $q \neq 2$). Since $F(\zeta_q)/F$ is totally ramified at all primes lying over q (by $q \nmid \Delta_{E/Q}$) we conclude $M' = F$, contradiction. Hence $M = F$, as required. □

Proof of (12.4), (c) ⇒ (b), in the number field case. Let T be as in (12.5). For $q \nmid T$ and d as in (12.5) (ii) we have

$$\mu(dq) = -\mu(d)$$

$$f(dq) = f(d)$$

$$[L_{dq} \cdot E : F] = q(q-1)[L_d \cdot E : F],$$

by linear disjointness. Therefore the limit in (12.3) becomes

$$\left(\sum_{d|T} \frac{\mu(d) f(d)}{[L_d \cdot E:F]}\right) \cdot \left(\prod_{q \nmid T} (1 - \frac{1}{q(q-1)})\right).$$

The second factor is a converging infinite product and clearly nonzero. The first factor is nonzero by (12.4) (c) (with m = T) and (12.2). Hence if we assume (12.3) then $M_{t,C}$ has indeed nonzero density.

We give a sketch of the proof of (c) ⇒ (b) in the function field case. Corresponding to lemma (12.5) we have:

(12.6) Lemma. Suppose F is a function field with finite field of constants k. Then there exists a positive squarefree integer T not divisible by char(F) with the following property.

Let $\bar{k}$ denote an algebraic closure of k and let $K = (E \cdot L_T) \cap \bar{k}$ denote the largest finite field contained in $E \cdot L_T$. Then for every squarefree integer $d > 0$ which is relatively prime to T.char(F) we have

$$[L_{dT}\cdot E:F] = d\cdot[K(\zeta_d):K] \cdot [L_T E:F].$$

Proof of (12.6): left to the reader. □

Now (12.4), (c) ⇒ (b) can be proved for function fields in the following way. Let T be as in (12.6), and put

$$C' = \{\tau \in \mathrm{Gal}(L_T\cdot E/F) \,|\, (\tau|E) \in C, \text{ and } \tau|L_\ell \neq \text{id for all primes } \ell|T\}.$$

From (c), with $m = T$, we know $C' \neq \emptyset$. For $\tau \in C'$ and d as in (12.6) we define

$$f_\tau(d) = 1 \text{ if } \exists\ \sigma \in \mathrm{Gal}(L_{dT}\cdot E/L_d) \text{ with } \sigma|L_T\cdot E = \tau,$$

$$f_\tau(d) = 0 \text{ else.}$$

Note that $f_\tau(d) = 1$ precisely when $\tau|L_d \cap (L_T\cdot E) = \text{id}$; but (12.6) implies $L_d \cap (L_T\cdot E) = F\cdot(K \cap k(\zeta_d))$ and it follows that f_τ is multiplicative: $f_\tau(d\cdot d') = f_\tau(d)\cdot f_\tau(d')$. Here we assume that k is the exact field of constants of F.

Using (12.2) and (12.6) we now can rewrite the limit in (12.3) as:

$$\frac{1}{[L_T\cdot E:F]} \cdot \lim_m \sum_{\tau\in C'} \sum_{d|m} \frac{\mu(d)f_\tau(d)}{d\cdot[K(\zeta_d):K]},$$

m ranging over the squarefree positive integers relatively prime to T.char(F). But for fixed $\tau \in C'$, it follows from theorems of Romanoff [34] and Heilbronn [35] (cf.[28,p.482]) that the limit

$$\lim_m \sum_{d|m} \frac{\mu(d)\cdot f_\tau(d)}{d\cdot[K(\zeta_d):K]}$$

exists and is positive (we need multiplicativity of $f_\tau(d)$ for Heilbronn's theorem). Summing over $\tau \in C'$ we find that the density of $M_{t,C}$ is positive, as required. This proves (c) ⇒ (b).

Proof of (12.4), (d) ⇒ (c). Let $\sigma \in \mathrm{Gal}(E(\zeta_h)/F)$ be as in (d), and let m be as in (c). Clearly it suffices to find an element $\varphi \in \mathrm{Gal}(L_m\cdot E(\zeta_h)/F)$ which satisfies

$$(\varphi|E(\zeta_h)) = \sigma$$
$$(\varphi|L_\ell) \neq \text{id} \quad \text{for all primes } \ell|m.$$

If ℓ divides n then $(\varphi|L_\ell) \neq$ id is automatic from $(\varphi|E(\zeta_h)) = \sigma$ and $(\sigma|L_\ell) \neq$ id. Hence there is no loss in generality if we assume that m and n are relatively prime.

Suppose there does not exist such a φ. Then choose an element $\varphi \in \mathrm{Gal}(L_m \cdot E(\zeta_h)/F)$ such that $(\varphi|E(\zeta_h)) = \sigma$ and such that the smallest prime ℓ dividing m for which $(\varphi|L_\ell) =$ id is largest possible. We derive a contradiction.

Let this smallest prime be called p, and let r be the product of all $\ell < p$ which divide m. We have

$$(\varphi|L_p) = \text{id}$$
$$(\varphi|L_\ell) \neq \text{id for all primes } \ell|r.$$

We distinguish two cases.

Case 1. $L_r \cdot E(\zeta_h) \subsetneqq L_p \cdot L_r \cdot E(\zeta_h)$. In this case we can choose $\tau \in \mathrm{Gal}(L_m \cdot E(\zeta_h)/L_r \cdot E(\zeta_h))$ such that $(\tau|L_p) \neq$ id. But then $\psi = \tau\varphi$ satisfies

$$(\psi|L_\ell) \neq \text{id} \quad \text{for all primes } \ell \leq p \text{ which divide } m,$$
$$(\psi|E(\zeta_h)) = \sigma,$$

contradicting the choice of φ.

Case 2. $L_p \subset L_r \cdot E(\zeta_h)$. If $\ell_1, \ldots, \ell_s$ are the primes dividing r, then $[L_r \cdot E(\zeta_h) : E(\zeta_h)]$ divides $(\ell_1 - 1)\cdot\ell_1 \ldots (\ell_s - 1)\cdot\ell_s$ which is not divisible by p. Hence $L_p \subset L_r \cdot E(\zeta_h)$ implies that $X^p - t$ must have a zero in $E(\zeta_h)$. If $X^p - t$ is irreducible over F, then normality of $E(\zeta_h)/F$ implies $L_p \subseteq E(\zeta_h)$ so $p|n$, contradicting that n and m are relatively prime. If $X^p - t$ is reducible over F, then $p|h$, and since h divides n this gives the same contradiction.

This concludes the proof of (12.4). □

The following corollary is needed in the next section. We note that in the function field case the conditions of (12.7) imply that the field E is linearly disjoint over F with all fields $L_m, m \not\equiv 0 \mod \mathrm{char}(F)$. This assumption simplifies the proof of (12.4), (c) ⇒ (b) a bit, cf. [18].

<u>(12.7) Corollary.</u> Assume the following.

(i) $t \notin F^{*\ell}$ for every prime number $\ell \neq \mathrm{char}(F)$;

(ii) E/F is abelian, and every prime $\underline{p}$ with $\mathrm{ord}_{\underline{p}}(t) \neq 0$ is unramified in E/F;

(iii) for every subextension $F \subsetneq E' \subset E$ there is a finite prime $\underline{p}$ of E' which ramifies in E'/F.

Assume moreover that $M_{t,C}$ is finite and that (12.3) holds. Then F is a number field, and there exists a prime number ℓ such that:

(iv) some finite prime $\underline{\ell}$ of F lying over ℓ ramifies in E;

(v) F contains a primitive ℓ-th root of unity;

(vi) if $C = \{\sigma\}$ then $L_\ell = F(\sqrt[\ell]{t})$ is contained in $E^\sigma = \{x \in E \mid \sigma(x) = x\}$;

(vii) $[E:F]$ is divisible by ℓ.

<u>Proof.</u> If $M_{t,C}$ is finite and (12.3) holds, then (12.4) (d) is not satisfied. Since $h = 1$ by (i), this means that there exists a prime number $\ell \neq \mathrm{char}(F)$ for which $L_\ell \subset E$ and $(\sigma | L_\ell) = \mathrm{id}$.

