ON IDEAL THEORY IN HIGH PRUFER DOMAINS

Moshe Jarden*

Let R be a Dedekind domain with the quotient field K, and let e be a positive integer. For every $(\sigma) \in \mathcal{G}(K_s/K)^e$ we denote by $K_s(\sigma)$ the fixed field of (σ) in the separable closure K_s of K, by $I(\sigma)$ the integral closure of R in $K_s(\sigma)$ and by $C(\sigma)$ the ideal class group of $I(\sigma)$. The following theorems are proved: A) If $R = \mathbb{Z}$ or $R = K_o[x]$, where K_o is an algebraic extension of a finite field and x is a transcendental element over K_o, then $I(\sigma)$ is a Bezout domain, for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$. B) If K_o is not an algebraic extension of a finite field then rank $C(\sigma)$ is infinite for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$. C) If K is denumerable and hilbertian then every prime ideal $\mathcal{P}$ of $I(\sigma)$ is idempotent for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$. Here "almost all" is used in the sense of the Haar measure of the compact group $\mathcal{G}(K_s/K)^e$.

* This work was carried out whilst the author was working at Heidelberg University.

INTRODUCTION AND DEFINITIONS

Let S be an integral domain with quotient field L. Recall that an S-submodule $\mathfrak{a}$ of L is said to be a fractional ideal of S if it is non-zero and there is an element $a \neq 0$ of S such that $a\mathfrak{a} \subseteq S$. The set of all fractional ideals of S forms an abelian semi-group under multiplication with S as the unit (c.f. Gilmer [8, p. 23]). We denote it by $J(S)$. If $\mathfrak{a} \in J(S)$ then $\mathfrak{a}^{-1} = \{x \in L | x\mathfrak{a} \subseteq S\}$ belongs also to $J(S)$. The fractional ideal $\mathfrak{a}$ is said to be invertible if $\mathfrak{a}\mathfrak{a}^{-1} = S$. Recall that S is said to be a Dedekind domain if every fractional ideal of S is invertible. Correspondingly, S is said to be a Prüfer domain if every finitely generated fractional ideal of S is invertible. In this case the subset $J^*(S)$ of all finitely generated fractional ideals of S forms a subgroup of the semi-group $J(S)$. From now on we assume that S is a Prüfer domain. The subset of all principal fractional ideals of S, i.e. all the S-modules of the form aS, where $a \in L$ and $a \neq 0$, forms a subgroup $J_o^*(S)$ of $J^*(S)$. Two elements of $J^*(S)$ are said to be linearly equivalent if they are congruent modulo $J_o^*(S)$. A finite subset $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_\ell\}$ of $J^*(S)$ is said to be linearly independent if $\mathfrak{a}_1^{n_1} \ldots \mathfrak{a}_\ell^{n_\ell} \; J_o^*(S)$ always implies $n_1 = \ldots = n_\ell = 0$. The quotient group $C(S) = J^*(S)/J_o^*(S)$ is known as the ideal class group of S. Clearly every class can be represented by a finitely generated ideal of S. In the case where $C(S) = 1$, i.e. when every finitely generated ideal of S is principal, S is known as a Bezout domain.

Consider now a Prüfer domain R with quotient field K. Then R is integrally closed (c.f. Cassels and Fröhlich [3, p. 7]). On the other hand, if L is an algebraic extension of K then the integral closure, $I(L)$, of R in L is a Prüfer domain (c.f. Gilmer [8, p. 257]). We put $J(L)$, $J^*(L)$ and $C(L)$ for

$J(I(L))$, $J^*(I(L))$ and $C(I(L))$ respectively. In addition we denote by $P(L)$ the set of all non-zero proper prime ideals of $I(L)$.

Further, write $\tilde{K}$, K_s and $\mathcal{G}(K_s/K)$ for the algebraic closure of K, the separable closure of K, and the Galois group of K_s over K, respectively. Consider, for a fix positive integer e, an e-tuple $(\sigma) = (\sigma_1,\ldots,\sigma_e) \in \mathcal{G}(K_s/K)^e$. Let $K_s(\sigma)$ be the fixed field of (σ) in K_s and put $I(\sigma)$, $J(\sigma)$, $J^*(\sigma)$ and $C(\sigma)$ and $C(\sigma)$ for $I(K_s(\sigma))$, $J(K_s(\sigma))$, $J^*(K_s(\sigma))$ and $C(K_s(\sigma))$, respectively. In the first three paragraphs we study properties of the group $C(\sigma)$ that are valid for almost all (σ) in $\mathcal{G}(K_s/K)^e$. Here "almost all" is used in the sense of the Haar measure of the compact group $\mathcal{G}(K_s/K)^e$ (c.f. 10, Sec. 1.3]). This study is motivated by the fact that $I(Q)$ is a Bezout domain. (c.f. Kaplanski [12, p. 72]).

Our main results in these sections are:
A) If $R = \mathbb{Z}$ or $R = K_o[x]$, where K_o is an algebraic extension of a finite field and x is a transcendental element over K_o, then $I(\sigma)$ is a Bezout domain, for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$.
B) If K_o is not an algebraic extension of a finite field then rank $C(\sigma)$ is infinite for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$.

The crucial point in the proof of (B) is the existence of an elliptic curve A defined over K_o with a K_o-rational point of infinite order.

In section 4 we give an example of a high algebraic extension L of Q such that $I(L)$ is not a Bezout domain.

In sections 5-9 we consider a denumerable Dedekind ring R with a hilbertian quotient field K and we study properties of the semi-group $J(\sigma)$ that are valid for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$. At first we prove:

D) Almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ have the following two properties:

1) For every non-trival real valuation v of $K_s(\sigma)$ the completion $K_s(\sigma)_v$ is algebraically closed.

2) For every finite extension L of K which is contained in $K_s(\sigma)$ and for every prime ideal $\mathfrak{P}$ of $I(L)$ there exist in $I(\sigma)$ at least two different prime ideals which lie over $\mathfrak{P}$.

In sections 6-9 we deduce some more properties of $J(\sigma)$ which follow directly from (1) and (2) of (D). More precisely, we prove that every separable extension M of K which has the properties (1) and (2) of (D) has also the following properties:

E) 1) Every prime ideal $\mathfrak{P}$ of $I(M)$ is idempotent.

2) If $\mathfrak{Q}$ is a $\mathfrak{P}$-primary ideal then $\mathfrak{Q}$ is not finitely generated. If in addition $\mathfrak{Q} \neq \mathfrak{P}$, then $\bigcap_{n=1}^{\infty} \mathfrak{Q}^n = 0$.

3) The semi-group $J(M)$ and the group $J^*(M)$ are uniquely divisable.

In deducing (3) we follow Krull [13] and deduce a parametrization of $J(M)$ and $J^*(M)$ which generalizes the usual representation of fractional ideals in a Dedekind domain as a product of powers of prime ideals.

The author wishes to acknowledge his indebtness to P. Roquette for his constant encouragement and especially for calling his attention to Hasse's argument which is used in the proof of Lemma 1.3. He also thanks W.D. Geyer for his contribution to sections 2 and 3.

1. The $C(\sigma)$ as torsion-free groups

We recall that an integral domain R with the quotient field K is said to be hilbertian if every K-hilbertian set contains points with coordinates in R (c.f. Lang [14, p. 141]). A sequence $K_1, K_2, K_3, \ldots$ of extensions of K is said to be <u>linearly disjoint</u> over K if $K_1 \ldots K_n$ is linearly disjoint from K_{n+1} for every

positive integer n (c.f. [10, section 1.2]). Finally, we say that an algebraic element α over K is integral over R (resp. an algebraic unit) if it is integral over R (resp. a unit in the ring $I(\tilde{K})$ of all integral algebraic elements). With these definitions we have the following lemma:

LEMMA 1.1: Let R be a hilbertian integral domain with the quotient field K. Consider an element $a \in R$, $a \neq 0$ and let $\alpha \in \tilde{K}$ be an element for which $\alpha^n = a$. Then there exists an infinite sequence $\beta_1, \beta_2, \beta_3, \ldots$, of separable algebraic integral elements such that

i) β_i/α is an algebraic unit;

ii) $[K(\beta_i) : K] = n$;

iii) the sequence $K(\beta_1)$, $K(\beta_2)$, $K(\beta_3)$, ... is linearly disjoint over K.

Let $b \in R$, $b \neq 0$ and consider an element $\beta \in K$ which satisfies

$$\beta^n + ab\beta - a = 0 .$$

Then β is seperable and integral. Moreover, β/α and α/β satisfy the relations

$$\left(\frac{\beta}{\alpha}\right)^n + b\alpha\,\frac{\beta}{\alpha} - 1 = 0 \quad \text{and} \quad 1 + b\alpha\left(\frac{\alpha}{\beta}\right)^{n-1} - \left(\frac{\alpha}{\beta}\right)^n = 0 .$$

Hence they are integral over $R[\alpha]$ which in turn is integral over R. It follows that both β/α and α/β are integral, i.e. β/α is an algebraic unit.

