Repeating our method for all other prime power factors of \(e\) instead of \(u'\), we get our theorem.

When the class number of \(k\) is relatively prime to \(n\), we can delete the condition on \(q\) that it splits into principal \(k\)-primes and state the theorem in the following manner:

**Theorem 2.** Let \((k, Q) = n\) and let the class number of \(k\) be relatively prime to \(n\). Let \(e\) be a positive integer such that

\[
e(n/e) = 1 \quad \text{and} \quad e | (q_{e_p}, e_p, p-1).
\]

Then

\[
e | (p-1)/ord_p q
\]

where \(e = 1\) if \(e\) is odd or \(p = 1 \mod 2e\) and \(e = 2\) otherwise.

**Proof.** Let \(K\) be the Hilbert class field of \(k\) and let \((k; K) = h\). Then \((h, n) = 1\) and \((K; Q) = nh\). Let \(e_r^f\) and \(g_r^f\) denote the ramification index of a \(K\)-prime lying above the rational prime \(l\) and the number of distinct \(K\)-primes lying above \(l\) respectively. Then, we can easily see that

\[
e(n/e) = 1 \quad \text{implies} \quad (e, nh/e) = 1
\]

and

\[
e | (q_{e_p}, e_p, p-1) \quad \text{implies} \quad e | (g_{e_p}^f, e_p, p-1).
\]

Taking \(K\) for \(k\) in Theorem 1, we see that \(e\) satisfies the required conditions and so the theorem follows since every \(k\)-prime splits into principal \(K\)-primes.

Received on 20. 8. 1973  (444)

---

**Arithmetic Euclidean Rings**

by

CLIFFORD QUEEN (Bethlehem, Penn.)

1. **Introduction.** Let \(A\) be an integral domain. We shall say that \(A\) is a **Euclidean ring**, or simply \(A\) is **Euclidean**, if there exists a map \(\varphi: A \setminus \{0\} \to N, N\) the non-negative integers, satisfying the following two properties:

1. If \(a, b \in A \setminus \{0\}\), then \(\varphi(ab) \geq \varphi(a)\);
2. If \(a, b \in A\), \(b \neq 0\), then there exist \(q, r \in A\) such that \(a = bq + r\), where \(r = 0\) or \(\varphi(r) < \varphi(b)\).

It is easy to see that condition 1 is an unnecessary restriction; i.e., if there is a map \(\varphi: A \setminus \{0\} \to N\) satisfying only condition 2), then there is always another map \(\varphi'\), derived from \(\varphi\), such that \(\varphi'\) satisfies both 1) and 2). Further, it is apparently unknown whether one enforces the class of euclidean integral domains by enlarging \(N\) to a well-ordered set of arbitrary cardinality, but this question will not concern us here except to say that whenever \(A\) has finite residue classes; i.e., \(A\) modulo any non-zero ideal is finite, then insisting on \(N\) as a set of values is no restriction. We refer the reader to an excellent paper by P. Samuel [3] in which all of the above and much more is exposed with great clarity.

Let \(A\) be as above. We define subsets \(A_n\) of \(A\) for \(n \in N\) by induction as follows: \(A_0 = \{0\}\) and if \(n \geq 1\), then \(A_n = \bigcup_{m < n} A_m\). Finally \(A_n = \{b \in A\}

there is a representative in \(A_n\) of every residue class of \(A\) modulo \(b\).

Setting \(A' = \bigcup_{n \in N} A_n, A\) is Euclidean if and only if \(A' = A\) (see Motzkin [6]). Further when \(A' = A\) we get a map \(\varphi: A \setminus \{0\} \to N\), where if \(a \in A \setminus \{0\}\) then there exists a unique \(n \geq 0\) such that \(n \in A_{n+1} \setminus A_n\) and \(\varphi(a) = n\). Now not only does \(\varphi\) satisfy conditions 1) and 2) above, but if \(\varphi'\) is any other map satisfying condition 2), then \(\varphi(a) \leq \varphi'(a)\) for all \(a \in A \setminus \{0\}\). Hence Motzkin justifiably calls \(\varphi\) the minimal algorithm for \(A\).