Then $F(\sqrt[\ell]{t})$ is contained in the abelian extension E and must therefore be normal: $F(\sqrt[\ell]{t}) = L_\ell$. We conclude that (v), (vi) and (vii) hold. Since $F \subset F(\sqrt[\ell]{t})$ is unramified at all finite primes $\underline{p}$ for which $\mathrm{ord}_{\underline{p}}(\ell \cdot 1) = \mathrm{ord}_{\underline{p}}(t) = 0$, it follows from (ii) and (iii) that some $\underline{\ell}$ satisfying $\mathrm{ord}_{\underline{\ell}}(\ell) \neq 0$ ramifies in $F(\sqrt[\ell]{t})$. This clearly implies (iv), and $\mathrm{ord}_{\underline{\ell}}(\ell) \neq 0$ implies that F is a number field. □

13. The theorem of Weinberger and Queen.

Let F be a global field, S a finite non-empty set of primes of F containing the archimedean ones, and $\underline{O}_S$ the ring of S-integers (§7). A divisor of F is a formal product $\underline{a} = \prod_{\underline{p}} \underline{p}^{m(\underline{p})}$, with $\underline{p}$ ranging over the set of finite primes of F and $m(\underline{p}) \in \mathbb{Z}$, $m(\underline{p}) = 0$ for almost all $\underline{p}$. We identify the group of fractional $\underline{O}_S$-ideals with the group of divisors $\underline{a} = \prod_{\underline{p}} \underline{p}^{m(\underline{p})}$ satisfying $m(\underline{p}) = 0$ for all $\underline{p} \in S - S_\infty$. In particular, the prime ideals of $\underline{O}_S$ are identified with the primes of F outside S. In this section (0) is not considered as a prime ideal of $\underline{O}_S$.

(13.1) Theorem (Weinberger,Queen). Suppose that $\underline{O}_S$ is a principal ideal domain and that $\# S \geqslant 2$, and assume hypothesis (12.3). Then $\underline{O}_S$ is euclidean, and the smallest algorithm θ on $\underline{O}_S$ is given by

$$\theta(x) = \sum_{\underline{p} \notin S} \mathrm{ord}_{\underline{p}}(x) \cdot n_{\underline{p}}, \ x \neq 0, \ \theta(0) = \omega,$$

where $n_{\underline{p}} = 1$ if $\underline{O}_S^* \to (\underline{O}_S/\underline{p})^*$ is surjective and $n_{\underline{p}} = 2$ else.

Remark. It is not hard to see that (13.1) is also valid if S is infinite.

Proof. We prove, modulo (12.3), that the function θ defined in the theorem is an algorithm on $\underline{O}_S$. From (2.6) and (3.4) it then follows easily that θ is actually the smallest algorithm on $\underline{O}_S$.

Let $a,b \in \underline{O}_S$; we look for an element $r \in a + \underline{O}_S \cdot b$ such that $r = 0$ or $\theta(r) < \theta(b)$. Clearly we may asssume $b \neq 0$. Since $\underline{O}_S$ is a principal ideal domain there exists $d \in \underline{O}_S$ with $\underline{O}_S \cdot d = \underline{O}_S \cdot a + \underline{O}_S \cdot b$; let $a = a_1 d$ and $b = b_1 d$. From $\theta(xd) = \theta(d) + \theta(x)$, for $x \in \underline{O}_S$, we see that it suffices to find $r_1 \in a_1 + \underline{O}_S \cdot b_1$ with $r_1 = 0$ or $\theta(r_1) < \theta(b_1)$. This means that we may assume $(a,b) = 1$. We distinguish four cases.

Case 1. $\theta(b) = 0$. Then b is a unit and we can take $r = 0$.

Case 2. $\theta(b) = 1$. Then $\underline{O}_S \cdot b = \underline{p}$ is a prime ideal of $\underline{O}_S$ with $n_{\underline{p}} = 1$.

Therefore $\underline{O}_S^* \to (\underline{O}_S/\underline{O}_S\cdot b)^*$ is surjective and we can find $r \in \underline{O}_S^*$ with $r \equiv a$ mod $\underline{O}_S\cdot b$. Clearly $\theta(r) = 0 < 1 = \theta(b)$.

Case 3. $\theta(b) \geqslant 3$. By a suitable generalization of Dirichlet's theorem on primes in arithmetic progressions [26] we know that every residue class $C \in (\underline{O}_S/\underline{O}_S\cdot b)^*$ contains infinitely many elements π such that $\underline{O}_S\cdot\pi$ is a prime ideal. In particular the residue class $a + \underline{O}_S\cdot b$ contains an element r such that $\underline{O}_S\cdot r = \underline{p}$ is prime. Then $\theta(r) = n_{\underline{p}} \leqslant 2 < \theta(b)$, as required.

Case 4. $\theta(b) = 2$. Then the ideal $\underline{O}_S\cdot b = \underline{b}$ is of one of the following three types:

(13.2) $\underline{b} = \underline{\ell}$ with $\underline{\ell}$ prime and $n_{\underline{\ell}} = 2$;

(13.3) $\underline{b} = \underline{\ell}\cdot\underline{m}$ with $\underline{\ell} \neq \underline{m}$ primes and $n_{\underline{\ell}} = n_{\underline{m}} = 1$;

(13.4) $\underline{b} = \underline{\ell}^2$ with $\underline{\ell}$ prime and $n_{\underline{\ell}} = 1$.

Let $\mathrm{im}(\underline{O}_S^*)$ denote the image of $\underline{O}_S^*$ under the natural map $\underline{O}_S^* \to (\underline{O}_S/\underline{b})^*$, and let $\bar{a}$ be the image of a in $(\underline{O}_S/\underline{b})^*/\mathrm{im}(\underline{O}_S^*)$. Suppose we are able to find a prime ideal $\underline{r}$ of $\underline{O}_S$, not dividing $\underline{b}$, such that the following two conditions are satisfied:

(13.5) the map $\underline{O}_S^* \to (\underline{O}_S/\underline{r})^*$ is surjective;

(13.6) if $\underline{r} = \underline{O}_S\cdot r$ then the image of r in $(\underline{O}_S/\underline{b})^*/\mathrm{im}(\underline{O}_S^*)$ equals $\bar{a}$ (note that this image only depends on $\underline{r}$).

Then we can choose r in (13.6) in such a way that $r \in a + \underline{O}_S\cdot b$, and (13.5) guarantees $\theta(r) = n_{\underline{r}} = 1 < 2 = \theta(b)$, as required.

We first reduce the problem of finding primes $\underline{r}$ which satisfy (13.5) and (13.6) to the question considered in section 12.

Since S contains at least two elements, the group of units $\underline{O}_S^*$ contains a "fundamental" unit t, i.e. $t \notin F^{*\ell}$ for every prime ℓ. It is clear that condition (13.5) is satisfied if t is a primitive root mod $\underline{r}$.

Condition (13.6) is by the following lemma equivalent to

$$(\underline{r}, E/F) = C$$

for a suitable Galois extension $F \subset E$ and a suitable conjugacy class $C \subset \mathrm{Gal}(E/F)$.

(13.7) Lemma. There exists an abelian extension $F \subset E$ with the following properties:

(i) the groups $(\underline{O}_S/\underline{b})^*/\mathrm{im}(\underline{O}_S^*)$ and $\mathrm{Gal}(E/F)$ are naturally isomorphic, and if $\sigma \in \mathrm{Gal}(E/F)$ corresponds to $\bar{a}$, then (13.6) is equivalent to

$$(\underline{r}, E/F) = \sigma.$$

(ii) E/F is unramified at all infinite primes and at all finite primes not dividing $\underline{b}$.

(iii) for every intermediate field $F \subsetneq E' \subset E$ there exists a prime of F ramifying in E'/F.

Proof. We need class field theory [36,26]. Let $I(\underline{b})$ be the group of divisors of F which are "prime to $\underline{b}$":

$$I(\underline{b}) = \{\prod_{\underline{p}} \underline{p}^{m(\underline{p})} \mid m(\underline{p}) = 0 \text{ for all } \underline{p} \notin S \text{ dividing } \underline{b}\}.$$

Let I_S be the subgroup of $I(\underline{b})$ consisting of all divisors based on the finite members of S:

$$I_S = \{\prod_{\underline{p} \in S - S_\infty} \underline{p}^{m(\underline{p})} \mid m(\underline{p}) \in \underline{Z}\}.$$

For $x \in F^*$ the principal divisor (x) is defined by

$$(x) = \prod_{\underline{p}} \underline{p}^{\mathrm{ord}_{\underline{p}}(x)} .$$

Finally we define

$$P_{\underline{b}} = \{(x) \mid x \in F^*, \text{ and } \mathrm{ord}_{\underline{p}}(x-1) \geqslant \mathrm{ord}_{\underline{p}}(\underline{b})$$
$$\text{for all } \underline{p} \notin S \text{ dividing } \underline{b}\}.$$

The subgroup $I_S \cdot P_{\underline{b}} \subset I(\underline{b})$ is an ideal group in the sense of class field theory, so there exists a finite abelian extension $F \subset E$ such that the Artin reciprocity map gives an isomorphism

$$I(\underline{b})/I_S \cdot P_{\underline{b}} \cong \mathrm{Gal}(E/F).$$

It is clear that this field E satisfies condition (ii). More precisely:

(13.8) the conductor of E/F divides $\underline{b}$.

