29. A Characterization of Submodules of the Quotient Field of a Domain

By Tokuo IWAMOTO

(Comm. by Kenjiro SHODA, M. J. A., Feb. 12, 1973)

1. Introduction. Let D be an elementary unique factorization domain with identity and K its quotient field. Let $\boldsymbol{P}$ be the set of the prime elements of D, and we consider the set $\boldsymbol{F}$ of the maps f from $\boldsymbol{P}$ into $\boldsymbol{Z}\cup\{-\infty\}$ (the set of integers and negative infinity), provided that there exists only a finite number of prime elements p such that $f(p)>0$ for each map f of $\boldsymbol{F}$. Let $M(f)$ be the set of the elements $x\in K$ with $V_p(x)\geq f(p)$ for all $p\in\boldsymbol{P}$, where V_p denotes the p-valuation of K. Then we can prove that $M(f)$ is a D-module, which is called an *f-module.* Now in [2], R. A. Beaumont and H. S. Zuckerman have characterized the additive groups of rational numbers. The purpose of this paper is to extend the results in [2] for an elementary unique factorization domain D and to investigate D-submodules of K related with f-modules.

The author is thankful to Professor K. Murata for his valuable advices.

2. Properties of f-modules in an elementary unique factorization domain.

Let D be an elementary unique factorization domain (abv. EUFD) with the quotient field K, and let $\boldsymbol{P}$ be the set of all prime elements. Let a be a non-zero element of D and $a=\Pi_{j=1}^{s}p_j^{n_j}$ (n_j: positive integers) the factorization of a into prime factors. We define the valuation of K in the following way. We consider the map v_p of D into non-negative integers: $v_p(a)=n_j$, $v_p(0)=\infty$ for all p, and extend v_p to K as follows: $V_p(a)=v_p(ac)-v_p(c)$, where $0\neq a\in K$ and $ac\in D$ with $0\neq c\in D$. It is easy to see that the map V_p of K into integers does not depend on the choice of c, and satisfies the above conditions of the p-valuation. If $f(p)=0$, $f\in\boldsymbol{F}$, for all prime elements p, it is easily verified that $M(f)=D$.

Proposition 2.1. *Let D be EUFD with the quotient field K. Then $M(f)\supseteq M(f')$ if and only if $f(p)\leq f'(p)$ for each element p of $\boldsymbol{P}$.*

Proof. "If part" is evident. Suppose that $M(f)\supseteq M(f')$, and assume that $f(p_0)>f'(p_0)$ for some element p_0 of $\boldsymbol{P}$. Let $\boldsymbol{Q}=\{p_{k_1},\cdots,p_{k_r}\}$ be the set of the primes with $f(p_{k_j})>0$ or $f'(p_{k_j})>0$ ($j=1,\cdots,r$). If p_0 is in $\boldsymbol{Q}$, we take out it from the set, and if $f'(p_0)=-\infty$, we set $f'(p_0)=-n$ by taking an integer $n>0$ such that $f(p_0)>-n$. Let a

$=p_0^{f'(p_0)}\Pi_{j=1}^r p_{k_j}^{f_0(p_{k_j})}$, where $f_0(p_{k_j})=\mathrm{Max}\{f(p_{k_j}), f'(p_{k_j})\}$ $(j=1, \cdots, r)$. Put $a=p_0^{f'(p_0)}$, if the set Q is empty. Then $V_p(a)=0\geq f'(p)$ for primes p such that $p\neq p_0$ and $p\neq p_{k_j}$ $(j=y, \cdots, r)$, $V_{p_{k_j}}(a)=f_0(p_{k_j})\geq f'(p_{k_j})$, and $V_{p_0}(a)=f'(p_0)<f(p_0)$. Hence we have $a\notin M(f)$ and $a\in M(f')$, a contradiction.

Corollary. *$M(f)=M(f')$ if and only if $f(p)=f'(p)$ for all primes p.*

Proof. It is immediate from Proposition 2.1.