Let \(F\) be a global field, so \(F\) is a finite extension of the rational numbers \(Q\) or \(F\) is a function field of one variable over a finite field. Let \(S\) be a non-empty finite set of prime divisors of \(F\) such that \(S\) contains all infinite (i.e. archimedean) prime divisors. For each finite (i.e. non-archimedean)
prime divisor \( P \), we denote by \( O_P \) the valuation ring associated to \( P \) in \( F \). Letting \( P \) range over all prime divisors of \( F \) we get a ring for each such set \( S \) as follows:

\[
O_S = \bigcap_{P \in S} O_P.
\]

For each such finite set \( S \), \( O_S \) is a Dedekind ring with finite residue classes.

It is known that there always exists a finite set \( S \) such that \( O_S \) is a principal ideal domain, or as we shall say "\( O_S \) is P.I.D."). Further, as we have shown in [7], one can always find finite \( S \) so that \( O_S \) is Euclidean. The question that concerns us here is: If \( S \) is a finite set of prime divisors, as above, and \( O_S \) is P.I.D., is \( O_S \) Euclidean? That the answer to our question is not always yes is well known, but as we shall see, there is excellent reason to believe that the only time the answer is no is in the finite number of examples already known.

In Section 2 we prove an essential lemma using transcendental techniques. In Section 3 we prove the following: If \( F \) is a function field over a finite field and \( S \) a finite non-empty set of prime divisors of \( F \) such that \( O_S \) is P.I.D., then \( O_S \) is Euclidean if \( S \) contains at least two elements. Further we display the evidence, due mostly to P. Weinberger (see [11]), that the above result is also true in the case when \( F \) is a number field.

2. Let \( F \) be a global field and \( S \) a finite non-empty set of prime divisors of \( F \) such that \( S \) contains all infinite primes of \( F \) and has cardinality at least two. Assume further that \( O_S \) is P.I.D. Let \( F_S \) denote the group of \( S \)-units of \( F \) and denote by \( M_S \) the set of finite prime divisors \( P \) of \( F \) such that \( P \nmid S \) and the non-zero residue classes of \( O_P \) modulo its maximal ideal \( \mathfrak{m}_P \) are represented by elements of \( F_S \). We shall say that an integral divisor \( D \) is prime to the elements of \( S \) if for finite \( P \) in \( S \), \( V_P(D) = 0 \), where for any finite prime divisor \( P \) of \( F \), \( V_P \) denotes the additive normalized valuation associated with \( P \). We establish notation as follows: Let \( D \) be an integral divisor of \( F \) prime to the elements of \( S \).

\( E_D \) — denotes the rays of \( F \) modulo \( D \), i.e., the group of principal divisors \( (x) \), where \( \infty = F - \{0\} \) and \( V_P(x - 1) \geq V_P(D) \) for all finite \( P \) such that \( V_P(D) > 0 \);

\( I_D \) — denotes the group of divisors of \( F \) prime to the set of finite prime divisors \( P \) such that \( V_P(D) > 0 \);

\( \mathcal{I}_D \) — denotes the group of divisors generated by finite members of \( S \).

Now let \( D \) be any integral divisor of \( F \) prime to the elements of \( S \) and consider the tower of subgroups \( I(D) \supseteq H_{S}(D) \supseteq R_{P} \), where \( H_{S}(D) = \mathcal{I}_{S} \cdot R_{P} \). Because \( S \neq \emptyset \) and \( H_{S}(D) \) has finite index in \( I(D) \) and thus by class field theory (see [1]) there is a finite abelian extension \( E_{D} \) of \( F \) which is classfield to \( H_{S}(D) \). Let \( C \) range over the classes of \( I(D) \) modulo \( H_{S}(D) \). For each \( C \) we set \( K_{C} \) equal to the set of prime divisors \( P \) such that \( P \nmid S \) and \( P \nmid C \). Our objective in this section is to investigate the sets \( M_{S} \cap K_{C} \).