In order to conclude the proof of the Lemma we consider the absolutely irreducible polynomial $f(T,X) = X^n + aTX - a$. Since R is hilbertian we can construct by induction a sequence of pairs $\{(b_i,\beta_i)\}_{i=1}^{\infty}$ such that $b_i \in R$, $f(b_i,\beta_i) = 0$, $[K(\beta_i) : K] = n$ and such that the sequence $\{K(\beta_i)\}_{i=1}^{\infty}$ is linearly disjoint over K (c.f. [10, the proof of Lemma 2.2]). By the first part of the proof, the sequence $\{\beta_i\}_{i=1}^{\infty}$ satisfies

all the requirements of the Lemma.

LEMMA 1.2: Let S be a Prüfer domain and let $\mathfrak{a}$, $\mathfrak{b}$ be two fractional ideals of S which satisfy $\mathfrak{a}^n = \mathfrak{b}^n$ for some positive integer n. Then $\mathfrak{a} = \mathfrak{b}$.

PROOF: It suffices to consider the case where S is a valuation ring, since in the general case the local rings $S_\mathfrak{p}$ of S with respect to prime ideals are valuation rings (c.f. Gilmer [8, p. 254]) and $\mathfrak{a} = \bigcap_\mathfrak{p} \mathfrak{a} S_\mathfrak{p}$ where $\mathfrak{p}$ runs over all prime ideals of S. Let v be the corresponding valuation of the quotient field of S and let $a \in \mathfrak{a}$. Then $a^n \in \mathfrak{b}^n$ and hence $a^n = \sum_{(i)} b_{i_1} \ldots b_{i_n}$ where the b_{i_j} are in $\mathfrak{b}$. Among the b_{i_j} there must be one whose value is $\leq v(a)$, since otherwise we would have

$$nv(a) \geq \min_{(i)} \{v(b_{i_1}) + \ldots + v(b_{i_n})\} > nv(a) ,$$

which is a contradiction. For this b we have $a = \frac{a}{b} b \in \mathfrak{b}$. Hence $\mathfrak{a} \subseteq \mathfrak{b}$. Symmetrically we have $\mathfrak{b} \subseteq \mathfrak{a}$. Hence $\mathfrak{a} = \mathfrak{b}$.

We note that Lemma 1.2 follows also from 2.0 of [9].

LEMMA 1.3: Let R be a hilbertian Prüfer domain with the quotient field K. Let $\mathfrak{a} \in J^*(R)$ be an element which is of finite order modulo $J_0^*(R)$. Then for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ $\mathfrak{a} I(\sigma) \in J_0^*(\sigma)$.

PROOF: By assumption there exists a positive integer n and an element $a \in R$, $a \neq 0$, such that $\mathfrak{a}^n = aR$. Let $\alpha \in \tilde{K}$ be an element for which $\alpha^n = a$ and consider a corresponding sequence $\beta_1, \beta_2, \beta_3, \ldots$ obtained by Lemma 1.1. Then $\{K(\beta_i)/K\}_{i=1}^\infty$ is a linearly disjoint sequence of separable extensions of degree n and $\varepsilon_i = \beta_i/\alpha$ is an algebraic unit. We use now an argument of Hasse to show that aR_i is a principal ideal in

$R_i = I(K(\beta_i))$. Indeed, $\varepsilon_i^n = \beta_i^n/a \in K(\beta_i)$, hence ε_i^n is a unit in R_i. Therefore, $(\mathfrak{a}R_i)^n = (\beta_i R_i)^n$, and by Lemma 1.2, we have that $\mathfrak{a}R_i = \beta_i R_i$.

Now, by [10, Lemma 1.10], $K_s(\sigma)$ contains at least one of the $k(\beta_i)$ for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$. Since $\mathfrak{a}$ becomes principal in $I(K(\beta_i))$, it remains so in $I(\sigma)$.

THEOREM 1.4: Let R be a denumerable hilbertian Prüfer domain with the quotient field K. Then for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$, $C(\sigma)$ is a torsion-free abelian group.

PROOF: Let L be a finite separable extension of K and let $\mathfrak{a}$ be a finitely generated ideal of $I(L)$ for which there exists an $n > 1$ such that $\mathfrak{a}^n$ is principal. Denote by $T(L,\mathfrak{a})$ the set of the $(\sigma) \in \mathcal{G}(K_s/K)^e$ for which $\mathfrak{a}I(\sigma)$ is not a principal ideal in $I(\sigma)$. Then by Lemma 1.3 $T(L,\mathfrak{a})$ has the measure 0. Since K is denumberable there are only countably many such $T(L,\mathfrak{a})$. Hence their union T is of measure 0. It is clear now that if $(\sigma) \in \mathcal{G}(K_s/K)^e$ and if $C(\sigma)$ is not torsion-free, then (σ) must belong to one of the $T(L,\mathfrak{a})$ and hence to T. It follows that the set of all the $(\sigma) \in \mathcal{G}(K_s/K)^e$ for which $C(\sigma)$ is not torsion-free has the measure 0.

COROLLARY 1.5:

a) If $R = \mathbb{Z}$, then for almost all $(\sigma) \in \mathcal{G}(\tilde{Q}/Q)^e$ $I(\sigma)$ is a Bezout domain.

b) If K_o is a countable field, x is a transcendental element over K, $R = K_o[x]$ and $K = K_o(x)$, then for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ $C(\sigma)$ is torsion-free abelian group.

c) In the notations of (b), if K_o is an algebraic extension of a finite field, then for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$, $I(\sigma)$ is a Bezout domain.

PROOF: In each case R is a denumberable hilbertian Dedekind domain (c.f. Lang [14, p. 155]), hence, in each case $C(\sigma)$ is a torsion-free abelian group for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$. Statement (b) is thus proved.

In order to complete the proofs of (a) and (c) we note that in both cases $C(L)$ is a finite abelian group for every finite extension L of K (c.f. [4, p. 7]). Hence if L is an arbitrary algebraic extension of K then $C(L)$ is either trivial or a torsion group. Since the $C(\sigma)$ cannot be torsion group they are trivial; i.e. $I(\sigma)$ is a Bezout domain.

PROBLEM 1: Is the following generalization of Corollary 1.5a true? "Let $R = \mathbb{Z}$. Then for almost all $(\sigma) \in \mathcal{G}(\tilde{Q}/Q)^e$ and for all fields $\tilde{Q}(\sigma) \subseteq L \subseteq \tilde{Q}$, $I(L)$ is a Bezout domain."

2. The rank of $C(\sigma)$ in the one-variable-function field case.

Let K_o be a field which is not algebraic over a finite field, let x be a transcendental element over K_o and put $R = K_o[x]$, $K = K_o(x)$. Then R is a principal ideal ring and hence a Dedekind ring, so that all the conventions made in the introduction are valid for R. We shall fix this notation throughout the whole section.

LEMMA 2.1: Let R be a Prüfer domain with the quotient field K and let L be an algebraic extension of K. If $a_1,\dots,a_\ell$ are ℓ linearly independent elements of $J^*(K)$ then $a_1 I(L),\dots,a_\ell I(\ell)$ are ℓ linearly independent elements of $J^*(L)$. In particular if $C(R)$ is not a torsion group then $C(L)$ is also not a torsion group.

PROOF: Assume that $\mathfrak{a}_1 I(L),\ldots,\mathfrak{a}_\ell I(L)$ are linearly dependent. Then there exists a finite extension L' of K contained in L, such that $\mathfrak{a}_1 I(L'),\ldots,\mathfrak{a}_\ell I(L')$ are linearly dependent. This means that there exists a non-zero ℓ-tuple $(m_1,\ldots,m_\ell)$ of integers and an element $\alpha \in L'$ such that

$$\prod_{i=1}^{\ell} (\mathfrak{a}_i I(L'))^{m_i} = \alpha I(L') .$$

Applying the norm function $N_{L'/K}$ to this equality we get

$$\prod_{i=1}^{\ell} \mathfrak{a}_i^{m_i[L':K]} = N_{L'/L}(\alpha)R$$

(c.f. [4, pp. 15, 16]). Hence the $\mathfrak{a}_i$'s are linearly dependent, which is a contradiction.

LEMMA 2.2: Let $\{K_i/K\}_{i=1}^{\infty}$ be a linearly disjoint sequence of finite Galois extensions. For every $e \geq 1$ let $\mathfrak{a}_i$ be an ideal in $I(K_i)$ which is of infinite order modulo principal ideals. Let L be an algebraic extension of K which contains all the K_i's. Then the sequence of ideals, $\{\mathfrak{a}_i I(L)\}_{i=1}^{\infty}$, of $I(L)$ is linearly independent.