We prove (iii). Let

$$P(\underline{b}) = \{(x) \mid x \in F^*, \ (x) \in I(\underline{b})\}.$$

We claim

(13.9) $\quad I(\underline{b}) = I_S \cdot P(\underline{b})$.

In fact, let $\underline{a} = \prod_{\underline{p}} \underline{p}^{m(\underline{p})} \in I(\underline{b})$. Since $\underline{O}_S$ is a principal ideal domain there exists $x \in F^*$ with

$$\mathrm{ord}_{\underline{p}}(x) = m(\underline{p}) \qquad \text{for all } \underline{p} \notin S.$$

Then $\underline{a} = \underline{a}' \cdot (x)$ where $\underline{a}' \in I_S$ and $(x) \in P(\underline{b})$, as required.

A fortiori, we have

$$I(\underline{b}) = (I_S \cdot P_{\underline{b}}) \cdot P(\underline{b}).$$

Translating this statement about ideal groups in one about their class fields we find

$$F = E \cap (\text{maximal abelian unramified extension of } F).$$

This is exactly condition (iii).

To prove (i), first note

$$P(\underline{b}) \cap I_S = \{(x) \mid x \in \underline{O}_S^*\}.$$

Using (13.9) this yields

$$\mathrm{Gal}(E/F) \cong I(\underline{b})/I_S \cdot P_{\underline{b}} \cong I_S \cdot P(\underline{b})/I_S \cdot P_{\underline{b}}$$

$$\cong P(\underline{b})/(P(\underline{b}) \cap I_S) \cdot P_{\underline{b}}$$

$$\cong P(\underline{b})/\{(x)\,|\,x \in \underline{O}_S^*\}\cdot P_{\underline{b}}$$
$$\cong (\underline{O}_S/\underline{b})^*/\mathrm{im}(\underline{O}_S^*)$$

the last isomorphism being straightforward. The verification of the rest of (i) is immediate. This proves (13.7). □

Using the remarks preceding the lemma we arrive at the following conclusion.

Conclusion. Let E and σ be as in (13.7). Then there exists a prime ideal $\underline{r}$ of $\underline{O}_S$, not dividing $\underline{b}$, which satisfies (13.5) and (13.6), if there exists a fundamental unit $t \in \underline{O}_S^*$ such that $M_{t,\{\sigma\}}$ is infinite; here $M_{t,\{\sigma\}}$ is as in §12.

Hence assume that $M_{t,\{\sigma\}}$ is finite, for fixed t. We apply (12.7), the conditions of which are satisfied by the choice of t and by (13.7)(ii),(iii). We conclude first of all that F is a number field. So we have dealt with the function field case without using that $\underline{b}$ has one of the types (13.2-4). Further, we conclude (modulo (12.3)):

(13.10) some prime dividing $\underline{b}$ lies over ℓ;

(13.11) $\zeta_\ell \in F$;

(13.12) $F(\sqrt[\ell]{t}) \subset E^\sigma$;

(13.13) $[E:F]$ is divisible by ℓ.

We distinguish three cases, according to the type of $\underline{b}$.

Case a. $\underline{b} = \underline{\ell}$ with $\underline{\ell}$ prime and $n_{\underline{\ell}} = 2$.

In this case (13.10) implies $\underline{\ell}|\ell$, hence $\ell = \mathrm{char}(\underline{O}_S/\underline{\ell})$. By (13.7)(i), the degree $[E:F]$ divides $\#(\underline{O}_S/\underline{\ell})^*$ which is $\ell^f - 1$ for some $f > 0$. This contradicts (13.13).

Case b. $\underline{b} = \underline{\ell}\cdot\underline{m}$ with $\underline{\ell} \neq \underline{m}$ primes and $n_{\underline{\ell}} = n_{\underline{m}} = 1$. In this case (13.10) implies $\underline{\ell}|\ell$ or $\underline{m}|\ell$, say $\underline{\ell}|\ell$. The degree $[E:F]$ equals $\#(\underline{O}_S/\underline{b})^*/\mathrm{im}(\underline{O}_S^*)$. But $(\underline{O}_S/\underline{b})^* \cong (\underline{O}_S/\underline{\ell})^* \times (\underline{O}_S/\underline{m})^*$, and $\mathrm{im}(\underline{O}_S^*)$ projects onto the second factor since $n_{\underline{m}} = 1$. Therefore $\#(\underline{O}_S/\underline{b})^*/\mathrm{im}(\underline{O}_S^*)$ divides $\#(\underline{O}_S/\underline{\ell})^*$ which is $\ell^f - 1$ for some

$f > 0$. This again contradicts (13.13).

Case c. $\underline{b} = \underline{\ell}^2$ with $\underline{\ell}$ prime and $n_{\underline{\ell}} = 1$.

Again ℓ is the unique prime number divisible by $\underline{\ell}$. The set $M_{t,\{\sigma\}}$ can very well be finite (cf.below); if it is finite for all t, then (13.12) sharpens to

(13.14) $$F(\sqrt[\ell]{O^*_{\underline{S}}}) \subset E^{\sigma}$$

since $O^*_{\underline{S}}$ is generated by the fundamental units.

The group Gal(E/F) is isomorphic to $(O_{\underline{S}}/\underline{\ell}^2)^*/\mathrm{im}(O^*_{\underline{S}})$; since $O^*_{\underline{S}}$ projects onto $(O_{\underline{S}}/\underline{\ell})^*$ this is a factor group of $\mathrm{Ker}((O_{\underline{S}}/\underline{\ell}^2)^* \to (O_{\underline{S}}/\underline{\ell})^*)$ which is an elementary abelian ℓ-group. Therefore Kummer theory and (13.11) give us

(13.15) $E = F(\sqrt[\ell]{a_1},\dots,\sqrt[\ell]{a_n})$ for some $n \geq 0$, and $a_i \in F^* - F^{*\ell}$.

Fix i, $1 \leq i \leq n$, for the moment. Since E/F is unramified outside $\underline{\ell}$ we have $\ell \mid \mathrm{ord}_{\underline{p}}(a_i)$ for all finite primes $\underline{p} \neq \underline{\ell}$. But $O_{\underline{S}}$ is a principal ideal domain, so we can modify a_i by an ℓ-th power so as to achieve

(13.16) $\mathrm{ord}_{\underline{p}}(a_i) = 0$ for all $\underline{p} \notin S \cup \{\underline{\ell}\}$

$$0 \leq \mathrm{ord}_{\underline{\ell}}(a_i) \leq \ell-1 .$$

We claim $\mathrm{ord}_{\underline{\ell}}(a_i) = 0$. Suppose this is false. We compute the conductor $\underline{f}_i$ of $F(\sqrt[\ell]{a_i})/F$. Since this extension is cyclic of prime degree, $\underline{f}_i$ equals the conductor of any one of its non-trivial characters. Taking the product over all characters we find by the conductor-discriminant product formula

$$\underline{f}_i^{\ell-1} = \text{discriminant } (F(\sqrt[\ell]{a_i})/F).$$

But if $\mathrm{ord}_{\underline{\ell}}(a_i) \neq 0$ then over the $\underline{\ell}$-adic completion $F_{\underline{\ell}}$ of F we have

$$F_{\underline{\ell}}(\sqrt[\ell]{a_i}) = F_{\underline{\ell}}(\sqrt[\ell]{\pi}),$$

for some $\pi \in F_{\underline{\ell}}$ with $\mathrm{ord}_{\underline{\ell}}(\pi) = 1$. Since $X^{\ell} - \pi$ has discriminant $\pm \ell^{\ell}\pi^{\ell-1}$ and

and since there is no ramification outside $\underline{\ell}$ we conclude

$$\text{discriminant } (F(\sqrt[\ell]{a_i})/F) = \underline{\ell}^{\ell\cdot\mathrm{ord}_{\underline{\ell}}(\ell)+\ell-1}$$

so

$$\underline{f}_i = \underline{\ell}^{(\ell\cdot e/(\ell-1))+1}, \quad \text{where} \quad e = \mathrm{ord}_{\underline{\ell}}(\ell).$$

From $F(\sqrt[\ell]{a_i}) \subset E$ and (13.8) we know that $\underline{f}_i$ divides $\underline{b} = \underline{\ell}^2$. Hence $(\ell\cdot e/(\ell-1)) + 1 \leq 2$ which is a contradiction. This proves $\mathrm{ord}_{\underline{\ell}}(a_i) = 0$.