To that end we record some definitions and results regarding the idea of Dirichlet density (we follow [2] and [3]). Letting \( P \) range over all finite prime divisors of \( F \), we set

\[
\xi(\sigma, F) = \prod_{P} \left(1 - \frac{1}{N(P)^{\sigma}}\right)^{-1},
\]

where \( N(P) \) denotes the absolute norm of \( P \) and \( \sigma > 1 \) is taken on real values. We note that \( \xi(\sigma, F) \) is absolutely convergent for \( \sigma > 1 \) and it is called the real zeta-function of \( F \). If \( M \) is a set of finite prime divisors of \( F \), we define a real valued continuous function (\( \sigma > 1 \))

\[
\omega(\sigma, M) = \left(\sum_{P \in M} \frac{1}{N(P)^{\sigma}}\right) \left(\log \xi(\sigma, F)\right)^{-1}.
\]

Next

\[
\lim_{\sigma \to 1+} \omega(\sigma, M) = \omega(M)
\]

is called the Dirichlet density of \( M \), when the limit exist. Evidently \( M \) is an infinite set if \( \omega(M) > 0 \). Of particular interest to us, for later application, is the following:

**Theorem 1.** If \( F \) is a function field (i.e., a function field of one variable over a finite field), then for any class \( C \) of \( I(D) \) modulo \( H_{S}(D) \)

\[
M_{S} \cap K_{C}
\]

is an infinite set.

**Proof.** Let \( k \) be the exact field of constants of \( F \) and set \( q = |k| \).

If \( F_{S} \) denotes the group of \( S \)-units of \( F \), then because \( |S| \geq 2 \), there exists \( t \in F_{S} \) such that \( t \nmid \mathfrak{m}^{m} \) for any positive integer \( m \), where \( (m, q) = 1 \). We denote by \( T \) the set of prime divisors \( P \in M_{S} \) such that \( t \mid P \) represents the generator of the multiplicative group of the field \( O_{P} / \mathfrak{m}^{m} \), i.e., \( t \) is a primitive root modulo \( P \). Following Bilharz [2], we discuss the existence and positivity of \( \omega(T) \). To that end let \( P \) be a prime divisor of \( F \) such that \( P \nmid S \cup T \).

There exists a rational prime \( p \) such that \( p \nmid q \) and \( N(P) = 1 \mod p \) and \( t^{p} = 1 \mod \mathfrak{m}^{m} \) in \( O_{P} \). If \( m \) is a positive integer, \( (m, q) = 1 \), we
denote by $\mathcal{S}(L_m)$ the set of prime divisors $P$ such that $P \nmid S$ and $P$ splits completely in $L_m = \mathcal{F}(V_1, V_0)$. For convenience we shall also denote by $\mathcal{S}(L)$ the set of prime divisors of $F$ not in $S$. Now if $P$ is a rational prime, $p\nmid q$, then $P \in \mathcal{S}(L_P)$ if and only if $P \nmid S$, $N(P) \equiv 1 \mod p$ and $t^{-1}P \equiv 1 \mod I_P$. Thus letting $p$ range over all rational primes we have

$$T = \bigcap_{p \nmid q} \mathcal{S}(L_p),$$

where $\mathcal{S}(L_p) = \mathcal{S}(L) - \mathcal{S}(L_p)$. We note that $\mathcal{S}(L_m) = \bigcap_{p \nmid m} \mathcal{S}(L_p)$ if $m$ is a square free positive integer. Hence setting $T_m = \bigcap_{p \nmid m} \mathcal{S}(L_p)$, $m \geq 1$, we obtain $T_m$ as an algebraic sum of sets (see [2])

$$T_m = \sum_{m_0 | m} \mu(m) \mathcal{S}(L_{m_0}),$$

where $m_0 = \prod_{p | m} p$. The significance of writing $T_m$ as an algebraic sum of sets is that it gives us $\omega(\sigma, T_m)$ in terms of the $\omega(\sigma, \mathcal{S}(L))$, namely

$$\omega(\sigma, T_m) = \sum_{m_0 | m} \mu(m_0) \omega(\sigma, \mathcal{S}(L_{m_0})).$$