PROOF: It suffices to prove that for every n, the first n ideals $\mathfrak{a}_1 I(L),\ldots,\mathfrak{a}_n I(L)$ are linearly independent, and in order to do this, it suffices to prove, by Lemma 2.1, that $\mathfrak{a}_1 S_n,\ldots,\mathfrak{a}_n S_n$ are linearly independent, where $S_n = I(K_1\ldots K_n)$. Indeed, suppose that these ideals satisfy a relation of the form

$$(1) \qquad \prod_{i=1}^{n} (\mathfrak{a}_i S_n)^{m_i} = uS_n$$

where the $m_i \in \mathbb{Z}$, $u \in S_n$, and not all of the m_i's are zero. Assume, for example, that $m_n \neq 0$. Denote by N the norm function from $K_1\ldots K_n$ to K_n. Let

$1 \leq i \leq m-1$. Then $N(\mathfrak{a}_i S_n)^{m_i}$ is an ideal which is generated by elements belonging to $K_1 \ldots K_{n-1} \cap K_n$, hence to K, since K_n and $K_1 \ldots K_{n-1}$ are linearly independent over K. But, as R is a principal domain, there exists a $u_i \in R$ such that

$$N(\mathfrak{a}_i S_n)^{m_i} = u_i I(K_n) . \tag{2}$$

On the other hand $\mathfrak{a}_n \subseteq I(K_n)$, hence

$$N(a_n S_n)^{m_n} = \mathfrak{a}^{dm_n} , \tag{3}$$

where $d = [K_1 \ldots K_n : K_n]$ (c.f. 4, p. 16]). If we apply now N on (1) we get by (2) and (3) that

$$\mathfrak{a}_n^{dm_n} = u_1^{-1} \ldots u_{n-1}^{-1} (Nu) S_n$$

which is a contradiction. //

For every prime p denote by $\mathbb{F}_p$ the field with p elements.

LEMMA 2.3: There exists an elliptic curve E defined over K_o which has a K_o-rational point P of infinite order.

PROOF: We distinguish between several cases:

a) $\mathrm{Char}(K_o) = 0$.

E is given by the equation

$$Y^2 = X^3 + 2X + 4$$

and $P = (\frac{1}{4}, 2 + \frac{1}{8})$. By a theorem of Lutz, [15, p. 244, Thm III] P has an infinite order since its coordinate is not integral.

b) $\mathrm{Char}(K_o) = 2$.

Let $t \in K_o$ be transcendental over $\mathbb{F}_2$. Then E is given by

$$Y^2 + XY = X^3 + tX^2 + (t^3+1)$$

and $P = (t^2,(t+1)^3)$. By Zimmer's Theorem [16] P has an infinite order on E since the square t^4 of its x coordinate does not divide (in $\mathbb{F}_2[t]$) the discriminant t^3+1 of E.

c) $\mathrm{Char}(K_o) = 3$.

Let $t \in K_o$ be transcendental over $\mathbb{F}_3$. Then E is given by the equation

$$Y^2 = X^3 + 2t(t+1)X^2 + (t+1)^2$$

and $P = (t^{-2},t^{-3}+t+1)$. By Zimmer's Theorem, P has an infinite order on E since its x-coordinate, t^{-2}, does not belong to $\mathbb{F}_3[t]$.

(d) $\mathrm{Char}(K_o) = p > 3$.

Let $t \in K_o$ be transcendental over $\mathbb{F}_p$. Then E is given by

$$Y^2 = X^3 + 2X + t^2$$

and $P = (t^{-2},t+t^{-3})$. By Zimmer's Theorem, P has infinite order on E, since its x-coordinate, t^{-2}, does not belong to $\mathbb{F}_p[t]$.

LEMMA 2.4: Let E be an elliptic curve defined by a cubic normal form (as in Lemma 2.3) over K_o and suppose that E has a K_o-rational point $P = (a,b)$ of an infinite order. Let (x,y) be a generic point of E over K_o. Then $[K(y):K] = 2$, $R[y]$ is the integral closure of R in $K(y)$ and $\mathfrak{p} = R[y](x-a)+R[y](y-b)$ is a prime ideal of $R[y]$ which has infinite order modulo principal ideals.

PROOF: By assumption, y satisfies a monic quadratic irreducible equation over $K = K_o(x)$, hence $[K(y):K] = 2$, and y is integral over $R = K_o[x]$. The point (x,y)

is normal on E, so that the ring $R[y] = K_o[x,y]$ is integrally closed. It follows that $R[y]$ is the integral closure of R in $K(y)$. Now, $\mathfrak{p}$ is the kernel of the K_o-epimorphism $K_o[x,y] \to K_o$ which is defined by the specialization $(x,y) \to (a,b)$. Hence $\mathfrak{p}$ is a prime ideal. Let ϕ be the prime divisor of $K(y)$ which is induced by $\mathfrak{p}$ and let ϕ_∞ be the prime divisor of $K(y)$ which corresponds to the infinite point of E. If there were a positive integer m and an element $u \in R[y]$ such that $\mathfrak{p}^m = R[y]u$, then we would have $\phi^m \phi_\infty^{-m} = (u)$, where (u) is the principal divisor of $K(y)$ which corresponds to u. Hence $mP = 0$ (c.f. Cassels [3, p. 211]); which is a contradiction. //

LEMMA 2.5: Let $A,B,C \in K_o$ and put for every $a \in K_o$

$$f_a(X) = (X+a)^3 + A(X+a)^2 + B(X+a) + C .$$

Then there exist only finitely many $b \in K_o$ such that $f_a(x)$ and $f_b(x)$ have a common factor in R.

PROOF: If there were infinitely many $b \in K_o$ such that $f_b(x)$ is not relatively prime to $f_a(x)$ then there would exist a $c \in K_o$ and infinitely many $b \in K_o$ such that $f_b(c) = 0$. But $f_b(c) = f_c(b)$. Hence $f_c(X) = 0$ identically, which is a contradiction. //

LEMMA 2.6: There exists an infinite sequence $\{y_i\}_{i=1}^{\infty}$, of elements of K_s such that

a) $[K(y_i):K] = 2$.

b) $R[y_i]$ is the integral closure of R in $K(y_i)$.

c) There exists a prime ideal $\mathfrak{p}_i$ in $R[y_i]$, which is of infinite order modulo principal ideals.

d) The sequence of iextensions $|\{K(y_i)/K\}_{i=1}^{\infty}$ is linearly disjoint.

PROOF: We define by induction a sequence of pairs (x_i,y_i) of K_s such that they satisfy the conditions

i) $K_o[x_i] = R$

ii) (x_i,y_i) is a generic point over K_o of the elliptic curve E which was defined in Lemma 2.3.

iii) For each $i \geq 2$ the fields $K(y_1,\ldots,y_{i-1})$ and $K(y_i)$ are linearly disjoint over K.

Then Lemma 2.4 together with conditions (i) and (ii) imply (a), (b) and (c). Condition (ii) is equivalent to (d). Suppose that $(x_1,y_1),\ldots,(x_i,y_i)$ have already been defined and they satisfy (i), (ii) and (iii). Write $L = K(y_1,\ldots,y_i)$ and let D be the discriminant of L over K. Then D is an element of R. We distinguish between two cases:

CASE 1: $\mathrm{Char}(K_o) \neq 2$. In this case E is defined by an equation of the form

$$Y^2 = X^3 + AX^2 + BX + C$$

with $A,B,C \in K_o$. We choose an element $a \in K_o$ such that the polynomial $(x+a)^3 + A(x+a)^2 + B(x+a) + C$ does not divide D (in R). This is possible, by Lemma 2.5. Let $x_{i+1} = x+a$ and let y_{i+1} be an element of K_s which satisfies the equation

$$y_{i+1}^2 = (x+a)^3 + A(x+a)^2 + B(x+a) + C .$$

Then $K_o[x_{i+1}] = K_o[x] = R$ and (x_{i+1},y_{i+1}) is a generic point of E over K_o. It follows, by Lemma 2.4, that $[K(y_{i+1}):K] = 2$ and that $R[y_{i+1}]$ is the integral closure of R in $K(y_{i+1})$. Hence the discriminant of $K(y_{i+1})$ over K is equal to $4f(x)$ and hence it

is linearly disjoint from L over K.

CASE 2: $\mathrm{Char}(K_o) = 2$. In this case E is defined by the equation

$$Y^2 + XY = X^3 + tX^2 + (t^3+1)$$

with t in K_o. We choose an $a \in R$ such that $(x+a)^2$ does not divide D. Write $x_{i+1} = x+a$ and let $y_{i+1} \in K_s$ such that

$$y_{i+1}^2 + (x+a)y_{i+1} = (x+a)^3 + t(t+a)^2 + (t^3+1) .$$

The discriminant of the extension $K(y_{i+1})/K$ is equal to $(x+a)^2$. Hence we conclude as before that (x_{i+1}, y_{i+1}) satisfies (i), (ii) and (iii). //

THEOREM 2.7: Let K_o be a field which is not algebraic over a finite field, let x be a transcendental element over K_o and write $R = K_o[x]$, $K = K_o(x)$. Let e be a positive integer. Then, for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ and for every field $K_s(\sigma) \subseteq L \subseteq K$, the class group $C(L)$ has an infinite rank.

