PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 35, Number 2, October 1972

GAUSS' LEMMA

HWA TSANG TANG

ABSTRACT. Let $f(x)$ be a polynomial in several indeterminates with coefficients in an integral domain R with quotient field K. We prove that the principal ideal generated by f in the polynomial ring $R[x]$ is prime iff f is irreducible over K and $A^{-1}=R$ where A is the content of f. We also prove that if $f(x)$ is such that $A^{-1}=R$ and $g(x)$ is a primitive polynomial in the sense that only a unit of R can divide each coefficient of g, then fg will be primitive.

1. **Introduction.** Let $R[x]=R[x_1, x_2, \cdots, x_n]$ be a polynomial ring in n indeterminates with coefficients in an integral domain R, and $f(x) \in R[x]$. We give a necessary and sufficient condition for f to generate a principal prime ideal in $R[x]$.

THEOREM A. *$(f)R[x]$ is prime iff f is irreducible over K and $A^{-1}=R$, where K is the quotient field of R and A is the R-ideal generated by the coefficients of f and $A^{-1}=R:_K A$.*

We define f to be *super-primitive* if $A^{-1}=R$.

THEOREM D. *(Over any integral domain) the product of a super-primitive polynomial with a primitive polynomial is primitive.*

We also show that super-primitive implies primitive (Theorem C) and that these two notions coincide over an integral domain in which every pair of elements has a "greatest common divisor", i.e., a common divisor which is a multiple of any other common divisor (Theorem H). Henceforth we will call such a ring a GCD domain. For instance any valuation domain is a GCD domain, whereas $J[\sqrt{(-5)}]$ is not.

Thus we have genealized two related classical results:

(1) Gauss' Lemma: Over a unique factorization domain, the product of primitive polynomials is primitive. Kaplansky [**1**, Example 8, p. 42] showed that the same is true over a GCD domain.

(2) If R is a unique factorization domain, so is $R[x]$; and $f(x) \in R[x]$ is prime iff f is irreducible over K and f is primitive.

Received by the editors September 7, 1971 and, in revised form, February 10, 1972.

AMS 1970 *subject classifications*. Primary 13B25, 13A15; Secondary 13B20, 13F15.

Key words and phrases. Gauss' Lemma, integral domain, content of polynomial, principal prime ideal, primitive polynomial, greatest common divisor, unique factorization domain, integrally closed domain.

The results here are contained in the author's doctoral dissertation. The author expresses her gratitude to Professor Irving Kaplansky for his help and encouragement.

2. **Principal prime ideals in** $R[x]$. Throughout this paper R is an (arbitrary) integral domain with K as its quotient field. If $f(x) \in R[x] = R[x_1, \cdots, x_n]$, we define $c(f)$ = the *content* of f = the R-ideal generated by the coefficients of f.

Now let $f(x)$ be a nonzero, nonconstant polynomial in $R[x]$, with $c(f) = A$. Let $H=(f)R[x]$, $W=(f)K[x]\cap R[x]$, and $J=A^{-1}H$. Clearly $H\subset J\subset W$ are ideals of $R[x]$. When is H or J prime? First we state (omitting the proof, which is routine) an easy technical result.

PROPOSITION. *Let X be an ideal in $R[x]$ such that $H\subset X\subset W$. Then X is prime iff f is irreducible over K and $X=W$.*

We now study the conditions for H or J to coincide with W. We introduce the additional notations to be used throughout the paper. Let $S=\{1/r : r\in R, r\neq 0\}$. Clearly $R\cap S$ is the set of units of R.

If $g(x)\in R[x]$, let $B=c(g)$, and $C=c(fg)$. Clearly $C\subset AB$.

LEMMA 1. *$W=H$ iff $J=H$ iff $A^{-1}=R$ iff $B^{-1}\cap S=C^{-1}\cap S$ for every $g(x)$.*

LEMMA 2. *$W=J$ iff $(AB)^{-1}\cap S=C^{-1}\cap S$ for every $g(x)$.*

PROOF. $W=\{f(x)\cdot g(x)/t : g(x)\in R[x], \quad t\in R, \quad t\neq 0\}\cap R[x]$; $J=\{f(x)\cdot \sum k_jx^j : \text{each } k_j\in A^{-1}\}$; $H=\{f(x)\cdot g(x) : g(x)\in R[x]\}$.

(i) $W=H$ iff $fg/t\in R[x]\Rightarrow g/t\in R[x]$ iff $1/t\in C^{-1}\Rightarrow 1/t\in B^{-1}$ iff $C^{-1}\cap S\subset B^{-1}\cap S$ for every $g(x)$.