Since $T_{m+1} \subseteq T_m$, $m \geq 1$, we have (for $\sigma > 1$)

$$\omega(\sigma, T_m) \geq \omega(\sigma, T_{m+1}).$$

Further because $T_m - T = \bigcup_{p \nmid q} \mathcal{S}(L_p)$,

$$0 \leq \omega(\sigma, T_m) - \omega(\sigma, T) \leq \sum_{p \nmid q} \omega(\sigma, \mathcal{S}(L_p)).$$

Now for each positive integer $m$, $(m, q) = 1$, we have by Tebhotaray's theorem that

$$\omega(\mathcal{S}(L_m)) = \lim_{n \to \infty} \omega(\sigma, \mathcal{S}(L_m)) = \frac{1}{n(m)},$$

where $n(m) = [L_m : F]$. Next in view of [2]

$$\lim_{n \to \infty} \omega(T_m) = \sum_{m_0 | m} \mu(m_0) \omega(\mathcal{S}(L_{m_0})) = \sum_{m_0 | m} \mu(m_0) \frac{1}{n(m_0)} > 0.$$

We would have that

$$\lim_{n \to \infty} \omega(\sigma, T_m) = \omega(\sigma, T) \quad \text{and} \quad \omega(T) = \sum_{m_0 | m} \frac{\mu(m_0)}{n(m_0)} > 0,$$

in view of (1) and (2), if the following held:

$$\sum_{p \nmid q} \omega(\sigma, \mathcal{S}(L_p)) \text{ is uniformly convergent in any interval}$$

$$1 < \sigma \leq \sigma_0, \sigma_0 > 1.$$

Bihazh shows in [2] that (3) is true modulo the Riemann Hypothesis for function fields over finite fields. According to Weil [10], the Riemann Hypothesis holds for function fields and thus indeed

$$\omega(T) = \sum_{m_0 | m} \mu(m_0) \frac{1}{n(m_0)} > 0.$$

Now let $G$ be any class in $I(D)$ modulo $H_0(D)$. Let $E_D$ be classfield to $H_0(D)$ and for any positive integer $m$, consider $E_D \cap L_m$. Since $D$ is prime to the elements of $S$ and only elements of $S$ can ramify in $L_m$, we have that $E_D \cap L_m$ is an unramified extension of $F$. Since $E_D \cap L_m$ is unramified over $F$ and contained in $E_D$, we have $H_0(D) \cdot R(D) \subseteq H_0$, where $R(D)$ denotes the group of principal divisors of $F$ prime to $D$ and $H_0$ denotes the divisor group in $I(D)$ to which $E_D \cap L_m$ is classified. Since $E_D \subseteq R(D), H_0(D) \cdot R(D) = I_D, R(D) = I(D)$ and because $H_0$ is P.I.D., $I_D = R(D) = I(D)$. Thus $H = I(D), i.e., H_D = I_D$. Now if $H_D$ is the Galois group of $E_D$ over $F$, $H_m$ that of $L_m$ over $F$ and $G$ that of $E_D$ over $F$,