PROOF: Let the y_i's and the P_i's be as in Lemma 2.6. Then the set of all $(\sigma) \in \mathcal{G}(K_s/K)^e$ for which $K_s(\sigma)$ contains infinitely many $K(y_i)$'s has measure 1, since the $K(y_i)/K$ are quadratic extensions and since they are linearly disjoint. (c.f. [10, Lemma 1.4]). Our theorem follows now from Lemma 2.2.

The author would like to thank Roquette for his idea of translating x to $x+a$ in the proof of Lemma 2.6. This idea made it possible to improve an earlier version of this section.

3. Algebraic extensions of $\mathbb{Q}$

In this section we take our ring R to be the ring of integers $\mathbb{Z}$ and we consider its integral closure $I(L)$ in an algebraic extension L of $\mathbb{Q}$. We have already mentioned that $C(L)$ is a torsion group. It is therefore natural to look for conditions under which $I(L)$ is a Bezout domain. In this direction we have already shown that $I(\mathbb{Q})$ and almost all the $I(\sigma)$ are Bezout domains. We can further show that if σ is an involution in $\mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})$, i.e. if $\sigma^2 = 1$ and $\sigma \neq 1$, then $I(\sigma)$ is a Bezout domain. The proof of this statement uses ideas which appeared in section 1, so we omit it. One is therefore led to the following question:

PROBLEM 2: Does there exist a $\sigma \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})$ such that $I(\sigma)$ is not a Bezout ring?

G. Frey proved in [7, section 2] that for almost all the $(\sigma) \in \mathcal{G}(\tilde{\mathbb{Q}}/\mathbb{Q})^e$ all the completions of $\tilde{\mathbb{Q}}(\sigma)$ are algebraically closed. One can therefore ask whether this is the reason for the $I(\sigma)$ to be Bezout domain. More precisely we formulate the following problem:

PROBLEM 3: Does there exist a subfield L of $\tilde{\mathbb{Q}}$ such that $I(L)$ is not a Bezout domain but such that all

the completions of L are algebraically closed?

We give here an example of an algebraic extension L of $\mathbb{Q}$ for which $I(L)$ is not a Bezout domain but such that all the complements $L_{\mathfrak{Q}}$ of L with respect to prime ideals $\mathfrak{Q}$ of $I(L)$ are infinite extensions of the corresponding completions of $\mathbb{Q}$.

We consider the field $K = \mathbb{Q}(\sqrt{-5})$. Its class number is 2 (c.f. Borevich and Shafarevich [2, p. 425]). Therefore there exists a prime ideal $\mathfrak{p}$ of $I(K)$ which has the order 2 modulo principal ideals.

Now, let p be an odd prime. For every prime $q \leqslant p$ we find a polynomial

$$f_{p,q}(X) = X^p + a_{1,q}X^{p-1} + \ldots + a_{p,q}$$

with coefficients in $\mathbb{Z}$ which is irreducible modulo q. By the Chinese Remainder Theorem there exists for every $1 \leqslant i \leqslant p$ an integer a_i such that $a_i \equiv a_{i,q} \pmod{q}$ for every prime $q \leqslant p$. Put $f_p(X) = X^p + a_1X^{p-1} + \ldots + a_p$. By Lemma 4.1 we can choose the a_i such that f_p is irreducible over $\mathbb{Q}(\alpha_q \mid q < p)$.

Then $f_p(X)$ is a monic polynomial of degree p and it is irreducible modulo q for every $q \leqslant p$. Let α_p be a root of f_p and denote by L the field generated over K by all the α_p. We show that K has the desired properties.

Indeed, $f_p(X)$ is certainly irreducible over $\mathbb{Q}$, hence $[\mathbb{Q}(\alpha_p) : \mathbb{Q}] = p$. By construction, the sequence of fields $K, \mathbb{Q}(\alpha_3), \mathbb{Q}(\alpha_5), \mathbb{Q}(\alpha_7), \ldots$ is linearly disjoint over $\mathbb{Q}$. Hence the sequence of fields $K(\alpha_3), K(\alpha_5), K(\alpha_7), \ldots$ is linearly disjoint over K. In particular we have that every finite subextension of L/K has an odd degree. Assume that $I(L)$ is a Bezout domain. Then $pI(L)$ must be a principal ideal of $I(L)$. It follows, as in the proof of Lemma 2.1, that there exists a finite subextension K'/K of L/K such that $p^{[K':K]}$ is a principal ideal in $I(K)$. Since p has the order 2 modulo principal ideals we have that $[K' : K]$ is an even number, which is a contradiction.

Now, let q be a prime and let $\mathfrak{Q}$ be a prime ideal of $I(L)$ which extends $q\mathbf{Z}$. Then for all primes p greater than q the polynomial $f_p(X)$ is irreducible modulo q and hence $[L_{\mathfrak{Q}} : \mathbb{Q}_q] \geq [\mathbb{Q}_q(\alpha_p) : \mathbb{Q}_q] = p$. It follows that $[L_{\mathfrak{Q}} : \mathbb{Q}_q] = \infty$.

PROBLEM 4: Is $I(\mathbb{Q}_{ab})$ a Bezout domain? ($\mathbb{Q}_{ab}$ denotes the maximal abelian extension of $\mathbb{Q}$.)

4. Prime ideals in $I(\sigma)$ over a Dedekind domain

In this section we consider a denumerable Dedekind domain R with a hilbertian quotient field K and show that for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ the prime ideals in the ring $I(\sigma)$ behave like the prime ideals in the ring $I(\tilde{K})$. We begin by proving a general Lemma on hilbertian valuated fields.

LEMMA 4.1: Let v be a non-trivial valuation of a hilbertian field K. Then every hilbertian subset H of K^r is dense in K^r in the v-topology.

PROOF: We write v additively and denote by Γ the value group of K under v. Let H be a hilbertian set of K^r. Then there exist irreducible polynomials $f_\lambda \in K(T_1,\ldots,T_r)[X_1,\ldots,X_n]$, $\lambda = 1,\ldots,l$, such that $H = \{(t) \in K^r \mid f_\lambda(t,X)$ is defined and irreducible in $K[X]$ for every $1 \leqslant \lambda \leqslant l\}$.

Let $(a) \in K^r$ and let $\gamma \in \Gamma$. Then there exists $c \in K$, $c \neq 0$ such that $v(c) > \gamma$. Consider the finite set of all the polynomials of the form

$$f_\lambda(a_1 + cT_1^{\varepsilon_1},\ldots,a_r + cT_r^{\varepsilon_r},X)$$

where $1 \leqslant \lambda \leqslant l$ and $\varepsilon_i = \pm 1$ for $i = 1,\ldots,r$. All these polynomials are defined and irreducible in $K(T)[X]$. Since K is hilbertian there exist $s_1,\ldots,s_r \in K$ such that all the polynomials

$$f_\lambda(a_1 + cs_1^{\varepsilon_1},\ldots,a_r + cs_r^{\varepsilon_r},X)$$

are defined and irreducible in $K[X]$. For every $1 \leqslant i \leqslant r$ we specify ε_i to be 1 or -1 according to whether $v(s_i) \geqslant 0$ or $v(s_i) < 0$. Then we put $t_i = a_i + cs_i^{\varepsilon_i}$ and it is clear that $v(t_i - a_i) > \gamma$ for every $1 \leqslant i \leqslant r$ and $(t) \in H$.

It follows that H is v-dense in K_r. //

PROBLEM 5: Let R be a Kedekind domain with a hilbertian quotient field K. Is R itself a hilbertian domain?

We recall that if L is a finite separable extension of a hilbertian field K then every hilbertian subset of L^r contains a hilbertian subset of K^r (c.f. Lang [14, p. 152]). With this in mind we have the following Lemma:

LEMMA 4.2: Let R be a Dedekind domain with a hilbertian field K. Let $\mathfrak{p}$ be a prime ideal of R and let L' be a finite separable extension of K. Then there exists a quadratic separable extension L of K which is linearly disjoint from L' over K such that $\mathfrak{p}$ decomposes in L to a product of two different prime ideals.

PROOF: Consider the absolutely irreducible polynomial $X^2 + T_1X + T_2$. By Lemma 4.1 there exist $t_1, t_2 \in R_{\mathfrak{p}}$ such that

$$t_1 \equiv 1 \pmod{\mathfrak{p}}, \quad t_2 \equiv 0 \pmod{\mathfrak{p}},$$

and such that the polynomial $X^2 + t_1X + t_2$ is irreducible over L'. Then $X^2 + t_1X + t_2$ decomposes modulo $\mathfrak{p}$ to a product of two different linear factors,

$$X^2 + t_1X + t_2 \equiv X(X + 1) \pmod{\mathfrak{p}}.$$

Hence, if x is a root of $X^2 + t_1X + t_2$ in K, then $L = K(x)$ is the desired quadratic extension of K (c.f. Borevich-Shafarevich [2, p. 203]).