By (13.16) we now have $a_i \in \underline{O}_S^*$, which by (13.15) implies $E \subset F(\sqrt[\ell]{\underline{O}_S^*})$. Combination with (13.14) shows $E^\sigma = E$ so $\sigma \in \mathrm{Gal}(E/F)$ is the identity element. By (13.7)(i) this means that $\bar{a}$ is the identity of $(\underline{O}_S/\underline{b})^*/\mathrm{im}(\underline{O}_S^*)$ so there exists an element $r \in a + \underline{O}_S\cdot b$ for which $r \in \underline{O}_S^*$. Clearly $\theta(r) = 0 < 2 = \theta(b)$, as required. This proves theorem (13.1). □

An example which shows that in case (c) the set $M_{t,\{\sigma\}}$ can be empty for *all* $t \in \underline{O}_S^*$ is given by

$$F = \underline{Q}(\zeta_5),\ S = S_\infty,\ \underline{\ell} = (2),\ \underline{b} = (4),\ \sigma = \mathrm{id}.$$

14. The theorem of O'Meara.

In this section F denotes a number field of degree n and discriminant Δ over $\mathbb{Q}$. By r_1 and r_2 we mean the number of real and complex archimedean primes of F, respectively. We write B for the Minkowski constant

$$B = \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^{r_2} \cdot \sqrt{|\Delta|}$$

where π denotes the Ludolphsche Zahl. Finally, $\underline{O} = \underline{O}_{S_\infty}$.

(14.1) Theorem. Let $\omega_0, \omega_1, \ldots, \omega_{[B]}$ be $[B] + 1$ different elements of the ring of integers $\underline{O}$ of F. Then the ring

$$\underline{O}\left[(\omega_i - \omega_j)^{-1} \mid 0 \leq i < j \leq [B]\right] = \underline{O}_S$$

where

$$S = S_\infty \cup \{\, \underline{p} \mid \underline{p} \text{ is a finite prime dividing } \prod_{i<j} (\omega_i - \omega_j)\}$$

is norm-euclidean.

Proof. First we recall the classical geometry of numbers approach. Embed F in the $\mathbb{R}$-algebra $F_{\mathbb{R}} = F \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Let $\mu_{\mathbb{R}}$ be the Haar measure on $\mathbb{R}$ such that $\mu_{\mathbb{R}}([0,1]) = 1$, as usual, let $\mu_{\mathbb{C}}$ be the Haar measure on $\mathbb{C}$ for which $\mu_{\mathbb{C}}([0,1] + [0,1] \cdot i) = 2$ (this is twice the usual one), and let μ be the product measure on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = F_{\mathbb{R}}$.

The ring $\underline{O}$ is a lattice of rank n in $F_{\mathbb{R}}$. Let D be a measurable subset of $F_{\mathbb{R}}$ which is a fundamental domain for $\underline{O}$, i.e. the natural map $D \to F_{\mathbb{R}}/\underline{O}$ is bijective. It is well known that $\mu(D) = \sqrt{|\Delta|}$. We define

$$U = \{(x_i)_{i=1}^{r_1+r_2} \in F_{\mathbb{R}} \mid \Sigma_{i=1}^{r_1} |x_i| + 2 \cdot \Sigma_{i=r_1+1}^{r_1+r_2} |x_i| < \tfrac{1}{2} n\}.$$

A classical computation shows

$$\mu(U) = (\tfrac{\pi}{4})^{r_2} \cdot \frac{n^n}{n!}, \quad \text{so} \quad B\cdot\mu(U) = \mu(D),$$

and the arithmetic-geometric mean inequality implies

(14.2) $u,\ v \in U \Rightarrow N(u-v) < 1.$

Here we mean by N the function

$$N(x) = \prod_{i=1}^{r_1} |x_i| \cdot \prod_{i=r_1+1}^{r_1+r_2} |x_i|^2, \quad x=(x_i)_{i=1}^{r_1+r_2} \in F_{\underline{R}},$$

which on F restricts to the absolute value of the field norm $F \to \underline{Q}$ and coincides with the S_∞-norm N_{S_∞} defined in § 7.

We turn to the proof of the theorem. Given $x \in F$ we have to find $q \in \underline{O}_S$ such that $N_S(x-q) < 1$, by (9.7).

The strong approximation theorem asserts the existence of an $x' \in F$ for which

(14.3) $\text{ord}_{\underline{p}}\ (x-x') \geq 0$ for all $\underline{p} \in S-S_\infty$,

$\text{ord}_{\underline{p}}\ (x') \geq 0$ for all $\underline{p} \notin S$.

Then $x' \in \underline{O}_S$ so $\{ x-q \mid q \in \underline{O}_S \} = \{ (x-x') - q \mid q \in \underline{O}_S \}$.

Hence we may replace x by $x-x'$ without changing the problem, and by (14.3) this means that we may assume

$$\text{ord}_{\underline{p}}\ (x) \geq 0 \qquad \text{for all } \underline{p} \in S-S_\infty$$

so

(14.4) $|x|_{\underline{p}} \leq 1$ for all $\underline{p} \in S-S_\infty$.

Consider the $[B] + 1$ sets $x\cdot\omega_i + U$. The sum of their volumes equals

$$\Sigma_{i=0}^{[B]}\ \mu(x\omega_i+U) = ([B]+1)\cdot\mu(U) > B\cdot\mu(U) = \mu(D)$$

which means that the natural map

$$\bigcup_{i=0}^{[B]} (x\omega_i + U) \to F_{\underline{R}}/\underline{O} \cong D$$

cannot be injective. Hence there are i, j, and u, v $\in$ U such that

$$x\omega_i + u \neq x\omega_j + v$$

$$x\omega_i + u \equiv x\omega_j + v \bmod \underline{O}.$$

If we would have $i = j$ then $u-v \in \underline{O} - \{0\}$ so $N(u-v) \geqslant 1$, contradicting (14.2). Therefore $i \neq j$ and

$$x\cdot(\omega_i-\omega_j) - y = v-u, \quad \text{for some } y \in \underline{O}.$$

We claim that $q = y \,/\, (\omega_i-\omega_j)$ satisfies

(14.5) $\quad N_S\ (x-q) < 1$

which solves our problem since $q \in \underline{O}_S$. To prove the claim, we note first that

$$N_S\ (x-q) = N_S\ (x\cdot(\omega_i-\omega_j)-y)$$

since $(\omega_i-\omega_j) \in \underline{O}_S^*$; secondly, (14.4) implies $|x\cdot(\omega_i-\omega_j)-y|_{\underline{p}} \leqslant 1$ for all $\underline{p} \in S-S_\infty$ and therefore

$$N_S\ (x\cdot(\omega_i-\omega_j)-y) \leqslant N_{S_\infty}\ (x\cdot(\omega_i-\omega_j)-y)$$

and thirdly we have

$$N_{S_\infty}(x\cdot(\omega_i-\omega_j)-y) = N_{S_\infty}(v-u) < 1$$

by (14.2). Combining these three remarks we immediately get (14.5). □

Compare [37].

(14.6) Corollary. Let $S=S_\infty \cup \{\underline{p} \text{ finite} \mid \#(\underline{O}/\underline{p}) \leqslant [B]\cdot B\}$; then $\underline{O}_S$ is norm-euclidean.

Proof. Let $E = [[B]\cdot B]$. Then $(E+1)\cdot\mu(U) > [B]\cdot\mu(D)$ so we can choose $t \in \underline{R}_{>0}$ such that

$$(E+1)\cdot\mu(U) > t^n\cdot\mu(U) = \mu(tU) > [B]\cdot\mu(D).$$

Consider the natural map

$$tU \to F_{\underline{R}} \,/\, \underline{O} \cong D.$$

If each point of D is the image of at most $[B]$ elements of tU, then we would have $\mu(tU) \leq [B]\cdot\mu(D)$, contradiction. Hence there exist $[B] + 1$ different elements $v_0,\ldots,v_{[B]}$ of tU which map to the same point in D, i.e.

$$v_i - v_j \in \underline{O} - \{0\}, \quad \text{for } 0 \leq i < j \leq [B].$$

Now apply (14.1) to the elements $\omega_i = v_i - v_0$ of $\underline{O}$, for $0 \leq i \leq [B]$; then we find that $\underline{O}_{S'}$ is euclidean for

$$S' = S_\infty \cup \{\underline{p} \text{ finite} \mid \exists\ i<j: \omega_i - \omega_j \in \underline{p}\}.$$

For each $\underline{p} \in S'-S_\infty$ there are $i \neq j$ with $\omega_i - \omega_j \in \underline{p}$ so using (14.2) we get

$$\#(\underline{O}/\underline{p}) \leq \#(\underline{O}/\underline{O}(\omega_i - \omega_j)) = N(\omega_i - \omega_j) < t^n < E + 1.$$

Since $\#(\underline{O}/\underline{p})$ is an integer this means $\#(\underline{O}/\underline{p}) \leq E$ and $\underline{p} \in S$. Hence we proved $S' \subset S$, and since $\underline{O}_{S'}$ is norm-euclidean it follows easily from (3.6) that also $\underline{O}_S$ is norm-euclidean. □

(14.7) Corollary. Let T be a finite set of finite primes of F, such that $\#(\underline{O}/\underline{p}) > B$ for all $\underline{p} \in T$. Then there is a finite set S of primes of F, containing S_∞, such that $S \cap T = \emptyset$ and such that $\underline{O}_S$ is norm-euclidean.