$$G \cong H_m \times H_D.$$

There exists unique $\sigma_0$, $H_D$ such that $(G, E_D/F) = \sigma_0$, where $(G, E_D/F)$ denotes the Artin reciprocity map. Now if $F'$ is a prime of $L_m, E_D$, which does not ramify over $F$ and $F', L_m, E_D/F' = (1, \sigma_0)$, then $F \in \mathcal{S}(I_m) \cap K_C$ if $F' / F$ and $F' \nmid S$. Conversely if $F \in \mathcal{S}(I_m) \cap K_C$ then $F \nmid S, F$ does not ramify in $L_m, E_D$, and there exists a prime divisor $F'$ of $L_m, E_D$, such that $F' / F$ and $F', L_m, E_D/F' = (1, \sigma_0)$. So because $(1, \sigma_0)$ is in the center of $G$, we have by Tejbhotaray's theorem

$$\omega(I_m) \cap K_C = \omega(I_m) \cdot \omega(K_C).$$

Next

$$\omega(T_m \cap K_C) = \sum_{m_0 | m} \mu(m_0) \omega(I_m) \omega(K_C)$$

and

$$\omega(\sigma, T_m \cap K_C) = \sum_{m_0 | m} \mu(m_0) \omega(\sigma, I_m) \omega(K_C).$$

Since

$$T_{m+1} \cap K_C \subseteq T_m \cap K_C \quad \text{and} \quad T_m \cap K_C - T_m \cap K_C \subseteq \bigcup_{p \nmid q} \mathcal{S}(L_p),$$

we have

$$\omega(\sigma, T_m \cap K_C) \geq \omega(T, T_{m+1} \cap K_C),$$

(2')
and

\[(3') \quad 0 \leq \omega(\sigma, T_a \cap K_C) - \omega(\sigma, T \cap K_C) \leq \sum_{g} \omega(\sigma, \varphi(I_g)).\]

Finally \((1')\), \((2')\), \((3')\) and \((3)\) yield

\[\omega(T \cap K_C) = \lim_{n \to \infty} \omega(T_n \cap K_C) = \omega(T \cap K_C),\]

and since \(\omega(K_C) = \frac{1}{d}, \quad d = [E_F: F]\), and \(T \cap K_C \subseteq M_S \cap K_C\), we have

\[\omega(M_S \cap K_C) > 0.\]

Q.E.D.

3. Let \(F\) be a global field and \(S\) a finite non-empty set of prime divisors such that \(S\) contains all infinite primes and \(|S| \geq 2\). Consider the homomorphism \(\theta_S\) from the group \(I\) of all divisors of \(F\) into the rational integers \(Z\), determined on finite prime divisors \(P\) as follows: \(\theta_S(P) = 0\) if \(P \in S\), \(\theta_S(P) = 1\) if \(P \in M_S\) and \(\theta_S(P) = 2\) if \(P \not\in S \cup M_S\). We have an exact sequence

\[0 \to I_S \to I \to \mathbb{Z}.\]

Remark 1. If \(F\) is a function field, then by \([2]\) \(\theta_S\) is surjective. If \(F\) is a number field then there is good reason to believe that \(\theta_S\) is also surjective and we will have more to say about that later.

Definition. We define a homomorphism \(\varphi_S: \mathbb{Z}^* \to \mathbb{Z}\) as follows:

If \(x \in \mathbb{Z}^*\), we denote by \((x)\) the principal divisor of \(I\) associated to \(x\) and set \(\varphi_S(x) = \theta_S((x))\). We have an exact sequence

\[1 \to F_S \to \mathbb{Z}^* \to \mathbb{Z},\]

and further \(\varphi_S\) restricted to \(O_S - \{0\}\) takes on only non-negative values in \(Z\).

Theorem 2. If \(F\) is a function field and \(|S| \geq 2\), then \(O_S\) is P.I.D. if and only if \(O_S\) is Euclidean with respect to \(\varphi_S\).

Proof. Since any euclidean integral domain is P.I.D., we need only show that P.I.D. implies euclidean. To that end assume that \(O_S\) is P.I.D. and denote by \(I(O_S)\) the group of divisors of \(F\) with respect to \(O_S\). We have an exact sequence

\[1 \to I \to I \to I(O_S) \to 1.\]

Now if \(0 \neq b \in O_S\), we set \(D_b = \bigcap_{P \in S} P^{\varphi_S(b)}\). Next \(D_b \cap I(S) = (b) \cap I(S)\).

