ON INTEGRAL CLOSURE

HUBERT BUTTS, MARSHALL HALL JR. AND H. B. MANN

1. Introduction. Let J be an integral domain (i.e., a commutative ring without divisors of zero) with unit element, F its quotient field and $J[x]$ the integral domain of polynomials with coefficients from J. The domain J is called integrally closed if every root of a monic polynomial over J which is in F also is in J. If J has unique factorization into primes, a well-known lemma of Gauss asserts: "If $p(x)$ is a polynomial in $J[x]$ factoring over F, then $p(x)$ factors over J." For proof see **(2**, p. 73**)**. We shall show that if J is integrally closed but unique factorization is not assumed in J and if $p(x) = ax^m + \ldots + a_m$ is in $J[x]$ and $p(x) = g(x)\,h(x)$ in $F[x]$, then $ap(x)$ factors in $J[x]$. The case $a = 1$, which asserts that the Gauss lemma holds for monic polynomials, is important in many applications.

We show further a hereditary property of integral closure, namely, that $J[x]$ is integrally closed if J is integrally closed. These two theorems permit us to generalize a theorem on the relation between the Galois group of a monic polynomial over J and the Galois group of the corresponding polynomial mod p where p is a prime ideal of J.

2. Theorems on integral domains. An element β algebraic over F is called an algebraic integer if β satisfies a monic equation (not necessarily irreducible) with coefficients in J. A well-known theorem on symmetric polynomials then shows that the algebraic integers form a ring J^* and that this ring is integrally closed. Moreover if J is integrally closed and if an algebraic integer β lies in F, then it must lie in J. From our definition, it follows that the conjugates over F of an algebraic integer are also integral, and so the monic irreducible equation over F of an integer has its coefficients in J.

THEOREM 1. *Let J be an integrally closed integral domain with unit element, F its quotient field. Let $f(x) \in J[x]$ and $f(x) = g(x)\,h(x)$ where $g(x), h(x) \in F[x]$. Let $f(x), g(x), h(x)$ have first coefficients a, b, c respectively. Then*

$$\frac{a}{b}\,g(x), \quad \frac{a}{c}\,h(x)$$

have integral coefficients. Hence

$$af(x) = \left(\frac{a}{b}\,g(x)\right)\left(\frac{a}{c}\,h(x)\right)$$

is a decomposition of $af(x)$ in $J[x]$.

Received November 5, 1953.

https://doi.org/10.4153/CJM-1954-049-3 Published online by Cambridge University Press

Proof. Let ρ be a root of $f(x)$. An argument completely analogous to that given in (**1**, p. 91) for the case that J is the domain of algebraic integers in the usual sense shows that

$$\frac{f(x)}{x-\rho}$$

has integral coefficients. Applying this to all the roots ρ of $h(x)$, we deduce that

$$\frac{cf(x)}{h(x)} = cg(x) = \frac{a}{b}g(x)$$

has integral coefficients. For $a = 1$ we have:

COROLLARY. *If J is integrally closed and the monic polynomial $f(x) \in J[x]$ factors in $F[x]$, then it also factors in $J[x]$.*

For the applications of Theorem 1 and its Corollary, it will be necessary to show that the property of algebraic closure carries over to the polynomial domain $J[x]$.

THEOREM 2. *If J is integrally closed, then $J[x]$ is integrally closed.*

Let $f(x)/g(x)$ be a root of a monic polynomial with coefficients in $J[x]$. Since unique factorization holds in $F[x]$, it follows that $F[x]$ is integrally closed. Hence $g(x)$ must be an element of F and we can choose it in J. Let now $f(x)/\alpha$, $f(x) \in J[x]$, $\alpha \in J$ satisfy a monic equation with coefficients in $J[x]$. Since the domain of integers over J is integrally closed, $f(\beta)/\alpha$ must be integral for all integers β. Let