Proof. Using the Chinese remainder theorem one chooses $\omega_0,\ldots,\omega_{[B]} \in \underline{O}$ such that $\omega_i \not\equiv \omega_j \bmod \underline{p}$ for all $i<j$ and all $\underline{p} \in T$. Then (14.7) is immediate from (14.1). □

It is unknown whether the restriction " $\#(\underline{O}/\underline{p}) > B$ for all $\underline{p} \in T$ " can be missed or not. It is easily seen to be superfluous if one only requires $\underline{O}_S$ to be a principal ideal domain.

An instructive example is the ring $\underline{Z}\left[\sqrt{-5}, \frac{1}{3}\right]$. Methods analogous to those used above show that this ring is norm-euclidean (cf. Wedderburn, [38, p. 138]), but this cannot be proved by means of theorem (14.1): one has $[B] = 2$, and the prime lying over 2 divides any product $(\omega_0 - \omega_1)(\omega_0 - \omega_2)(\omega_1 - \omega_2)$, where $\omega_i \in \underline{Z}\,[\sqrt{-5}]$.

Let the constants M and M' be defined by

$$M = \max \{ m \mid \text{there are } \omega_i \in \underline{O}, \text{ for } 1 \leq i \leq m, \text{ such that } \omega_i - \omega_j \in \underline{O}^* \text{ for all } 1 \leq i < j \leq m \},$$

$$M' = \min \{ \# (\underline{O}/\underline{a}) \mid \underline{a} \subsetneq \underline{O} \text{ is an ideal} \}.$$

One proves easily $2 \leq M \leq M' \leq 2^n$, and (14.1) immediately gives:

(14.8) Corollary. If $B < M$ then $\underline{O}$ is norm-euclidean. □

This compares nicely with a classical result of Minkowski: if $B < M'$ then $\underline{O}$ is a principal ideal domain.

It is an amusing exercise to show that $B \neq M$ for all number fields F. Hence in (14.8) we can replace $B < M$ by $B \leq M$.

The following proposition is slightly sharper than (14.8):

(14.9) Proposition. Let $R \subset F$ be a subring which is integral over $\underline{Z}$ and has F as its field of fractions. Let Δ_R be the discriminant or R over $\underline{Z}$ and put

$$B_R = \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^{r_2} \cdot \sqrt{|\Delta_R|},$$

$$M_R = \max \{ m \mid \text{there are } \omega_i \in R, \text{ for } 1 \leq i \leq m, \text{ such that } \omega_i - \omega_j \in R^* \text{ for all } 1 \leq i < j \leq m \}.$$

Suppose $M_R > B_R$. Then R is euclidean with algorithm

$$\psi(x) = \# (R/Rx), \quad x \neq 0, \qquad \psi(0) = \omega.$$

Remark. Of course (14.9) is not more general than (14.8) in the sense that the only R which can possibly satisfy the conditions of (14.9) is $R = \underline{O}$ (any euclidean domain is integrally closed); but (14.9) is more convenient in the applications since one need not show beforehand that the order R to be proved euclidean is actually the maximal order $\underline{O}$.

Proof of (14.9). The proof of (14.1) carries over without problems. One just notes the formula

$$\# (R/Rx) = N(x), \qquad x \in R - \{0\},$$

and the fact that the part of the proof concerned with (14.4) can be forgotten since $S=S_\infty$. □

Examples. Let $F = \mathbb{Q}(\zeta_p)$, where p is prime and ζ_p is a primitive p-th root of unity. We have

$$B = \frac{(p-1)!}{(p-1)^{p-1}} \cdot \left(\frac{4}{\pi}\right)^{(p-1)/2} \cdot p^{(p-2)/2} \qquad (p \geqslant 3)$$

and $M' = p$. Consideration of the elements $\omega_i = (\zeta_p^i - 1)/(\zeta_p - 1)$ (for $1 \leqslant i < p$) shows that we also have $M = p$. One easily checks

$$B < p \qquad \text{for} \quad p = 3, 5, 7,$$

so it follows that the rings $\mathbb{Z}[\zeta_3]$, $\mathbb{Z}[\zeta_5]$ and $\mathbb{Z}[\zeta_7]$ are norm-euclidean. For $p = 11$ we have $B > p$, although $\mathbb{Z}[\zeta_{11}]$ is known to be norm-euclidean (cf. § 15).

Some other examples:

$R = \mathbb{Z}[\alpha]$, where:	n	r_2	B_R	M'	M_R
$\alpha^4 = \alpha + 1$	4	1	2.008	7	$\geqslant 6$
$\alpha^5 = 2\alpha + 1 \neq -1$	4	1	2.832	3	3
$\alpha^5 = \alpha + 1$	5	2	3.334	4	4
$\alpha^6 = \alpha^2 + 1$	6	2	4.603	8	8

The last column is obtained by considering sequences of the form $(0, 1, \alpha, \ldots, \alpha^n)$. It follows that each one of these rings is norm-euclidean.

15. Norm-euclidean number rings.

In this section we survey the number fields F the ring of integers of which is known to be norm-euclidean. Let n, r_1, r_2 be as in section 14.

For n = 1 there is only F = $\underline{Q}$.

For n = 2, $r_1 = 0$, $r_2 = 1$ there are F = $\underline{Q}(\sqrt{\Delta})$ where $\Delta = -3, -4, -7, -8, -11$, and as we have seen in §8 this list is complete.

For n = 2, $r_1 = 2$, $r_2 = 0$ there are F = $\underline{Q}(\sqrt{\Delta})$ with Δ = 5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 57, 73, 76. A theorem of Chatland and Davenport asserts that this list is complete [39,40,41].

For n = 3, $r_1 = 1$, $r_2 = 1$ it is known that there are only finitely many such F, see [42,43]. The known ones are those with discriminants, -23, -31, -44, -59, -76, -83, -87, -104, -107, -108, -116, -135, -139, -140, -152 [44].

For n = 3, $r_1 = 3$, $r_2 = 0$ it is known that there are only finitely many examples which are Galois extensions of Q, see [45,46]. The known ones [47,48] have discriminants 7^2, 9^2, 13^2, 19^2, 31^2, 37^2, 43^2, 61^2, 67^2. For F/$\underline{Q}$ not Galois there are examples [47,53] with discriminants 148, 229, 257, 316 and 44 others (discriminants ranging from 321 to 1994) which were found with the help of a computer.

For n = 4, $r_1 = 0$, $r_2 = 2$ the number of examples is finite [42,49]. In [50] one finds 30 non-isomorphic examples which are quadratic over a totally imaginary quadratic extension of $\underline{Q}$;among these examples are $\underline{Q}(\zeta_8)$ and $\underline{Q}(\zeta_{12})$. The only other known one in this category is $\underline{Q}(\zeta_5)$, see [51,pp.228-231; 52].

For n = 4, $r_1 = 2$, $r_2 = 1$ only the two examples mentioned at the end of §14 are known, with discriminants -283 and -563.

For n = 4, $r_1 = 4$, $r_2 = 0$ one finds nine examples with discriminants 725, 1125, 1600, 1957, 2225, 2304, 2624, 2777 and 4205 in [54].

For n $\geqslant$ 5 eight examples are known:

n	r_1	r_2	F	Δ	reference
5	5	0	$\underline{Q}(\zeta_{11}+\zeta_{11}^{-1})$	11^4	[54]
5	1	2	$\underline{Q}(\theta),\theta^5=\theta+1$	19×151	§14
6	0	3	$\underline{Q}(\zeta_7)$	-7^5	§14
6	0	3	$\underline{Q}(\zeta_9)$	-3^9	[55]
6	2	2	$\underline{Q}(\theta),\theta^6=\theta^2+1$	$2^6\cdot23^2$	§14
8	0	4	$\underline{Q}(\zeta_{15})$	$3^4\cdot5^6$	[55]
8	0	4	$\underline{Q}(\zeta_{20})$	$4^4\cdot5^6$	[55]
10	0	5	$\underline{Q}(\zeta_{11})$	-11^9	[55].

The number of known examples is:

$n =$	1,	2,	3,	4,	≥ 5,	≥ 1,
$\# =$	1,	21,	72,	42,	8,	144.