If EUFD D satisfies the following condition (c), it is denoted by D^*.

(c) Every principal ideal of D is maximal.

Let $a=\Pi_{j=1}^s p_p^{m_j}$ and $b=\Pi_{j=1}^s p_j^{n_j}$ be prime factorizations of a and b, where $\{p_j\}_{j=1}^s$ are all prime factors of a and b with $m_j\neq 0$ or $n_j\neq 0$. The element $\Pi_{j=1}^s p_j^{d_j}$ is called the greatest common divisor of a and b, and it is denoted by (a, b) where $d_j=\mathrm{Min}\{m_j, n_j\}$ $(j=1, \cdots, s)$.

Lemma 1. *Let M be a D^*-module. If $a, a'\in M\cap D^*$, then $(a, a')\in M\cap D^*$.*

Proof. If $a+a'=(a, a')(b+b')$, then $(b, b')=1$. Thus if $b=\Pi_{i=1}^s p_{ki}^{m_i}$ and $b'=\Pi_{j=1}^t p_{k'_j}^{n_j}$ are factorizations of b and b' into prime factors, then $p_{k_i}\neq p_{k'_j}$ for all i, j, and (p_{k_i}) and $(p_{k'_j})$ are prime ideals. Therefore $(p_{k_i})+(p_{k'_j})=(1)$ for all i, j, and thus $(b)+(b')=(1)$. Consequently, there exist d and d' such that $db+d'b'=1$ and $d, d'\in D$. Therefore we have proved that $(a, a')=(a, a')(db+d'b')=da+d'a'\in M\cap D^*$.

If there exist primes p_i with $V_{p_i}(a)>0$ for all elements a of $M\cap D^*$, we collect those primes, and let it be $\{p_1, p_2, \cdots, p_n\}$.

Lemma 2. *The element $E=\Pi_{i=1}^n p_i^{e_i}$ is contained in $M\cap D^*$, where $e_i=\mathrm{Min}\{V_{p_i}(x)\,|\,x\in M\cap D^*\}$.*

Proof. We choose elements $a_1, a_2, \cdots, a_n$ with $V_{p_i}(a_i)=e_i$, $a_i\in M\cap D^*$ $(i=1, 2, \cdots, n)$. Now, let a_0 be any element of $M\cap D^*$, and b_1 be the element such that

$$b_1=(a_0, a_1)=p_1^{e_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}p_{r_1}^{k_1}p_{r_2}^{k_2}\cdots p_{r_s}^{k_s},\ \alpha_i\geq e_i(\alpha_i, k_j\text{: positive integers}).$$

Next, we choose elements $c_1, c_2, \cdots, c_s$ with $V_{p_{r_i}}(c_i)=0$, $c_i\in M\cap D^*$ $(i=1, 2, \cdots, s)$, and we take elements $b_2, b_3, \cdots, b_{s+1}$ as follows:

$$b_2=(b_1, c_1)=p_1^{e_1}p_2^{\alpha'_2}\cdots p_n^{\alpha'_n}p_{r_2}^{k'_2}\cdots p_{r_s}^{k'_s},\ \alpha'_i\geq e_i,\ k_j\geq k'_j\geq 0,$$
$$b_3=(b_2, c_2)=p_1^{e_1}p_2^{\alpha''_2}\cdots p_n^{\alpha''_n}p_{r_3}^{k''_3}\cdots p_{r_s}^{k''_s},\ \alpha''_i\geq e_i,\ k'_j\geq k''_j\geq 0,$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$b_{s+1}=(b_s, c_s)=p_1^{e_1}p_2^{\alpha_2^{(s)}}\cdots p_n^{\alpha_n^{(s)}},\ \alpha_i^{(s)}\geq e_i.$$

Moreover we take the following elements:

$$h_2=(a_2, b_{s+1})=p_1^{e_1}p_2^{e_2}p_3^{\beta_3}\cdots p_n^{\beta_n},\ \beta_i\geq e_i,$$
$$h_3=(a_3, h_2)=p_1^{e_1}p_2^{e_2}p_3^{e_3}p_4^{\beta'_4}\cdots p_n^{\beta'_n},\ \beta'_i\geq e_i,$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$h_n=(a_n, h_{n-1})=p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots p_n^{e_n}.$$

Then $h_n=E$ and hence $E\in M\cap D^*$ by Lemma 1.