$$f(x) = A_0x^m + \dots,$$

then

$$\frac{f(x) - f(\beta)}{\alpha} = \frac{(x-\beta)f_1(x)}{\alpha}$$

is integral valued for all integral values of x. Moreover the first coefficient of $f_1(x)$ is A_0. Suppose now that we have constructed a polynomial:

$$\phi_s(x) = \frac{(x-\rho_1)\dots(x-\rho_s)f_s(x)}{\alpha},$$

where the ρ_i are integers such that $\phi_s(x)$ is integral, whenever x is integral and such that the first coefficient of $f_s(x)$ is A_0. Let ρ_{s+1} be a root of the equation

$$(x-\rho_1)\dots(x-\rho_s) = 1.$$

Then ρ_{s+1} is an integer and $\phi_s(\rho_{s+1}) = f_s(\rho_{s+1})/\alpha$. Hence

$$\frac{(x-\rho_1)\dots(x-\rho_s)f_s(x)}{\alpha} - \frac{(x-\rho_1)\dots(x-\rho_s)f(\rho_{s+1})}{\alpha}$$
$$= \frac{(x-\rho_1)\dots(x-\rho_{s+1})f_{s+1}(x)}{\alpha}$$

https://doi.org/10.4153/CJM-1954-049-3 Published online by Cambridge University Press

is integral whenever x is integral and $f_{s+1}(x)$ has again A_0 as first coefficient. Continuing in this manner, we arrive at a polynomial

$$\frac{A_0\,(x - \rho_1) \ldots (x - \rho_m)}{\alpha}$$

which is integral whenever x is an integer. Let β be a root of the equation,

$$(x - \rho_1) \ldots (x - \rho_m) = 1.$$

Then β is an integer and it follows that A_0 is divisible by α. We may therefore write:

$$\frac{F(x)}{\alpha} = bx^m + \frac{g(x)}{\alpha}, \qquad b \in J,\ g(x) \in J[x],$$

where $g(x)$ is a polynomial of degree at most $m - 1$. Substituting in the equation for $F(x)/\alpha$, we see that $g(x)/\alpha$ is also root of a monic polymonial with coefficients in $J[x]$. Theorem 2 now follows by induction.

COROLLARY. *If J is integrally closed, then $J[x_1, \ldots, x_n]$ is integrally closed.*

3. Application to Galois theory. The corollary can be used to generalize a theorem that has been known to hold for unique factorization domains (**2**, p. 190) as well as for algebraic number fields (**3**, p. 122, eq. 10.6).

THEOREM 3. *Let J be an integrally closed integral domain, p a prime ideal in J. Let $\bar{J}$ be the residue ring of J (mod p) and $f(x)$ a monic polynomial in $J(x)$, $\bar{f}(x)$ the corresponding polynomial in $\bar{J}(x)$. Let Δ, $\bar{\Delta}$, be the quotient fields of J and $\bar{J}$ respectively. If $f(x)$ and $\bar{f}(x)$ do not have any double roots, then the roots of $f(x)$ and $\bar{f}(x)$ can be so numbered that the Galois group of $\bar{f}(x)$ is a subgroup of the Galois group of $f(x)$.*

A study of the proof of this theorem in (**2**, p. 190), readily shows that the assumption of unique factorization in J made there is used only to establish the factorization of a monic polynomial over the ring $J[u_1, \ldots, u_n]$ from its factorization in the quotient field of $J[u_1, \ldots, u_n]$. It can therefore be replaced by Theorem 1 coupled with the Corollary to Theorem 2. The proof itself is word by word the same as in (**2**).

REFERENCES

1. Erich Hecke, *Vorlesungen ueber die Theorie der algebraischen Zahlen* (New York, 1948).
2. B. L. van der Waerden, *Modern Algebra*, Vol. 1 (New York, 1949).
3. Herman Weyl, *Algebraic Theory of Numbers* (Princeton, 1940).

Louisiana State University *Ohio State University*

https://doi.org/10.4153/CJM-1954-049-3 Published online by Cambridge University Press