Among these examples there are eleven cyclotomic ones: $F = \underline{Q}(\zeta_m)$ with $m = 1, 3, 4, 5, 7, 8, 9, 11, 12, 15, 20$. A unified treatment of these fields can be found in [55]. Nothing about the completeness of this list is known. Note that $\underline{Q}(\zeta_{2m}) = \underline{Q}(\zeta_m)$ for m odd. For $m \equiv 0 \bmod 2$ the field $\underline{Q}(\zeta_m)$ has class number one if and only if $[\underline{Q}(\zeta_m):\underline{Q}] \leq 20$ or $m \in \{70,84,90\}$ (thirty cases) [56].

In [46] one can find information about the finiteness of the number of examples in certain classes of number fields. Also a candidate for an infinite class of examples is proposed.

There are six quaternion division algebras over number fields which are known to have an order which is euclidean with respect to the norm.

In section 10 we mentioned already that there are exactly three such examples over $\underline{Q}$ which ramify at infinity: $(\frac{-1,-1}{\underline{Q}})$, $(\frac{-1,-3}{\underline{Q}})$ and $(\frac{-3,-5}{\underline{Q}})$, cf. [57]. There are two known examples over $\underline{Q}$ which split at infinity: $(\frac{-1,3}{\underline{Q}})$ and $(\frac{-2,5}{\underline{Q}})$. The sixth example is the unique quaternion division algebra over $\underline{Q}(\sqrt{5})$ which splits at all finite primes. This algebra contains the euclidean order

$$\underline{Z}[i,\zeta_5, \frac{1}{\zeta_5-1}(1+2i)], \qquad i^2=-1,\ \zeta_5^5 = 1 \neq \zeta_5,\ i\zeta_5 = \zeta_5^{-1}i,$$

as can be proved by the methods of [55].

16. Rings of algebraic functions.

Let F be a function field in one variable over an arbitrary field k, cf. [24]. We assume that k is the exact field of constants of F. Each place $\underline{p}$ of F over k gives rise to an exponential valuation $\mathrm{ord}_{\underline{p}}$ on F whose image is $\underline{Z} \cup \{\infty\}$. The degree $d(\underline{p})$ of $\underline{p}$ is the degree of its residue class field over k.

A divisor of F/k is a formal finite product $\underline{a} = \prod_{\underline{p}} \underline{p}^{m(\underline{p})}$ where $\underline{p}$ ranges over the places of F/k and $m(\underline{p}) \in \underline{Z}$, $m(\underline{p}) = 0$ for almost all $\underline{p}$. We put $d(\underline{a}) = \Sigma_{\underline{p}}\, m(\underline{p})\cdot d(\underline{p})$ and $L(\underline{a}) = \{x \in F \mid \mathrm{ord}_{\underline{p}}(x) \geqslant m_{\underline{p}}$ for all $\underline{p}\}$. The dimension of $L(\underline{a})$ over k is denoted by $\ell(\underline{a})$. The theorem of Riemann-Roch implies $\ell(\underline{a}) \geqslant d(-\underline{a}) + 1 - g$ for all $\underline{a}$, where g is the genus of F/k.

For $x \in F^*$ the principal divisor (x) is defined to be $\prod_{\underline{p}} \underline{p}^{\mathrm{ord}_{\underline{p}}(x)}$. We have $d((x)) = 0$ for all $x \in F^*$.

Let S be a non-empty set of places of F/k. Then $\underline{O}_S = \{x \in F \mid \mathrm{ord}_{\underline{p}}(x) \geqslant 0$ for all $\underline{p} \notin S\}$ is a Dedekind domain, and the group of fractional ideals of $\underline{O}_S$ can be identified with the group of divisors $\underline{a} = \prod \underline{p}^{m(\underline{p})}$ for which $m(\underline{p}) = 0$ for all $\underline{p} \in S$. Here we agree that also F itself is a Dedekind domain. If $\underline{a} \subset \underline{O}_S$ is a nonzero ideal, $\underline{a} = \prod \underline{p}^{m(\underline{p})}$, then $\dim_k(\underline{O}_S/\underline{a}) = \Sigma_{\underline{p} \notin S}\, m(\underline{p}) d(\underline{p}) = d(\underline{a})$.

The following theorem is the function field analogue of (14.6).

(16.1) Theorem. Let S be a non-empty set of places of F/k, and let $d = \text{g.c.d.}\{d(\underline{p}) \mid \underline{p} \in S\}$. Put $T = \{\underline{p} \mid d(\underline{p}) \leqslant 2d + 2g - 2\}$. Then $\underline{O}_{S\cup T}$ is euclidean with respect to the function

$$\varphi(x) = \dim_k(\underline{O}_{S\cup T}/\underline{O}_{S\cup T}\cdot x) \qquad (x \in \underline{O}_{S\cup T}).$$

Remark. In (16.9) we determine under which conditions T is finite.

Proof. The definition of d implies the existence of a divisor "based on S":

$$\underline{c} = \prod_{\underline{p} \in S} \underline{p}^{n(\underline{p})}$$

which satisfies

$$-d - 2g + 2 > d(\underline{c}) \geqslant -2d - 2g + 2.$$

Riemann-Roch implies

(16.2) $$\ell(\underline{c}) \geqslant d(-\underline{c}) + 1 - g > d + g - 1.$$

Note that $L(\underline{c}) \subset \underline{O}_S$.

For a divisor $\underline{a} = \prod_{\underline{p}} \underline{p}^{m(\underline{p})}$, let us define

$$d_0(\underline{a}) = \sum_{\underline{p} \notin S} m(\underline{p}) \cdot d(\underline{p}),$$

$$d_\infty(\underline{a}) = \sum_{\underline{p} \in S} m(\underline{p}) \cdot d(\underline{p}).$$

Clearly $d_0(\underline{a}) + d_\infty(\underline{a}) = d(\underline{a})$, so $d_0((x)) = -d_\infty((x))$ for $x \in F^*$.

<u>(16.3) Lemma.</u> Let $a,b \in \underline{O}_S$, $b \neq 0$. Then there exists a nonzero element $t \in L(\underline{c})$ such that the residue class $ta + \underline{O}_S \cdot b$ contains an element r for which $r = 0$ or $d_0((r)) < d_0((b))$.

<u>Proof.</u> The divisor $\prod_{\underline{p} \in S} \underline{p}^{\operatorname{ord}_{\underline{p}}(b)}$ is based on S and has degree $-d_0((b))$. Hence we can find a divisor $\underline{r}$ which is based on S and has degree $d(\underline{r}) = d - d_0((b))$.

The space $L(\underline{r})$ is contained in $\underline{O}_S$ and has k-dimension at least $d_0((b)) - d - g + 1$. We claim

$$L(\underline{r}) \cap \underline{O}_S \cdot b = \{0\}.$$

In fact, if $x \neq 0$ would be in the intersection, then $x \in \underline{O}_S \cdot b$ would imply $d_0((x)) \geqslant d_0((b))$, and $x \in L(\underline{r})$ would give $d_\infty((x)) \geqslant d_\infty(\underline{r}) = d - d_0((b))$, so $d_0((x)) + d_\infty((x)) \geqslant d > 0$, contradiction.

We conclude that the map $L(\underline{r}) \to \underline{O}_S / \underline{O}_S \cdot b$ is injective. Denote the image again by $L(\underline{r})$. Since $\dim_k(\underline{O}_S/\underline{O}_S\cdot b) = d_0((b))$ we find

$$\dim_k((\underline{O}_S/\underline{O}_S\cdot b)/L(\underline{r})) \leqslant d + g - 1.$$

Consider the maps

$$\begin{aligned} L(\underline{c}) &\to \underline{O}_S/\underline{O}_S\cdot b \to (\underline{O}_S/\underline{O}_S\cdot b)/L(\underline{r}), \\ t &\mapsto (ta \bmod \underline{O}_S b). \end{aligned}$$

By (16.2) we have $\dim_k L(\underline{c}) > d + g - 1$ so the composite map is not injective. Hence for some $t \in L(\underline{c})$, $t \neq 0$, the element $(ta \bmod \underline{O}_S b)$ is inside the image of $L(\underline{r})$, say $ta \equiv r \bmod \underline{O}_S\cdot b$, with $r \in L(\underline{r})$. Then either $r = 0$, or $d_0((r)) = -d_\infty((r)) < -d_\infty(\underline{r}) = d_0((b)) - d < d_0((b))$ so the lemma is proved. $\square$

<u>(16.4) Lemma.</u> $L(\underline{c}) - \{0\} \subset \underline{O}^*_{S\cup T}$.