In the case of $\mathrm{Min}\{V_p(x)\,|\,x\in M\cap D^*\}=0$ for all primes p, E is a unit of D^*. There exists an element E^{-1} in D^* and M is a D^*-module, so $1 \in M \cap D^*$. Hence we may assume without loss of generality that $E=1$. Any element of $M \cap D^*$ can be represented as aE, where $a \in D^*$. Moreover we can show that any element of M is in the form qE, where $q \in K$ and $V_{p_i}(q) \geq 0$ $(i=1,2,\cdots,n)$. For, if $x \in M$, then there exists an element a of D^* such that $ax \in M \cap D^*$ and $(ax, a)=1$, and there exists an element a' of D^* such that $ax=a'E$. Let $a^{-1}a'=q$, then $V_{p_i}(q) \geq 0$ for all i, and $x=qE$. We assume in the proof of the remaining properties that the elements of M are written in the form qE, where $q \in K$ and $V_{p_i}(q) \geq 0$ $(i=1,2,\cdots,n)$.

Lemma 3. *Let M be a D^*-module. If $qE \in M$, $aq \in D^*$ and $(aq, a)=1$, then $a^{-1}E \in M$.*

Proof. Take elements d and d' of D^* such that $daq+d'a=1$. Then we have $a^{-1}E=a^{-1}E(daq+d'a)=dqE+d'E \in M$.

Lemma 4. *Let M be a D^*-module. If $qE \in M$, $q'E \in M$ and $(aq, a)=(bq'; b)=(a, b)=1$, then $a^{-1}b^{-1}E \in M$, where a, b, aq and bq' are elements of D^*.*

Proof. By Lemma 3, $a^{-1}E$ and $b^{-1}E$ are contained in M. Since there exist elements d and d' such that $da+d'b=1$, we have

$$a^{-1}b^{-1}E=a^{-1}b^{-1}E(da+d'b)=db^{-1}E+d'a^{-1}E \in M.$$

Proposition 2.2. *If M is any D^*-module, then M is represented as $M=M(f)$ for some $f \in \boldsymbol{F}$.*

Proof. Put $V_p(M)=-\infty$, if there exists an element q of M such that $V_p(q)=-n$ for any positive integer n: and if not, put $V_p(M)=\mathrm{Min}\{V_p(q) \mid q \in M\}$. Now, we define $f(p)=V_p(M)$. Then it is evident that $M \subseteq M(f)$. Conversely let x be any element of $M(f)$. Then it can be written in the form $x=qE$ $(q \in K)$. Let $\{p_{r_1}, p_{r_2}, \cdots, p_{r_s}\}$ be the set of the prime elements such that $V_{p_{r_i}}(q)=n_i$ (n_i: negative integers). If $V_p(q) \geq 0$ for all primes p, then $q \in D^*$ and $x \in M$ since $E \in M$. So we can assume the existence of such elements. By the definition of $f(p_{r_i})=V_{p_{r_i}}(M)$, there exists an element $a_i p_{r_i}^{n_i} E$ of M for each i. Here we may assume that $a_i \in D^*$ and $V_{p_{r_i}}(a_i)=0$ for each i. By Lemma 3, $p_{r_i}^{n_i}E \in M$ for each i, and then $\Pi_{i=1}^{s} p_{r_i}^{n_i} E \in M$ by Lemma 4. Consequently, $x=qE \in M$.