Further if \(D\) is an integral divisor of \(F\) such that \(D\) is prime to elements of \(S\), then since \(O_S\) is P.I.D. there exists \(0 \neq b \in O_S\) such that \(D = D_b\). Now if \(D\) is an integral divisor of \(F\) prime to the elements of \(S\) and \(d \in O_S - \{0\}\) such that \((d) \cap I(D)\), then \(\varphi_S(D) = \varphi_S(D)\) if and only if \(\varphi_S(D) = \varphi_S(D)\) if and only if \(\varphi_S(D) = \varphi_S(D)\) if and only if \(\varphi_S(D) = \varphi_S(D)\). Thus \(\varphi_S(D) = \varphi_S(D)\) if and only if \(\varphi_S(D) = \varphi_S(D)\) if and only if \(\varphi_S(D) = \varphi_S(D)\). So in particular if \(0 \neq b \in O_S\) such that the non-zero residue classes of \(O_S\) modulo \(\varphi_S\) are representable by elements of \(O_S\) then \(D_b = \mathbb{Z}\) and conversely. Let \(a, b \in O_S - \{0\}\) such that \((a, b) = 1\), then the principal divisor \((a)\) of \(F\) represents a divisor class \(C_a\) of \(I(D_b)\) modulo \(H_S\) of \(D_b\).

By Theorem 1 there exists \(P \in M_S\) such that \(P \in O_S\) hence there exists \(\varphi_S\) such that \(D_b = \varphi_S\) and there exists \(e \in E_F\) such that \(a = a \mod bO_S\).

We set \(A = O_S\) and recall the notation of Section 1, \(A_0, A_1, A_2, ...\) What we have shown above is the following

\[(A) \quad \varphi_S(A_0) - A_1 \text{ if and only if } D_b \not\in M_S.\]

\[(B) \quad \text{If } a, b \in A - \{0\} \text{ such that } (a, b) = 1, \text{ then there exists } \varphi_S \text{ such that } a = a \mod bO_S.\]

Our objective is to show that if \(0 \neq b \in A\) and \(a \neq a \mod bO_S\), then \(a = a \mod bO_S\) or \(a, b) = 1\).

If \(a = a \mod bO_S\), then \(a = a \mod bO_S\), and our result is immediate. So assume \(\varphi_S(b) > 1\). If \(a = a \mod bO_S\) or \(a, b) = 1\), then we have \((B)\) that there exists \(\varphi_S\) such that \(\varphi_S(a) = a \mod bO_S\), where \(\varphi_S(a) = \varphi_S(a)\). Now if \(\varphi_S(b) > 1\), then \(\varphi_S(b) > 1\), and further \(\varphi_S\) restricted to \(O_S - \{0\}\) takes on only non-negative values in \(Z\).

Theorem 3. If \(F\) is a function field and \(|S| \geq 2\) and \(O_S\) is P.I.D. We claim that \(\varphi_S\) is the minimal algorithm on \(O_S\).