<u>Proof.</u> Let $x \in L(\underline{c})$, $x \neq 0$. We have to prove $\text{ord}_{\underline{p}}(x) = 0$ for all $\underline{p} \notin S\cup T$. So let $\underline{q} \notin S$ satisfy $\text{ord}_{\underline{q}}(x) \neq 0$, we must show $\underline{q} \in T$.

For every $\underline{p} \notin S$ we have $\text{ord}_{\underline{p}}(x) \geqslant 0$, since $x \in L(\underline{c})$. In particular $\text{ord}_{\underline{q}}(x) > 0$,

so
$$d_0((x)) = \sum_{\underline{p}\notin S} \text{ord}_{\underline{p}}(x)d(\underline{p}) \geqslant \text{ord}_{\underline{q}}(x)\cdot d(\underline{q}) \geqslant d(\underline{q})$$

while on the other hand

$$d_0((x)) = -d_\infty((x)) \leqslant -d_\infty(\underline{c}) = -d(\underline{c}) \leqslant 2d + 2g - 2.$$

We conclude $d(\underline{q}) \leqslant 2d + 2g - 2$, i.e. $\underline{q} \in T$. This proves (16.4). $\square$

<u>Proof of (16.1).</u> Note the formulas

$$\begin{aligned} \varphi(x) &= \sum_{\underline{p}\notin S\cup T} \text{ord}_{\underline{p}}(x)\ d(\underline{p}) \\ &= d_0((x)) - \sum_{\underline{p}\in T-S} \text{ord}_{\underline{p}}(x)\ d(\underline{p}) \end{aligned}$$

(16.5) $$\varphi(xy) = \varphi(x) + \varphi(y)$$

for $x, y \in \underline{O}_{S\cup T} - \{0\}$.

Let $a,b \in \underline{O}_{S\cup T}$, $b \neq 0$. In order to prove the theorem, we have to exhibit an element $s \in a + \underline{O}_{S\cup T}\cdot b$ for which $s = 0$ or $\varphi(s) < \varphi(b)$. By (16.5) the problem does not change if we multiply a and b by the same non-zero constant $c \in \underline{O}_{S\cup T}$. This means that we may assume $a,b \in \underline{O}_S$.

Since $\underline{O}_S$ is Dedekind, the strong approximation theorem gives us an element $a' \in \underline{O}_S$ for which

$$\mathrm{ord}_{\underline{p}}(a-a') \geqslant \mathrm{ord}_{\underline{p}}(b) \qquad \text{for all } \underline{p} \notin T\cup S,$$

$$\mathrm{ord}_{\underline{p}}(a') \geqslant \mathrm{ord}_{\underline{p}}(b) \qquad \text{for all } \underline{p} \in T - S.$$

Than $a + \underline{O}_{S\cup T}\cdot b = a' + \underline{O}_{S\cup T}\cdot b$, so replacing a by a' does not change the problem, except that we may assume

(16.6) $\qquad \mathrm{ord}_{\underline{p}}(a) \geqslant \mathrm{ord}_{\underline{p}}(b) \qquad$ for all $\underline{p} \in T - S$.

Using (16.3) we choose $t \in L(\underline{c}) - \{0\}$ and $r \in ta + \underline{O}_S\cdot b$ such that $r = 0$ or $d_0((r)) < d_0((b))$. Then $\frac{r}{t} \in a + \underline{O}_{S\cup T}\cdot b$, by (16.4), and we claim that $s = \frac{r}{t}$ satisfies our requirement $s = 0$ or $\varphi(s) < \varphi(b)$.
In fact, if $s \neq 0$ then

$$\begin{aligned}\varphi(s) - \varphi(b) &= \varphi(r) - \varphi(b) = \\ &= d_0((r)) - d_0((b)) - \sum_{\underline{p}\in T-S} \mathrm{ord}_{\underline{p}}(\tfrac{r}{b})\cdot d(\underline{p}) \\ &< - \sum_{\underline{p}\in T-S} \mathrm{ord}_{\underline{p}}(\tfrac{r}{b})\cdot d(\underline{p}).\end{aligned}$$

But $r \in ta + \underline{O}_S\cdot b$ and (16.6) imply $\mathrm{ord}_{\underline{p}}(\frac{r}{b}) \geqslant 0$ for $\underline{p} \in T-S$, so we conclude

$$\varphi(s) - \varphi(b) < 0$$

as required. This proves (16.1).

<u>Remark.</u> The proof shows that in the definition of T we may replace $2d + 2g - 2$ by $d\cdot(2 + \left[\frac{2g-2}{d}\right])$. But this is no real improvement, since there is no loss in

generality in assuming $d|2g-2$. In fact, if ever $\underline{O}_U$ $(U \neq \emptyset)$ is to be a principal ideal domain, then U must always contain a (finite) set S' such that $d' = \text{g.c.d.} \{d(\underline{p}) | \underline{p} \in S'\}$ divides the degree of <u>every</u> divisor, in particular the degree of a canonical divisor, which equals $2g - 2$. Replacing S by S' we then have $d|2g - 2$, while moreover T is not enlarged by this replacement.

<u>(16.7) Theorem</u> (MacRae, [58]). Suppose that k is an infinite field and that there are only finitely many places of F/k of degree one. Let S be a finite non-empty set of places of F/k. Then $\underline{O}_S$ is not euclidean.

We need the following lemma, for the proof of which we refer to Samuel [2, prop. 18, cor.].

<u>(16.8) Lemma.</u> Let k be an infinite field and K a field extension of k such that K^*/k^* is a finitely generated abelian group. Then $k = K$. □

<u>Proof</u> of (16.7). Suppose $\underline{O}_S$ is euclidean. Using (3.6) we may assume that all places of degree one are in S.

Let θ be the smallest algorithm on $\underline{O}_S$, and choose $\pi \in \underline{O}_S$ such that $\theta(\pi) = 1$. Then $K = \underline{O}_S/\underline{O}_S\pi$ is a field extension of k and the map $\underline{O}_S^* \to K^*$ is surjective, cf. (2.6).

But $\underline{O}_S^*/k^*$ is finitely generated since it maps injectively to $\prod_{\underline{p} \in S} \underline{Z}$, by $\varepsilon \mapsto (\text{ord}_{\underline{p}}(\varepsilon))_{\underline{p} \in S}$. Hence K^*/k^* is finitely generated and by (16.8) we conclude $K = k$. This means that $\underline{O}_S \cdot \pi$ is a prime ideal of degree one of $\underline{O}_S$, contradicting the assumption that all places of degree one are in S. □

From (2.6) or (8.4) one easily deduces that the principal ideal domain $R = \underline{R}[X,Y]/(X^2+Y^2+1)$ is not euclidean. Theorem (16.7) implies that for every $a \in R - \{0\}$ the ring $R[a^{-1}]$ is a non-euclidean principal ideal domain.

<u>(16.9) Corollary.</u> Let S, d, T be as in (16.1). Then T is finite if and only if k is finite, or $d = 1$ and $g = 0$.

<u>Proof.</u> "If" is clear. "Only if". Suppose k is infinite and T is finite. Replacing S by a finite subset giving the same d we then have that $S \cup T$ is finite. Therefore (16.1) and (16.7) imply that F/k has infinitely many places

of degree one. Since T is finite we conclude $2d + 2g - 2 \leqslant 0$ so $d = 1$ and $g = 0$. □

(16.10) Theorem (Samuel, [2]). Suppose F/k has genus 0, and let S be a finite non-empty set of places of F/k. Then $\underline{O}_S$ is euclidean if and only if $\text{g.c.d.}\{d(\underline{p}) \mid \underline{p} \in S\} = 1$.

Proof. "If" is obvious from (16.1). "Only if". Let $\underline{O}_S$ be euclidean. If k is infinite then (16.7) implies that there exists a divisor $\underline{a}$ with $d(\underline{a}) = 1$. It is well known [59,p.148] that such a divisor also exists if k is finite. Since $\underline{O}_S$ is a principal ideal domain we may assume that $\underline{a}$ is based on S, and we conclude $\text{g.c.d.}\{d(\underline{p}) \mid \underline{p} \in S\} = 1$. □

Without proof we mention:

(16.11) Theorem (Samuel, [2]). Suppose F/k has genus 0 and k is infinite. Let S be as in (16.10) and assume that $\underline{O}_S$ is euclidean. Then the smallest algorithm θ of $\underline{O}_S$ is given by

$$\theta(x) = \dim_k(\underline{O}_S/\underline{O}_S x),\ x \neq 0, \quad \theta(0) = \omega. \quad \square$$

Various other results on the same subject can be found in papers of J.V. Armitage, which are recommended for careful reading [60,61,62,63].

References.