Theorem 1. *There is one to one correspondence between the set of D^*-modules and $\boldsymbol{F}$.*

Proof. It is straightfoward by Propositions 2.1 and 2.2.

Let $E=\Pi_{i=1}^{n} p_i^{f(p_i)}$ be a finite product of all prime elements such that $f(p_i)>0$ in an f-module $M(f)$ of EUFD D. Then any element of $M(f)$ is written in the form $qE(q \in K, V_{p_i}(q) \geq 0)$. But if $f(p) \leq 0$ for all primes p, then we can take as $E=1$.

Theorem 2. *Let D be EUFD. If $M(f)$ and $M(f')$ are D-modules, then the following conditions are equivalent.*

(1) *$M(f)$ is isomorphic to $M(f')$.*

(2) *$f(p)=f'(p)$ for almost all p, and whenever $f(p)\neq f'(p)$, both are not $-\infty$. Every isomorphism between $M(f)$ and $M(f')$ is given by $qE\leftrightarrow gqE'$, where $E=\Pi_{i=1}^{r}p_i^{f(p_i)}$, $f(p_i)>0$, $E'=\Pi_{j=1}^{s}p_j^{f'(p_j)}$, $f'(p_j)>0$, and $V_p(g)=f'(p)-f(p)-V_p(E')+V_p(E)$ for all primes p with $f(p)\neq-\infty$ and $f'(p)\neq-\infty$.*

Proof. The proof is similar to the one of Corollary 3 in [2].

Proposition 2.3. *Let D be EUFD, and let $M(f)$ and $M(f')$ be f-modules of D. Then the set $M=\{mm'\mid m\in M(f), m'\in M(f')\}$ is a D-module.*

Proof. Let $f_0(p)=f(p)+f'(p)$ for $p\in \boldsymbol{P}$. Then it is evident that $M\subseteq M(f_0)$. Now let x be any element of $M(f_0)$ and $x=\Pi_{i=1}^{s}p_i^{n_i}$ the factorization of x into prime factors. Since $n_i\geq f_0(p_i)=f(p_i)+f'(p_i)$ for all p_i, we have $p_i^{n_i}=p_i^{m_i}p_i^{f(p_i)}p_i^{f'(p_i)}$ for all p_i (m_i: non-negative integers). We write $a=\Pi_{i=1}^{s}p_i^{m_i}$. Then $x=(a\Pi_{i=1}^{s}p_i^{f(p_i)})\Pi_{i=1}^{s}p_i^{f'(p_i)}$. Since $a\in D$ and $a\Pi_{i=1}^{s}p_i^{f(p_i)}\in M(f)$, we have $x\in M$.

3. Subrings with the form $M(f)$.

Proposition 3.1. *Let D be EUFD with the quotient field K. $M(f)$ is a subring of K containing D if and only if $f(p)=0$ or $f(p)=-\infty$ for all prime elements p.*

Proof. Let $f(p)=0$ or $f(p)=-\infty$ for all p. Then $V_p(ab)=V_p(a)+V_p(b)\geq f(p)+f(p)=f(p)$ for $a,b\in M(f)$. Hence $ab\in M(f)$. Conversely we assume that D is EUFD and $M(f)$ is a subring of K such that $M(f)\supseteq D$. It is obvious that $f(p)\leq 0$ for all p. If $f(p_0)\neq-\infty$ and $f(p_0)<0$ for some p_0, then $a=p_0^{f(p_0)}\in M(f)$ since $f(p)\leq 0$ for all p. Then $a^2=p_0^{2f(p_0)}\in M(f)$ since $M(f)$ is a ring. On the other hand, $V_{p_0}(a^2)=2f(p_0)<f(p_0)$ since $f(p_0)<0$. It contradicts the containment $a^2\in M(f)$.