(ii) $J=H$ iff $A^{-1}=R$.

(iii) Now suppose $A^{-1}=R$ and $C\subset (t)$. Claim $B\subset (t)$. Otherwise, we pass to the ring $R[x]/(t)R[x]\approx R/(t)[x]$. Using $'$ to denote homomorphic images, we have $f'g'=0$ and $g'\neq 0$. By a theorem of McCoy [**2**, Theorem 4, p. 34] there is $r'\neq 0$ in $R/(t)$ such that $r'f'=0$. Hence in R, $r\notin (t)$ and $rA\subset (t)$. In other words $r/t\notin R$ and $(r/t)A\subset R$, hence $r/t\in A^{-1}=R$, a contradiction.

(iv) $W=J$ iff $fg/t\in R[x]\Rightarrow g/t=\sum k_jx^j$ where each $k_j\in A^{-1}$ iff $1/t\in C^{-1}\Rightarrow B/t\subset A^{-1}$, i.e., $(B/t)A\subset R$, or $1/t\in (AB)^{-1}$ iff $C^{-1}\cap S\subset (AB)^{-1}\cap S$.

THEOREM A. *$(f)R[x]$ is a prime ideal in $R[x]$ iff f is irreducible over K and $A^{-1}=R$ where $A=c(f)$.*

REMARK. Compare with [**1**, Examples 1–5, p. 102].

THEOREM B. *If R is integrally closed, then the ideal $A^{-1}(f)R[x]$ coincides with $(f)K[x]\cap R[x]$, and is prime iff f is irreducible over K.*

PROOF. Since R is integrally closed, $(AB)^{-1}=C^{-1}$ for every $g(x)$ [**1**, Example 6(e), p. 52]. We now apply Lemma 2.

3. **Primitive and super-primitive polynomials.** One consequence of Lemma 1 is: If $A^{-1}=R$ and $B^{-1}\cap S=R\cap S$ then $C^{-1}\cap S=R\cap S$ also.

The classical definition $g(x)$ is *primitive* iff only the units of R divide each coefficient of g translates easily to: iff $B^{-1}\cap S=R\cap S$ where $B=c(g)$.

DEFINITION. $f(x)$ is *super-primitive* iff $A^{-1}=R$ where $A=c(f)$.

THEOREM C. *Super-primitive implies primitive.*

THEOREM D. *The product of a super-primitive polynomial with a primitive polynomial is primitive.*

We give another characterization of super-primitive.

THEOREM E. *Let T be the set of prime ideals of R which are minimal primes over ideals of the form $(a):_R b=\{x\in R: xb\in Ra\}$. Then:*

(i) $R=\bigcap\{R_P: P\in T\}$.

(ii) *A finitely generated ideal I is contained in some $P\in T$ iff $I^{-1}\neq R$.*

PROOF. (i) Let $b/a\in\bigcap\{R_P:P\in T\}$. Let $J=(a):_R b$. We show $J=R$. Otherwise $J\subset$ some $P\in T$. For the P, let $b/a=r/s$, $s\notin P$. Then $sb=ra$, so $s\in J\subset P$, a contradiction.

(ii) First suppose $I\subset$ some P, minimal prime over $J=(a):_R b$. Localizing at P, P_P is the only prime ideal over J_P, so $I_P\subset P_P=\sqrt{J_P}$. Let $I=(c_1, c_2, \cdots, c_k)$. For each i, $(c_i/1)^{n_i}=j_i/s_i$ for $j_i\in J$, $s_i\notin P$. If $n=\sum n_i$ and $s=\prod s_i$, we have $sI^n\subset J$, $s\notin P$. Since $J\subset P$, $s\notin J$. For any integer $m\geqq 1$, we have $sI^m\subset J=(a):_R b$ iff $(sb/a)I^m\subset R$ iff $(sb/a)I^{m-1}\subset I^{-1}$. Let k be the least integer such that $sI^k\subset J$. Then $(sb/a)I^{k-1}\subset I^{-1}$ and $(sb/a)I^{k-1}\not\subset R$, whence $I^{-1}\neq R$.

Conversely, suppose $I\not\subset$ any $P\in T$. Let $b/a\in I^{-1}$ and let $P\in T$. Since $I\not\subset P$, there is $s\in I$, $s\notin P$. Since $b/a\in I^{-1}$, $(b/a)s=r\in R$. Hence, $b/a=r/s\in R_P$. Since this is true for every $P\in T$, $b/a\in R$ by (i).