THEOREM 4.3: Let R be a Dedekind domain with a denumerable hilbertian quotient field K. Then almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ have the following two properties:

1) For every nontrivial real valuation v of $K_s(\sigma)$ the completion $K_s(\sigma)_v$ is algebraically closed.

2) For every finite extension L of K which is contained in $K_s(\sigma)$ and for every prime ideal $\mathfrak{p}$ of $I(L)$ there exist in $I(\sigma)$ at least two distinct prime ideals which lie over $\mathfrak{p}$.

PROOF: Define S_1 to be the set of all $(\sigma) \in \mathcal{G}(K_s/K)^e$ that have the property that every absolutely irreducible algebraic variety which is defined over $K_s(\sigma)$ has a rational point over $K_s(\sigma)$. Fields with this property

are called PAC fields. In [10, Thm. 2.5] it was proved that $\mu(S_1) = 1$. It follows, by a theorem of Frey ([7], Thm. 2) that if $(\sigma) \in S_1$ and v is a real valuation of $K_s(\sigma)$ then $K_s(\sigma)_v$ is separably closed. But if M is any complete field under a real valuation v which is separably closed then it is algebraically closed. Indeed let $p = \mathrm{char}(M)$, let $a \in M$ and let $x \in \tilde{M}$ such that $x^q = a$ where $q = p^m$, $m \geq 1$. Take a $b \in M$, $b \neq 0$, such that $v(b)$ is a big real number. Then $Y^q - bY - a$ is a separable polynomial over M. Its roots $y_1,\ldots,y_q$ must lie in M. Now

$$bx = x^q + bx - a = \prod_{i=1}^{q}(x - y_i)$$

$$\Rightarrow v(b) + v(x) = \sum_{i=1}^{q} v(x - y_i) \quad .$$

It follows that for at least one i between 1 and q, $v(x - y_i)$ must be big. This means that M is dense in $\tilde{M}$. Since M is also closed it must coincide with $\tilde{M}$. It follows that $K_s(\sigma)_v$ is algebraically closed.

2) Let L be a finite separable extension of K and let $\mathfrak{p} \in P(L)$. According to Lemma 5.2 we can construct by induction a linearly disjoint sequence, $\{L_i/K\}_{i=1}^{\infty}$, of quadratic separable extensions such that $\mathfrak{p}$ decomposes in every L_i into a product of two different primes. If $(\sigma) \in \mathcal{G}(K_s/L_i)^e$ then $K_s(\sigma)$ contains L_i and hence there exist in $I(\sigma)$ at least two different prime ideals which lie over $\mathfrak{p}$. It follows that the set $\bigcup_{i=1}^{\infty} \mathcal{G}(K_s/L_i)^e$ is contained in the set $S(L,\mathfrak{p})$ of all the $(\sigma) \in \mathcal{G}(K_s/L)^e$ for which there exist in $I(\sigma)$ at least two different prime ideals which lie over $\mathfrak{p}$. By [10, Lemma 1.10], $\bigcup_{i=1}^{\infty} \mathcal{G}(K_s/L_i)^e$ is almost equal

to $\mathcal{G}(K_s/L)^e$, hence $\mu(\mathcal{G}(K_s/L)^e - S(L,\mathfrak{p})) = 0$. Denote now by S_2 the set of all $(\sigma) \in \mathcal{G}(K_s/K)^e$ which have the property (2). It is clear that

$$(3) \qquad \mathcal{G}(K_s/K)^e - S_2 = \bigcup_{L,\mathfrak{p}} [\mathcal{G}(K_s/L)^e - S(L,\mathfrak{p})]$$

where L runs over all finite separable extensions of K and $\mathfrak{p}$ runs over all elements in $P(L)$. Since there are only a countable number of pairs $(L,\mathfrak{p})$ we get that the measure of the right hand side of (3) is 0. It follows that $\mu(S_2) = 1$.

5. A fixed high field over a Dedekind domain

Let R be a Dedekind domain with the quotient field K. From now on we consider a fixed infinite separable algebraic extension M of K. Write $T = I(M)$ for the integral closure of R in M and let $\mathcal{L}$ be the family of all finite extensions L of K which are contained in M. Then T is a Prüfer domain in which every non-zero prime ideal is maximal.

In particular, if $\mathfrak{P} \in P(M)$ is a prime ideal of T then its local ring $T_{\mathfrak{P}}$ is a valuation ring (c.f. Gilmer [8, p. 254]). Let $v_{\mathfrak{P}}$ be the corresponding (additive) valuation, normalized in such a way that if $\mathfrak{p} = \mathfrak{P} \cap R$ then the restriction $v_{\mathfrak{p}}$ of $v_{\mathfrak{P}}$ to K satisfies $v_{\mathfrak{p}}(K) = \mathbb{Z}$. Then $v_{\mathfrak{P}}(M)$ is a subgroup of $\mathbb{Q}$. Assume that M satisfies the following two hypotheses which make it a "high" field:

(I) $v_{\mathfrak{P}}(M) = \mathbb{Q}$ for every $\mathfrak{P} \in P(M)$.

(II) For every $L \in \mathcal{L}$ and for every $\mathfrak{p} \in P(L)$ there exist at least two prime ideals of T which lie over $\mathfrak{p}$.

Using these two hypotheses we are able to give, with the help of some results of Krull a description of the structure of $J(M)$ and deduce some interesting

properties of it. Our interest in these high fields comes from the fact that if K is denumerable and hilbertian then for almost all $(\sigma) \in \mathcal{G}(K_s/K)^e$ the field $K_s(\sigma)$ satisfies hypotheses (I) and (II), as follows from Theorem 5.3. This means that any result which we prove for M is valid for the above $K_s(\sigma)$.

We begin with the following Theorem:

THEOREM 5.1:

a) Let $\mathfrak{p} \in P(K)$ and let e be a positive integer. Then there exists an $L \in \mathcal{L}$ such that for every $\mathfrak{P} \in P(M)$ which lies over $\mathfrak{p}$ the ramification index $e(\mathfrak{P} \cap L/\mathfrak{p})$ is divisible by e.

b) If $L \in \mathcal{L}$ and $\mathfrak{p} \in P(L)$, then there exist at least $2^{\aleph_0}$ distinct prime ideals of T which lie over $\mathfrak{p}$.

c) Every prime ideal $\mathfrak{P} \in P(M)$ is idempotent, i.e. $\mathfrak{P}^2 = \mathfrak{P}$.

d) For every prime ideal $\mathfrak{P} \in P(M)$, the prime ideal $\mathfrak{P}T_{\mathfrak{P}}$ of $T_{\mathfrak{P}}$ is not finitely generated, hence $T_{\mathfrak{P}}$ is not a noetherian domain.

e) Let $\mathfrak{P} \in P(M)$. Then every $\mathfrak{P}$-primary ideal $\mathfrak{Q}$ of T is not finitely generated and hence is not invertible.

f) If $\mathfrak{Q}$ is a $\mathfrak{P}$-primary ideal which is different from $\mathfrak{P}$ then $\bigcap_{n=1}^{\infty} \mathfrak{Q}^n = 0$.

g) Let $\mathfrak{a}$ be an ideal of T. If $\mathfrak{a}$ has a $\mathfrak{P}$-primary component which is properly contained in $\mathfrak{P}$ then $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = 0$, otherwise $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = \mathfrak{a}$.

h) If $\mathfrak{a}$ is finitely generated then the $\mathfrak{P}$-primary component $\mathfrak{a}T_{\mathfrak{P}} \cap T$ of $\mathfrak{a}$ is properly contained in $\mathfrak{P}$ for every $\mathfrak{P} \in P(M)$ which contains $\mathfrak{a}$; hence, if $\mathfrak{a} \neq T$ then $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = 0$.

PROOF:

a) Suppose that for every $L \in \mathfrak{L}$ there exists a $\mathfrak{P} \in P(M)$ which lies over $\mathfrak{p}$ such that $e(\mathfrak{P} \cap L/\mathfrak{p})$ is not divisible by e. Let $S(L)$ be the set of all $\mathfrak{p}' \in P(L)$ which lie over $\mathfrak{p}$ for which $e(\mathfrak{p}'/\mathfrak{p})$ is not divisible by e. By our assumption $S(L)$ is a finite non-empty set. If $L_1 \in \mathfrak{L}$, $L_1 \supseteq L$, and $\mathfrak{p}_1 \in S(L_1)$ then $e(\mathfrak{p}_1/\mathfrak{p})$ is divisible by $e(\mathfrak{p}_1 \cap L/\mathfrak{p})$, and hence $\mathfrak{p}_1 \cap L \in S(L)$. It follows that the collection of the sets $S(L)$ together with the maps $\mathfrak{p}_1 \longmapsto \mathfrak{p}_1 \cap L$ form an inverse system with respect to inclusion. The inverse limit of this system is not empty (c.f. Eilenberg and Steenord [5, Thm. 3.6]). Every element of this limit defines a $\mathfrak{P} \in P(M)$ such that $\mathfrak{P} \cap L \in S(L)$ for every $L \in \mathfrak{L}$. For such a $\mathfrak{P}$ we have, by (I)

$$\bigcup_{L \in \mathfrak{L}} v_{\mathfrak{P}}(L) = v_{\mathfrak{P}}(M) = Q \quad .$$

Hence there exists an $L \in \mathfrak{L}$ such that $\frac{1}{e} \in v_{\mathfrak{P}}(L)$.