Lemma 5. *Let D be EUFD and let $M(f)$ and $M(f')$ be subrings of K, each of which contains D. If we define $f_0(p)=\mathrm{Min}\{f(p),f'(p)\}$ for all p, then $M(f_0)$ is a subring which contains both $M(f)$ and $M(f')$, and $M(f_0)$ is unique minimal in such subrings.*

Proof. It is clear that $M(f)\subseteq M(f_0)$ and $M(f')\subseteq M(f_0)$. If $M(f_1)$ contains $M(f)$ and $M(f')$, then $f(p)\geq f_1(p)$ and $f'(p)\geq f_1(p)$ for all p by Proposition 2.1. Hence $f_0(p)\geq f_1(p)$. We have therefore $M(f_0)\subseteq M(f_1)$.

The ring $M(f_0)$ considered in Lemma 5 is denoted by $M(f)\cup M(f')$.

Lemma 6. *Let $D, M(f)$ and $M(f')$ be as above. If we define $f_0(p)=\mathrm{Max}\{f(p),f'(p)\}$, then $M(f_0)=M(f)\cap M(f')$.*

Proof. It is evident that $M(f_0)\subseteq M(f)$ and $M(f_0)\subseteq M(f')$ since $f_0(p)\geq f(p)$ and $f_0(p)\geq f'(p)$. Then $M(f_0)\subseteq M(f)\cap M(f')$. Conversely, let x be an arbitrary element of $M(f)\cap M(f')$. Then $V_p(x)\geq f(p)$ and $V_p(x)\geq f'(p)$. Hence we have $V_p(x)\geq \mathrm{Max}\{f(p),f'(p)\}=f_0(p)$.

Lemmas 5 and 6 imply that the set of rings of the form $M(f)$ which contains EUFD D forms a lattice. Moreover we set $f_D(p)=0$ and $f_K(p)=-\infty$ for all p. Then subrings of K contains D form a complemented lattice under inclusion, which has $K=M(f_K)$ as its greatest element and $D=M(f_D)$ as its least element, where the complement of $M(f)$ is $M(\underline{f})$ and $\underline{f}$ is defined in the following way: $f(p)=0\Rightarrow\underline{f}(p)=-\infty$, $f(p)=-\infty\Rightarrow\underline{f}(p)=0$.

Next we define a vector $X(f)=(\cdots f(p_\lambda)\cdots)$ ($p_\lambda\in\boldsymbol{P}$) and $\boldsymbol{W}$ denotes the set $\{X(f)\,|\,f\in\boldsymbol{F}'\}$, where $\boldsymbol{F}'$ is the subset of $\boldsymbol{F}$ such that $f(p)=0$ or $f(p)=-\infty$ for all p. Let us define the order $X(f)\geq X(f')$ in the following way: $f(p_\lambda)\leq f'(p_\lambda)$ for all $p\Longleftrightarrow X(f)\geq X(f')$. Then $\boldsymbol{W}$ forms a Boolean lattice under the above ordering.

Theorem 3.[1] *Let D be EUFD with the quotient field K. Then the set of subrings of K, each of which contains D and has of the form $M(f)$ forms a Boolean lattice under inclusion.*

Proof. $\{M(f)\}$ is lattice-isomorphic to $\boldsymbol{W}$ under the correspondence: $M(f)\leftrightarrow X(f)$.

Corollary. *Let K be the quotient field of D^*. Then the set of subrings of K which contains D^* as its least element forms an atomic Boolean lattice.*

Proof. It is verified by Proposition 2.2 and Theorem 3.

References

[1] K. Asano and K. Murata: Arithmetical ideal theory in semigroups. Journ. of Polytec., Osaka City Univ., **4**, 1–33 (1953).

[2] R. A. Beaumont and H. S. Zuckerman: A characterization of the additive rationals. Pacific J. Math., **1**, 169–177 (1951).

[3] K. Murata: On Dedekindean l-semigroups and its lattice-ideals. Proc. Japan Acad., **47**, 132–134 (1971).

1) cf: Theorem 5.11 in [1] and [3].