1. T. Motzkin, The Euclidean algorithm, Bull. Amer. Math. Soc. 55 (1949), 1142-1146.
2. P. Samuel, About Euclidean rings, J. Algebra 19 (1971), 282-301.
3. P.W. Carruth, Arithmetic of ordinals with applications to the theory of ordered abelian groups, Bull. Amer. Math. Soc. 48 (1942), 262-271.
4. O. Zariski, P. Samuel, Commutative Algebra, vol. I, Princeton, New Jersey 1958.
5. P. Eakin, W. Heinzer, More noneuclidian PID's and Dedekind domains with prescribed class group, Proc. Amer. Math. Soc. 40 (1973), 66-68.
6. N. Jacobson, A note on non-commutative polynomials, Ann. Math. 35 (1934), 209-210.
7. H.-H. Ostmann, Euklidische Ringe mit eindeutiger Partialbruchzerlegung, J. Reine Angew. Math. 188 (1950), 150-161.
8. H.J. Claus, Über die Partialbruchzerlegung in nicht notwendig kommutativen euklidischen Ringen, J. Reine Angew. Math. 194 (1955), 88-100.
9. A.V. Jategaonkar, A counter-example in ring theory and homological algebra, J. Algebra 12 (1969), 418-440.
10. A.V. Jategaonkar, Rings with transfinite left division algorithm, Bull. Amer. Math. Soc. 75 (1969), 559-561.
11. A.V. Jategaonkar. Left Principal Ideal Rings, Lect. Notes in Math. 123, Berlin 1970.
12. P.M. Cohn, Free rings and their Relations, New York 1971.
13. G. Picavet, Caractérisation de certains types d'anneaux Euclidiens, Enseignement Math., II Sér. 18 (1972), 245-254.
14. F. Dress, Stathmes euclidiens et séries formelles, Acta Arith. 19 (1971), 261-265.
15. H.H. Brungs, Left Euclidean Rings, Pacific J. of Math. 45 (1973) 27-33.
16. H.M. Stark, A Complete Determination of the Complex Quadratic Fields of Class-Number One, Mich. Math. J. 14 (1967), 1-27.

17. J.R.C. Leitzel, M.L. Madan, C.S. Queen, Algebraic function fields with small class number, J. Number Theory, to appear.

18. C.S. Queen, Arithmetic Euclidean Rings, to appear (cf. Bull. Amer. Math. Soc. 79 (1973), 1229-1232), Acta Arith. 26 (1974), 105-113.

19. P.J. Weinberger, On Euclidean rings of algebraic integers, Proc. Symp. Pure Math. 24 (Analytic Number Theory, 1973), 321-332.

20. A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Paris 1948.

21. E. Bombieri, Counting points on curves over finite fields (d'après S.A. Stepanov), Sém. Bourbaki 25 (1973), nr. 430.

22. O.T.O'Meara, On the finite generation of linear groups over Hasse domains, J. Reine Angew. Math. 217 (1965), 79-108.

23. E. Artin, Algebraic Numbers and Algebraic Functions, New York 1967.

24. C. Chevalley, Introduction to the theory of algebraic functions of one variable, Amer. Math. Soc. 1951.

25. P.M. Cohn, On the structure of the GL_2 of a ring, Publ. Math. I.H.E.S. 30 (1966), 5-53.

26. S. Lang, Algebraic Number Theory, Reading, Mass. 1970.

27. E. Artin, Collected papers, Reading, Mass. 1965.

28. H. Bilharz, Primdivisoren mit vorgegebener Primitivwurzel, Math. Ann. 114 (1937), 476-492.

29. C. Hooley, On Artin's conjecture, J.Reine Angew. Math. 225 (1967), 209-220.

30. H. Hasse, Über die Artinsche Vermutung und verwandte Dichtefragen, Ann. Acad. Sci. Fennicae, 1952.

31. L.J. Goldstein, Analogues of Artin's conjecture, Trans. Amer. Math. Soc. 149 (1970), 431-442.

32. P.J. Weinberger, A counterexample to an analogue of Artin's conjecture, Proc. Amer. Math. Soc. 35 (1972), 49-52.

33. L.J. Goldstein, Some remarks on arithmetic density questions, Proc. Symp. Pure Math. 24 (Analytic Number Theory, 1973), 103-110.

34. N.P. Romanoff, Über einige Sätze der additiven Zahlentheorie, Math. Ann. 109 (1934), 668-678.

35. H.A. Heilbronn, On an inequality in the elementary theory of numbers, Proc. Cambridge Philos. Soc. 33 (1937), 207-209.

36. H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Würzburg 1965.

37. A. Hurwitz, Der Euklidische Divisionssatz in einem endlichen algebraischen Zahlkörper, Math. Z. 3 (1919), 123-126.

38. J.H.M. Wedderburn, Non-commutative domains of integrity, J. Reine Angew. Math. 167 (1932), 129-141.

39. H. Chatland, H. Davenport, Euclid's algorithm in real quadratic fields, Canad. J. Math. 2 (1950), 289-296.

40. G.H. Hardy, E.M. Wright, An introduction to the theory of numbers, London 1960^4.

41. V. Ennola, On the first inhomogeneous minimum of indefinite binary quadratic forms and Euclid's algorithm in real quadratic fields, Ann. Univ. Turku Ser. A1 28 (1958), 9-58.

42. J.W.S. Cassels, The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms, Proc. Cambridge Philos. Soc. 48 (1952), 72-86, 519-520.

43. H. Davenport, Euclid's algorithm in cubic fields of negative discriminant, Acta Math. 84 (1950), 159-179.

44. H.J. Godwin, On Euclid's algorithm in some cubic fields with signature one, Quart. J. Math. Oxford Ser. 18 (1967), 333-338.

45. H. Heilbronn, On Euclid's algorithm in cubic self-conjugate fields, Proc. Cambridge Philos. Soc. 46 (1950), 377-382.

46. H. Heilbronn, On Euclid's algorithm in cyclic fields, Canad. J. Math. 3 (1951), 257-268.

47. H.J. Godwin, On the inhomogeneous minima of totally real cubic norm-forms, J. London Math. Soc. 40 (1965), 623-627.

48. J.R. Smith, On Euclid's algorithm in some cyclic cubic fields, J. London Math. Soc. 44 (1969), 577-582.

49. H. Davenport, Euclid's algorithm in certain quartic fields, Trans. Amer. Math. Soc. 68 (1950), 508-532.

50. R.B. Lakein, Euclid's algorithm in complex quartic fields, Acta Arith. 20 (1972), 393-400.

51. E. Landau, Vorlesungen über Zahlentheorie, Band 3, Leipzig 1927.

52. J. Ouspensky, Note sur les nombres entiers dépendant d'une racine cinquième de l'unité, Math. Ann. 66 (1909), 109-112.

53. J.R. Smith, The inhomogeneous minima of some totally real cubic fields, pp. 223-224 in: Computers in Number Theory, Proc. Atlas Symp. 2, London 1971.

54. H.J. Godwin, On Euclid's algorithm in some quartic and quintic fields, J. London Math. Soc. 40 (1965), 699-704.

55. H.W. Lenstra, Jr., Euclid's algorithm in cyclotomic fields, to appear in J. London Math. Soc.

56. J.M. Masley, H.L. Montgomery, to appear.

57. L.E. Dickson, Algebren und ihre Zahlentheorie, Zürich 1927.

58. R.E. MacRae, On Euclidean rings of algebraic functions, pp. 167-170 in: Conference on Commutative Algebra, Lecture Notes in Math. 311, Berlin 1973.

59. M. Deuring, Lectures on the theory of algebraic functions of one variable, Lecture Notes in Math. 314, Berlin 1973.

60. J.V. Armitage, Euclid's algorithm in certain algebraic function fields, Proc. London Math. Soc. (3) 7 (1957), 498-509.

61. J.V. Armitage, Euclid's algorithm in algebraic function fields, J. London Math. Soc. 38 (1963), 55-59; Corrigendum and Addendum: 43 (1968), 171-172.

62. J.V. Armitage, On unique factorization in algebraic function fields, Illinois J. Math. 11 (1967), 280-283; Appendix: 12 (1968), 5-6. (Misprints corrected in [63] and in J. London Math. Soc. (2) 6 (1972), 103-108).

63. J.V. Armitage, Euclid's algorithm in algebraic function fields, II, Acta Arith. 18 (1971), 337-348.

64. G. Cooke, P.J. Weinberger, On the construction of division chains in algebraic number rings, with applications to SL_2, preprint.

65. R.K. Dennis, References for Euclidean Rings and Generalizations Thereof. Cornell University, 1973.

Acknowledgements are due to A.W.M. Dress for inviting me to Bielefeld; to R.K. Dennis for encouragement; and to U. Rehmann for unfailing technical assistance.

Author's address:
Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
Amsterdam
The Netherlands