Proof. Let \(A = O_S\) and recall the notation of Section 1, \(A_0, A_1, A_2, ...\) Since \(O_S\) is euclidean \(\bigcup_{n=0}^{\infty} A_n = A\) and the minimal algorithm \(\varphi\) is defined on \(A\) as follows: for each \(a \neq 0\), we have \(A_n \subset A_{n+1}\) and if \(0 \neq a \in A\), then there exists unique \(n \neq 0\) such that \(a \in A_{n+1} - A_n\), with \(\varphi(a) = a\). Next if \(0 \neq \varphi(a)\) and \(\varphi(a)\) is a prime ideal, we have two cases, \(D_b \not\in M_S\) or \(D_b \in M_S\). If \(D_b \not\in M_S\), then by \((A)\) of Theorem 2, \(\varphi(A) = A_0\) and since \(\varphi(a) = \varphi(D_b) = 1\), \(\varphi(a) = \varphi(a)\). Next if \(D_b \in M_S\), then by \((B)\) of Theorem 2, \(\varphi(A) = A_0\) and again \(\varphi(a) = \varphi(a)\). Finally suppose \(0 \neq b \in A\) and let \(b = \pi_1 \pi_2 \ldots \pi_n\) be a prime factorization of \(b\). By \([5]\), pp. 201, we have \(\varphi(b) = \varphi(\pi_1) \varphi(\pi_2) \ldots \varphi(\pi_n)\) and since \(\varphi(\pi_i) = \varphi(\pi_i)\) for \(1 \leq i \leq n, \varphi(b) = \varphi(b)\). However since \(\varphi\) is minimal algorithm on \(A\) and
A is euclidean with respect to \( \nu_k \), \( \nu(b) \leq \nu_k(b) \) for all \( b \in A \) such that \( b \neq 0 \).

Q.E.D.

Theorem 3. Let \( F \) be a function field and \( S \) a finite non-empty set of prime divisors of \( F \) such that \( O_S \) is P.I.D. but not euclidean. Let \( k \) denote the exact field of constants of \( F \) and \( g_F \) the genus of \( F \), then \( F \) is isomorphic to one of the following fields: \( k(x, y) \), where \( x \not\equiv k \) and

1. \( |k| = 2, \ g_F = 1 \ and \ y^2 + y = x^3 + x + 1, \ or \)
2. \( |k| = 3, \ g_F = 1 \ and \ y^2 = x^3 + 3x + 2, \ or \)
3. \( |k| = 4, \ g_F = 1 \ and \ y^2 + y = x^4 + \eta, \ where \ \eta \ is \ a \ generator \ of \ the \ multiplicative \ group \ of \ k, \ or \)
4. \( |k| = 2, \ g_F = 2 \ and \ y^2 + y = x^3 + x^2 + 1. \)

Further in each case \( O_S = k(x, y) \).

Proof. In view of Theorem 2, \( |S| = 1 \). Further if \( S = \{P\} \), then by a relation of F. K. Schmidt (see [9]), \( \deg(P)h \mid h \), where \( h \) is the class number of \( F \).

Thus because \( h \not\equiv 1 \), we have \( h = \deg(P) = 1 \). Further \( g_F > 0 \), since otherwise \( O_S \) would be isomorphic to the polynomial ring in one variable over \( k \) which is clearly euclidean.

Thus according to [4], \( F \) must be isomorphic to one of the 4 fields mentioned in the statement of the theorem. Now if \( P_n \) denotes the pole divisor of \( x \) in \( F, \ S = \{P_n\} \), since \( F \) can have only one prime of degree one. Thus the only possibility, in each case, is that \( O_S = k(x, y) \). Now since the \( k(x, y) \) are evidently P.I.D. it remains to show that they are not euclidean. To that end set \( A = k(x, y) \). What we have seen above is that \( A \) has no prime ideal of degree one, but the units of \( A \) are evidently \( k' = k - \{0\} \). Hence \( A_0 = \{0\} \).

\( A_1 = k \), but \( A_2 \neq k \) and thus \( A' = \bigcup_{n=0}^{\infty} A_n \neq A \). Q.E.D.

Remark 2. Now let \( F \) be a number field. The evidence is that Theorem 1 and 2 are true in this case. In fact the arguments in [11] seem to generalize easily and give both theorems modulo the generalized Riemann Hypothesis. Given the truth of Theorem 1 an analogue of Theorem 3 is that the only \( O_S \) which are P.I.D. but not euclidean are the rings of integers in the imaginary quadratic number fields \( Q(\sqrt{-19}) \), \( Q(\sqrt{-43}) \), \( Q(\sqrt{-67}) \) and \( Q(\sqrt{-163}) \).

References