It follows that e divides $(v_{\mathfrak{P}}(L) : v_{\mathfrak{P}}(K)) = e(\mathfrak{P} \cap L/\mathfrak{p})$ which is a contradiction.

b) According to (II) there exists an $L_1 \in \mathfrak{L}$, $L_1 \supseteq L$, such that there exist two distinct prime ideals $\mathfrak{p}_0, \mathfrak{p}_1 \in P(L_1)$ which lie over $\mathfrak{p}$. Each one of these ideals can be extended in an appropriate extension $L_2 \in \mathfrak{L}$ of L in two different ways, and so on. Since this process continues indefinitely we get that there are at least $2^{\aleph_0}$ ideals in $P(M)$ which lie over $\mathfrak{p}$.

c) We prove first that $\mathfrak{P} T_{\mathfrak{P}} = \mathfrak{P}^2 T_{\mathfrak{P}}$. Indeed, let $x \in \mathfrak{P} T_{\mathfrak{P}}$, where $x \neq 0$. Then there exists a $z \in M$ such that $v_{\mathfrak{P}}(z) = \frac{1}{2} v_{\mathfrak{P}}(x)$. Hence $u = z^{-2}x$ is invertible in $T_{\mathfrak{P}}$, $z \in \mathfrak{P}$ and $x = uz^2 \in \mathfrak{P}^2 T_{\mathfrak{P}}$.

Now, $\mathfrak{P}^2$ is $\mathfrak{P}$-primary, since $\mathfrak{P}$ is maximal. Hence $\mathfrak{P}^2 = \mathfrak{P}^2 T_{\mathfrak{P}} \cap T = \mathfrak{P} T_{\mathfrak{P}} \cap T = \mathfrak{P}$.

d) Since $\mathfrak{P} T_{\mathfrak{P}} = \mathfrak{P}^2 T_{\mathfrak{P}}$, $\mathfrak{P} T_{\mathfrak{P}}$ is not invertible in $T_{\mathfrak{P}}$. This means that $\mathfrak{P} T_{\mathfrak{P}}$ is not finitely generated, since $T_{\mathfrak{P}}$ is a valuation ring.

e) If $\mathfrak{Q}$ were finitely generated then there would have exist an $L \in \mathfrak{L}$ and an ideal $\mathfrak{q}$ of $I(L)$ such that $\mathfrak{q} T = \mathfrak{Q}$. By (II) there exist at least two distinct prime ideals of T which contain $\mathfrak{q}$. These prime ideals must also contain $\mathfrak{Q}$ which is impossible.

f) By Gilmer [8, p. 269] $\bigcap_{n=1}^{\infty} \mathfrak{Q}^n$ is a prime ideal of T which is properly contained in . Hence it must be 0.

g) The $\mathfrak{P}$-primary component of $\mathfrak{a}$ is $\mathfrak{a} T_{\mathfrak{P}} \cap T$. If $\mathfrak{a} T_{\mathfrak{P}} \cap T$ is properly contained in $\mathfrak{P}$ for at least one $\mathfrak{P} \in P(M)$ then it follows from (f) that $\bigcap_{n=1}^{\infty} \mathfrak{a}^n = 0$. Otherwise $\mathfrak{a} T_{\mathfrak{P}} \cap T$ is equal to either T or to $\mathfrak{P}$. In both cases we have that $(\mathfrak{a} T_{\mathfrak{P}})^2 = \mathfrak{a} T_{\mathfrak{P}}$. Hence

$$\bigcap_{n=1}^{\infty} \mathfrak{a}^n = \bigcap_{n=1}^{\infty} \bigcap_{\mathfrak{P}} \mathfrak{a}^n T_{\mathfrak{P}} = \bigcap_{\mathfrak{P}} \bigcap_{n=1}^{\infty} \mathfrak{a}^n T_{\mathfrak{P}} = \bigcap_{\mathfrak{P}} \mathfrak{a} T_{\mathfrak{P}} = \mathfrak{a}.$$

h) There exists an $L \in \mathfrak{L}$ and an ideal $\mathfrak{A}$ of $I(L)$ such that $\mathfrak{a} = \mathfrak{A} T$. Let $\mathfrak{P} \in P(M)$, $\mathfrak{P} \supseteq \mathfrak{a}$. Put $\mathfrak{p} = \mathfrak{P} \cap L$; by (a) there exists an $L_1 \in \mathfrak{L}$, $L_1 \supseteq L$ such that $\mathfrak{p} I(L_1) \subseteq (\mathfrak{P} \cap L_1)^2$. If $\mathfrak{P} = \mathfrak{a} T_{\mathfrak{P}} \cap T$ then

$$\mathfrak{P} \cap L_1 = \mathfrak{A} T_{\mathfrak{P}} \cap I(L_1) \subseteq (\mathfrak{P} \cap L_1)^2$$

which is impossible. //

REMARK: The method of proof of (g) is essentiallly the same as that of Theorem 2.3 of [1].

6. Characterization of ideals by a pair of functions

It is well known that the set $J(M)$ can be given the Krull topology with a basis the sets of the form $\{\mathfrak{a} \in J(M) \mid \mathfrak{a} \cap L = \mathfrak{A}\}$ where $L \in \mathcal{L}$ and $\mathfrak{A}$ is an ideal of $I(L)$. Unfortunately the multiplication in $J(L)$ is not continuous in this topology, as we shall see later. Nevertheless it motivates the following parametrisation of $J(M)$, which is due to Krull, and which generalizes the usual representation of ideals in a Dedekind domain as products of powers of prime ideals.

Denote by $\mathcal{F}$ the set of all pairs (ϕ,ψ) of functions

$$\phi : P(M) \longrightarrow \{0,1\} \qquad \psi : P(M) \longrightarrow \mathbb{R}$$

which satisfy the following conditions:

1) $\phi(\mathfrak{p}) = 1 \Rightarrow \psi(\mathfrak{p}) \in \mathbb{Q}$.

2a) There exists only a finite number of prime ideals $\mathfrak{P} \in P(K)$ which are contained in the prime ideals of T belonging to the set

$$S(\phi,\psi) = \{\mathfrak{p} \in P(M) \mid \psi(\mathfrak{p}) \neq 0 \text{ or } \phi(\ ) = 0 \text{ and } \psi(\mathfrak{p}) = 0\}$$

(which we call "the support of (ϕ,ψ)").

2b) The function ψ is bounded.

3a) If $\phi(\mathfrak{p}_0) = 0$ then for every $\varepsilon > 0$ there exists an $L \in \mathcal{L}$ such that for every $\mathfrak{p} \in P(M)$

$$\mathfrak{p} \cap L = \mathfrak{p}_0 \cap L \Rightarrow \psi(\mathfrak{p}) \leq \psi(\mathfrak{p}_0) + \varepsilon .$$

3b) If $\phi(\mathfrak{P}_o) = 1$ then there exists an $L \in \mathfrak{L}$ such that for every $\mathfrak{P} \in P(M)$

$$\phi(\mathfrak{P}) = 1 \ \& \ \mathfrak{P} \cap L = \mathfrak{P}_o \cap L \Rightarrow \psi(\mathfrak{P}) \leqslant \psi(\mathfrak{P}_o)$$

$$\phi(\mathfrak{P}) = 0 \ \& \ \mathfrak{P} \cap L = \mathfrak{P}_o \cap L \Rightarrow \psi(\mathfrak{P}) < \psi(\mathfrak{P}_o) \ .$$

One easily verifies that $\mathfrak{F}$ is an abelian semi-group with respect to the composition law

$$(\phi,\psi) * (\phi_2,\psi_2) = (\phi_1\phi_2, \psi_1 + \psi_2) \ .$$

The unit of $\mathfrak{F}$ is the pair $(1,0)$.

To every fractional ideal $\mathfrak{a} \in J(M)$ we attach two functions

$$\phi_{\mathfrak{a}} : P(M) \longrightarrow \{0,1\} \qquad \psi_{\mathfrak{a}} : P(M) \longrightarrow \mathbb{R}$$

by means of the following rules:

a) $\phi_{\mathfrak{a}}(\mathfrak{P}) = 1$ if there exists an $a \in \mathfrak{a}$ such that $v_{\mathfrak{P}}(a) = v_{\mathfrak{P}}(\mathfrak{a}) = \mathrm{Inf}\{v_{\mathfrak{P}}(a) \mid a \in \mathfrak{a}\}$, otherwise $\phi_{\mathfrak{a}}(\mathfrak{P}) = 0$.
b) $\psi_{\mathfrak{a}}(\mathfrak{P}) = v_{\mathfrak{P}}(\mathfrak{a})$.