In this context, a super-primitive polynomial f is one such that $c(f)$ is not contained in any $P\in T$.

THEOREM F. *The product of super-primitive polynomials is super-primitive.*

PROOF. Let f, g be super-primitive and assume $c(fg)\subset P\in T$. Localizing at P, we get $c(fg)_P=c(f_P\cdot g_P)$. Since $c(f_P)=c(g_P)=R_P$, it follows from [**1**, Example 9, p. 8 or Example 6(c), p. 52] that $c(fg)_P=R_P$, a contradiction.

THEOREM G. *Let $a_i\in R$. If $(a_1, \cdots, a_n)^{-1}=R$ then $(a_1^{k_1}, \cdots, a_n^{k_n})^{-1}=R$ for any set of integers $k_i\geqq 0$.*

PROOF. Immediate from Theorem E (ii).

We give a sufficient condition for the existence of certain GCD's (for any integral domain).

LEMMA 3. *Let* $a_1, \cdots, a_n \in R$, *and* A *be the ideal they generate. Let* $d \in R$. *Then the following are equivalent*:

(i) $A^{-1}=R/d$.

(ii) *For every* $b \in R$, $\gcd(ba_i)=bd$.

(iii) *For every* $k \in A^{-1}$, $\gcd(ka_i)=kd$.

PROOF. The cyclic verification (i)$\Rightarrow$(iii)$\Rightarrow$(ii)$\Rightarrow$(i) is routine.

When R is a GCD domain, the special case $d=1$ yields

THEOREM H. *Over a GCD domain, super-primitive is the same as primitive.*

4. **The polynomial ring in one variable.** Let R be an integral domain, and $R[y]$ be the polynomial ring in one indeterminate y. We give some characterizations for R to be a GCD domain in terms of conditions on $R[y]$.

THEOREM I. *The following are equivalent*:

I. *R is a GCD domain.*

II. *Every linear polynomial in $R[y]$ is the product of an element in R with a super-primitive polynomial.*

III. (i) *Every linear polynomial in $R[y]$ is the product of an element in R with a primitive polynomial.*

(ii) *In $R[y]$ the product of two linear primitive polynomials is primitive.*

IV. *For every nonzero prime ideal P in $R[y]$ such that $P \cap R=0$, P is principal.*

V. *For nonzero elements a, b in R, the ideal $(a+by)K[y] \cap R[y]$ in $R[y]$ is principal.*

PROOF. I is equivalent to II, by Lemma 4. Clearly I implies III. We now assume III and prove II. Given $a+by$ in $R[y]$, by III(i), $a+by=r(u+vy)$, $r \in R$, $u+vy$ primitive. Claim $(u, v)^{-1}=R$. For, let $k=c/d \in (u, v)^{-1}$, c, $d \in R$. By III(i) we can assume $c+dy$ primitive. By III(ii), $(c+dy)(u+vy)=cu+(cv+du)y+dvy^2$ is primitive. Since $k \in (u, v)^{-1}$, d divides cu and dv. Thus d divides each of cu, $dv+du$ and dv. Hence d is a unit and $k \in R$.

I$\Rightarrow$IV. Select $f(y)$ primitive and of the lowest degree in P. It follows that f is irreducible and $(f)R[y]$ is prime. Thus $P=(f)R[y]$, both contracting to 0 in R.

Clearly IV$\Rightarrow$V.

V$\Rightarrow$II. Given $a+by$ in $R[y]$, by V, $(a+by)K[y]\cap R[y]=(f)R[y]$ for some $f(y)$ in $R[y]$. $a+by=fg$, $g\in R[y]$; and $f=(a+by)k$, $k\in K[y]$. Combining, $f=fgk$, $gk=1$, hence $g\in R$. Hence we have $a+by=r(u+vy)$, with r, u, v in R. But then $(u, v)^{-1}=R$ by Theorem A.

COROLLARY. *R is a unique factorization domain iff R satisfies the ascending chain condition on principal ideals and in $R[y]$ the product of two linear primitive polynomials is primitive.*

REFERENCES

1. I. Kaplansky, *Commutative rings*, Allyn and Bacon, Boston, Mass., 1970. MR **40** #7234.

2. N. H. McCoy, *Rings and ideals*, Carus Monograph Series, no. 8, Open Court, LaSalle, Ill., 1948. MR **10**, 96.

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY AT HAYWARD, HAYWARD, CALIFORNIA 94542