THEOREM 6.1: The map $\mathfrak{a} \longmapsto (\phi_{\mathfrak{a}},\psi_{\mathfrak{a}})$ is a unitary isomorphism of the semi-group $J(M)$ onto $\mathfrak{F}$.

PROOF: The theorem is a consequence of a theorem of Krull [13, Satz 23] which was proved for the case $R = \mathbb{Z}$ but is equally true over any Dedekind domain R. We note that in deducing our Theorem from that of Krull's one has to use hypothesis (I) and Theorem 5.1 d.

Corollary 6.2: For every $\mathfrak{a} \in J(M)$ and for every positive integer n there exists a unique $\mathfrak{B} \in J(M)$ such that $\mathfrak{B}^n = \mathfrak{a}$.

PROOF: This follows from the isomorphism established in Theorem 6.1 and from the fact that $\mathcal{F}$ has the corresponding property.

7. Primary ideals

In this section we consider a fixed prime ideal $\mathfrak{P} \in P(M)$ and the set of all $\mathfrak{P}$-primary ideals of T. This is a semi-group which we denote by $J(M,\mathfrak{P})$ (c.f. Gilmer [8, p. 269]). From the fact that each non-zero prime ideal of T is maximal it follows that a proper ideal $\mathfrak{Q} \in J(M)$ is $\mathfrak{P}$-primary if and only if $\phi_{\mathfrak{Q}}(\mathfrak{P}') = 1$ and $\psi_{\mathfrak{Q}}(\mathfrak{P}') = 0$ for every $\mathfrak{P}' \in P(M)$ which is different from $\mathfrak{P}$.

Denote by $J_0(M,\mathfrak{P})$ $(J_1(M,\mathfrak{P}))$ the set of all $\mathfrak{P}$-primary ideals $\mathfrak{Q}$ for which $\phi_{\mathfrak{Q}}(\mathfrak{P}) = 0$ $(\phi_{\mathfrak{Q}}(\mathfrak{P}) = 1)$. In order to describe these sets we introduce two new topologies in $\mathbb{R}$, the <u>right topology</u> and the <u>left topology</u>. A basis for the right (resp. left) topology is the set of all semi-closed intervals of the form $(a,b]$ (resp. $[a,b)$) where $a < b$ are rational numbers. Obviously both topologies are stronger then the usual topology.

<u>THEOREM 7.1:</u>

a) $J_1(M,\mathfrak{P})$ is a sub-semi-group of $J(M,\mathfrak{P})$ which is algebraicaly and topologically isomorphic to the additive semi-group $\mathbb{Q}_{>0}$ of the positive rational numbers with the right topology. An ideal $\mathfrak{Q} \in J_1(M,\mathfrak{P})$ corresponds under this isomorphism to $v_{\mathfrak{P}}(\mathfrak{Q})$. Conversely, $r \in \mathbb{Q}_{>0}$ corresponds to the ideal

$$\mathfrak{Q}_{1,r} = \{x \in T \mid v_{\mathfrak{P}}(x) \geq r \ \& \ [\forall \mathfrak{P}' \in P(M) : \mathfrak{P}' \neq \mathfrak{P} \Rightarrow v_{\mathfrak{P}'}(x) = 0]\}$$

b) $J_o(M,\mathfrak{P})$ is a unitary sub-semi-group of $J(M,\mathfrak{P})$ which is algebraically and topologically isomorphic to the additive semi-group $\mathbb{R}_{\geq 0}$ of the non-negative real numbers with the left topology. An ideal $\mathfrak{A} \in J_o(M,\mathfrak{P})$ corresponds to $v_{\mathfrak{P}}(\mathfrak{A})$. Conversely, $s \in \mathbb{R}_{\geq 0}$ corresponds to the ideal

$$\mathfrak{A}_{o,s} = \{x \in T \mid v_{\mathfrak{P}}(x) > s \ \& \ [\forall \mathfrak{P}' \neq \mathfrak{P} \Rightarrow v_{\mathfrak{P}'}(x) = 0]\} .$$

c) For every $r \in \mathbb{Q}_{>0}$ and $s \in \mathbb{R}_{\geq 0}$ we have

$$\mathfrak{A}_{1,r} \cdot \mathfrak{A}_{o,s} = \mathfrak{A}_{o,r+s} .$$

PROOF:

a) The fact that the map $\mathfrak{A} \longmapsto v_{\mathfrak{P}}(\mathfrak{A})$ is an algebraic isomorphism of $J_1(M,\mathfrak{P})$ onto $\mathbb{Q}_{>0}$ whose inverse is the map $r \longmapsto \mathfrak{A}_{1,r}$, follows easily from Theorem 6.1. In order to prove that this map is also a homeomorphism we need the following Lemma:

LEMMA: Let $L \in \mathfrak{L}$, $r \in \mathbb{Q}_{>0}$ and $m \in \mathbb{Z}_{>0}$. Then

$$(*) \qquad \frac{m-1}{e} < r \leq \frac{m}{e} \iff \mathfrak{A}_{1,r} \cap L = \mathfrak{P}_L^m$$

where $\mathfrak{P}_L = \mathfrak{P} \cap L$ and $e = e(\mathfrak{P}_L/\mathfrak{P}_K)$.

PROOF OF THE LEMMA: Suppose that $\mathfrak{A}_{1,r} \cap L = \mathfrak{P}_L^m$. There exists an $L' \in \mathfrak{L}$, $L' \supseteq L$ such that $v_{\mathfrak{P}}(\mathfrak{A}_{1,r} \cap L') = r$. Put $e' = e(\mathfrak{P}_{L'}/\mathfrak{P}_L)$. Then $\mathfrak{A}_{1,r} \cap L' = \mathfrak{P}_{L'}^i$ where

$$(m-1)e' + 1 \leq i \leq me' ,$$

since $\mathfrak{A}_{1,r} \cap L'$ lies over $\mathfrak{P}_L^m$. Hence

$$((m-1)e' + 1)v_{\mathfrak{P}}(\mathfrak{P}_{L'}) \leq v(\mathfrak{A}_{1,r} \cap L') \leq me' v_{\mathfrak{P}}(\mathfrak{P}_{L'}) .$$

Since $\mathfrak{P}_{L'}$ lies over $\mathfrak{P}_L$,

$$v_{\mathfrak{O}}(\mathfrak{P}_{L'}) = \frac{v_{\mathfrak{O}}(\mathfrak{P}_L)}{e'} = \frac{1}{ee'} \quad .$$

It follows that

$$\frac{m-1}{e} < \frac{(m-1)e'+1}{ee'} \leqslant r \leqslant \frac{m}{e} \quad .$$

Thus, we have proved that the right hand side of (*) implies its left hand side. Since this is true for every m, the converse implication is also valid.

We return now to the proof of (1) and prove that the map $\mathfrak{Q} \longmapsto v_{\mathfrak{O}}(\mathfrak{Q})$ is continuous. Let $\mathfrak{Q} \in J_1(M,\mathfrak{O})$, $r \in v_{\mathfrak{O}}(\mathfrak{Q})$ and a,b be two positive rational numbers such that $a < r \leqslant b$. We write r in the form $r = \frac{m'}{l}$ where $m', l \in \mathbb{Z}_{>0}$. By Theorem 5.1a there exists an $L \in \mathfrak{L}$ such that $e = e(\mathfrak{P}_L/\mathfrak{P}_K)$ is a multiple of l, $e = kl$ and such that $\frac{1}{e} < r - a$. Put $m = km'$. Let now $\mathfrak{Q}' \in J_1(M,\mathfrak{O})$ be an ideal which satisfies $\mathfrak{Q}' \cap L = \mathfrak{P}_L^m$. Then, by the lemma $a < v_{\mathfrak{O}}(\mathfrak{Q}') \leqslant b$. It follows that the map is continuous.

Conversely, let $r \in \mathbb{Q}_{>0}$, let $L \in \mathfrak{L}$, $e = e(\mathfrak{P}_L/\mathfrak{P}_K)$ and $\mathfrak{Q}_{1,r} \cap L = \mathfrak{P}_L^m$. Then $\frac{m-1}{e} < r \leqslant \frac{m}{e}$, by the Lemma. If r' is any element of $\mathbb{Q}_{>0}$ which satisfies $\frac{m-1}{e} < r' \leqslant \frac{m}{e}$ then $\mathfrak{Q}_{1,r'} \cap L = \mathfrak{P}_L^m$, by the lemma. It follows that the map $r \mapsto \mathfrak{Q}_{1,r}$ is also continuous.

b) The algebraic part of the statement follows from Theorem 6.1. The topological part follows as in (1) from the following lemma:

LEMMA: For every $s \geqslant 0$ and for every positive integer m

$$(**) \qquad \frac{m-1}{e} \leqslant s < \frac{m}{e} \iff \mathfrak{Q}_{0,s} \cap L = \mathfrak{P}_L^m$$

where $e = e(\mathfrak{P}_L/\mathfrak{P}_K)$.

PROOF OF THE LEMMA: Suppose that $\mathfrak{Q}_{o,s} \cap L = \mathfrak{P}_L^m$. Let $L' \in \mathfrak{L}$, $L' \supseteq L$ and put $e' = e(\mathfrak{P}_{L'}/\mathfrak{P}_L)$. As before we get that

$$\frac{m-1}{e} < v_{\mathfrak{P}}(\mathfrak{Q}_{o,s} \cap L') \leq \frac{m}{e} .$$

Now $s = \mathrm{Inf}\{v_{\mathfrak{P}}(\mathfrak{Q}_{o,s} \cap L') \mid L' \in \mathfrak{L}, L' \supseteq L\}$. Hence

$$\frac{m-1}{e} \leq s \leq \frac{m}{e} .$$

The equality $s = \frac{m}{e}$ is not possible since $v_{\mathfrak{P}}(\mathfrak{P}_L^m) = \frac{m}{e}$.

Hence $\frac{m-1}{e} \leq s < \frac{m}{e}$.

Thus, the right hand side of (**) implies its left hand side. Since this is true for every m, the converse implication is also valid.

c) This follows from Theorem 6.1.

COROLLARY 7.2:

a) $\mathfrak{P}\mathfrak{Q} = \mathfrak{Q}$ for every $\mathfrak{Q} \in J_o(M,\mathfrak{P})$.

b) The multiplication in $J_1(M,\mathfrak{P})$ is continuous.

c) The multiplication in $J_o(M,\mathfrak{P})$ and hence in $J(M)$ is not continuous.

PROOF: (a) and (b) are clear. For (c) one proves that the addition in $R_{>o}$ is not continuous in the left topology since there exist two irrational numbers $s_1, s_2 \geq 0$ whose sum $s_1 + s_2$ is rational. //

8. Finitely generated fractional ideals

Denote by $\mathfrak{F}^*$ the set of all functions $\psi : P(M) \longrightarrow \mathbb{Q}$ which satisfy the following conditions:

1) There exists only a finite number of prime ideals $\mathfrak{P} \in P(K)$ which are contained in prime ideals of T belonging to the set $\{\mathfrak{P} \in P(M) \mid \psi(\mathfrak{P}) \neq 0\}$.

2) The function ψ is bounded.

3) For every $\mathfrak{P}_0 \in P(M)$ there exists an $L \in \mathfrak{L}$ such that for every $\mathfrak{P} \in P(M)$

$$\mathfrak{P} \cap L = \mathfrak{P}_0 \cap L \Rightarrow \psi(\mathfrak{P}) = \psi(\mathfrak{P}_0) .$$

Obviously $\mathfrak{F}^*$ is an abelian group with respect to addition and the map $\psi \longmapsto (1,\psi)$ is an imbedding of $\mathfrak{F}^*$ in $\mathfrak{F}$.

THEOREM 8.1: The map $\mathfrak{a} \longmapsto \psi$ of $J^*(M)$ onto $\mathfrak{F}^*$ is an isomorphism.

PROOF: By Theorem 6.1 we have only to prove that in the isomorphism $\mathfrak{a} \longmapsto (\phi_{\mathfrak{a}}, \psi_{\mathfrak{a}})$ of $J(M)$ onto $\mathfrak{F}$, $J^*(M)$ is mapped onto $(1,\mathfrak{F}^*)$.

Indeed let $\mathfrak{a} \in J^*(M)$ and let $\mathfrak{P}_0 \in P(M)$. Then, by Theorem 6.1 there exists an $L \in \mathfrak{L}$ such that

$$\mathfrak{P} \cap L = \mathfrak{P}_0 \cap L \Rightarrow \psi_{\mathfrak{a}}(\mathfrak{P}) \leq \psi(\mathfrak{P}_0)\, \psi_{\mathfrak{a}^{-1}}(\mathfrak{P}) \leq \psi_{\mathfrak{a}^{-1}}(\mathfrak{P}_0)$$

$$\Rightarrow \psi_{\mathfrak{a}}(\mathfrak{P}) = \psi_{\mathfrak{a}}(\mathfrak{P}_0) .$$

Hence $\mathfrak{a}$ satisfies condition (3). Obviously it satisfies conditions (1) and (2). Hence $\psi_{\mathfrak{a}} \in \mathfrak{F}^*$. Also $\phi_{\mathfrak{a}} = 1$. Conversely it is clear that the map is surjective since $\mathfrak{F}^*$ is a group.

COROLLARY 8.2: For every $\mathfrak{a} \in J^*(M)$ and for every positive integer n there exists a unique $\mathfrak{B}$ in $J^*(M)$ such that $\mathfrak{B}^n = \mathfrak{a}$.

DEFINITION: A fractional ideal $\mathfrak{a} \in J(M)$ is said to be locally finitely generated if for every $\mathfrak{P}_o \in P(M)$ there exists an $L \in \mathfrak{L}$ and elements $a_1,\ldots,a_n \in L$ which generate $\mathfrak{a}T_{\mathfrak{P}}$ for every $\mathfrak{P} \in P(M)$ which satisfies $\mathfrak{P} \cap L = \mathfrak{P}_o \cap L$.

COROLLARY 8.3: Every locally finitely generated fractional ideal $\mathfrak{a} \in J(M)$ is finitely generated.

PROOF: Let $\mathfrak{P}_o \in P(M)$ and let L and $a_1,\ldots,a_n$ be as in the definition. Let $\mathfrak{P} \in P(M)$ be an ideal which satisfies $\mathfrak{P} \cap L = \mathfrak{P}_o \cap L$. Then

$$\psi_{\mathfrak{a}}(\mathfrak{P}) = \min_{1\leq i\leq n} v_{\mathfrak{P}}(a_i) = \min_{1\leq i\leq n} v_{\mathfrak{P}_o}(a_i) = \psi_{\mathfrak{a}_o}(\mathfrak{P})$$

Hence $\psi_{\mathfrak{a}} \in \mathfrak{F}^*$. By Theorem 8.1 $\mathfrak{a} \in J^*(M)$.

We note that an $\mathfrak{a} \in J(M)$ which is pointwise finitely generated, i.e. one for which $\mathfrak{a}T_{\mathfrak{P}}$ is finitely generated for every $\mathfrak{P} \in P(M)$, must not belong to $J^*(M)$. Indeed, if $\mathfrak{P}_o \in P(M)$ then any $\mathfrak{Q} \in J_1(\mathfrak{P}_o,M)$ is pointwise finitely generated but is not finitely generated, by Theorem 5.1. Such a $\mathfrak{Q}$ does exist by Theorem 7.1.

References

[1] ARNOLD, J.T., GILMER, R.: Idempotent ideals and unions of nets of Prüfer domains. J. Sci. Hiroshima Univ. Ser. A-I 3 131-145 (1967).

[2] BOREVICH, Z.I., SHAFAREVICH, I.R.: Number Theory, Academic Press, New York and London.

[3] CASSELS, J.W.S.: Diophantine equations with special reference to elliptic curves. Journal of the London Math. Soc. Vol. 41, 193-291 (1966).

[4] CASSELS, J.W.S., and FRÖHLICH, A.: Algebraic Number Theory. Academic Press, London-New York.

[5] CHEVALLEY, C.: Introduction to the theory of algebraic functions of one variable. A.M.S. (1951).

[6] EILENBERG, S., and STEENORD, N.: Foundation of algebraic topology. Princeton, (1952).

[7] FREY, G.: Pseudo algebraically closed fields with nonarchimedean real valuations, Journal of Algebra. Vol. 26, 202-207 (1973).

[8] GILMER, R.W.: Multiplicative ideal theory. Queens University, Kingston (1968).

[9] GILMER, R., and Ohm, J.: Primary ideals and valuation ideals. Trans. Amer. Math. Soc. 7, 237-250 (1965).

[10] JARDEN, M.: Elementary statements over large algebraic fields. Trans. of the A.M.S. Vol. 64, 67-91 (1972).

[11] JARDEN, M.: Roots of unity over large algebraic fields. To be published in. Math. Ann.

[12] KAPLANSKY, I.: Commutative rings. Allyn and Bacon Inc. Boston (1970).

[13] KRULL, W.: Idealtheorie in unendlichen algebraischen Zahlkörpern II, Mathematische Zeitschrift 31 (1930).

[14] LANG, S.: Diophantine Geometry. Interscience Publishers, New York-London (1962).

[15] Lutz, E.: Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps p-adic; J. reine angew. Math., 177, 237-247 (1937).

[16] ZIMMER, H.G.: Ein Analogon des Satzes von Nagell-Lutz über die Torsion einer elliptischen Kurve. To appear in Journal f. reine und angew. Math.

Moshe Jarden
Department of Mathematical Sciences
Tel Aviv University
Tel Aviv, Israel.

(Received September 1, 1973 ; in revised form August 1, 1974)