JOUR. FAC. SCI., SHINSHU UNIV. Vol. 2, No. 2, pp. 117—122, Dec. 1967

On Zeros of Polynomials and Galois Extensions of Simple Rings

By KAZUO KISHIMOTO

Department of Mathematics, Faculty of Science
Shinshu University
(Received Sept. 30, 1967)

Introduction. In [4], the author introduced the notion of the polynomial simple ring extensions* and studied some properties of polynomial Galois extensions.

In the present paper, we shall investigate the relationship between the zeros of polynomials and Galois extensions of simple rings. As a generalization of the commutative case, some type of a finite dimensional polynomial simple Galois extension can be considered as a simple ring in which every w-irreducible polynomial over a basic simple ring possessing a zero in the Galois extension can be factored into a product of its linear factors and conversely.

Let S be a simple ring, and let ρ be an automorphism in S, D a ρ-derivation in S. Then the followings are well known.

(1) $S[X;\rho,D]=\{\sum_i X^i s_i\,;\, s_i\in S\}$, the free right S-module with an S-basis $\{X^i\}$, can be regarded as a polynomial ring with an indeterminate X by the multiplication rule $sX = X(s\rho) + sD$ for each $s\in S$.

(2) Each two-sided ideal of $S[X;\rho,D]$ is generated by a (uniquely determined) monic polynomial, and hence, if T is a two-sided ideal, then $T = f(X)S[X;\rho,D]$ for some monic $f(X)$ which is called the generator of T.

A polynomial $f(X)$ is called *non-vanishing* (resp. *vanishing*) if $(f(X))$, the two-sided ideal generated by $f(X)$, is a proper ideal of $S[X;\rho,D]$ (resp. coincides with $S[X;\rho,D]$).

A non-vanishing polynomial $f(X)$ is called *w-irreducible* if each proper left factor $h(X)$ of it (i, e. $f(X)=h(X)g(X)$ and $deg\ h(X)<deg\ f(X)$) is vanishing.

(3) The generator of a two-sided ideal M is w-irreducible if and only if M is maximal.

(4) Every proper two-sided ideal ($\neq 0$) has a unique factorization as a product of maximal ideals. **

(5) Every non-vanishing polynomial has an essentially unique factorization as

* Cf. [1]
** Cf. [2], p. 38.

a product of w-irreducible polynomials and a vanishing polynomial in the sense of the factorization determined within a vanishing polynomial.

Let M be a maximal ideal of $S[X;\rho,D]$ whose generator is $f(X)=X^n+\sum_{i=0}^{n-1}X^is_i$. Then

(6) $R=S[y]=S\oplus yS\oplus y^2S\oplus y^3S\oplus\cdots\cdots\oplus y^{n-1}S\cong S[X;\rho,D]/M$, where y is the residue class of X modulo M, is called *an n-dimensional polynomial simple ring extension* over S.

$S[X;\rho]$, $S[X;D]$ mean the cases $D=0$, $\rho=1$ respectively, and finally, $S[X]$ means the case $D=0$ and $\rho=1$.

For the other notations and terminologies used in this paper, we refer to [4].

§ 1. w-irreducibility and zeros of polynomials

Lemma 1.1 *Let $X-s$ be a polynomial in $S[X;\rho,D]$. Then the followings are equivalent.*

(a) *$X-s$ is non-vanishing.*

(b) *$X-s$ is w-irreducible.*

(c) *$s(s\rho)=s^2$ and D is an inner ρ-derivation generated by s.*

In particular, if $D=0$,

(c′) *s is regular and $\rho=\tilde{s}^{-1}$ provided $s\neq 0$.*

Proof. (a)→(b). If we note that the generator of each ideal is a monic polynomial of the lowest degree which is contained in the ideal, the implication is clear.

(b)→(c)→(a). The first implication is a direct consequence of the fact that $X(X-s)\in(X-s)S[X;\rho,D]$ and $t(X-s)\in(X-s)S[X;\rho,D]$ for each $t\in S$. Next, the conditions (c) shows that $X(X-s)=(X-s)(X-(s-s\rho))$ and $t(X-s)=(X-s)(t\rho)$ for each $t\in S$. Hence, $X-s$ is non-vanishing. Now, let $D=0$. Then (c) yields that $ts=s(t\rho)$ for each $t\in S$. Hence $S=SsS=sS$ shows that the regularlity of s and $\rho=\tilde{s}^{-1}$.

Corollary 1.1 *Let $X-s$ be w-irreducible in $S[X;\rho,D]$.*

(a) *If $X-t$ is w-irreducible for some $t\neq s$, then $t-s$ is regular.*

(b) *If $D=0$, then $X-t$ is w-irreducible if and only if $t=sz$ for some $z\in Z=V_S(S)$.*

(c) *If $\rho=1$, then $X-t$ is w-irreducible if and only if $t=s+z$ for some $z\in Z$.*

Proof. (a) We have $ut-t(u\rho)=uD$, $us-s(u\rho)=uD$ for each $u\in S$ by Lemma 1.1. Hence $u(t-s)=(t-s)(u\rho)$ shows that the regularlity of $t-s$.

(b) Let $X-t$ be w-irreducible. If $t=0$, then $t=s\cdot 0$. On the other hand, if $t\neq 0$, $\rho=\tilde{t}^{-1}$ implies $s=tz$ for some $z\in Z$. The converse is clear.

(c) We can prove the assertion in the same way as in the proof of (a).

Let $f(X)=\sum_{i=0}^{n}X^is_i$ be a polynomial of $S[X;\rho,D]$. Then an element t in S

is called a *zero* of $f(X)$ if $f(t)=\sum_{i=0}^{n}t^is_i=0$.

Lemma 1.2 *Let $f(X)$ be a polynomial of $S[X;\rho,D]$. If $s_1,\cdots\cdots,s_k$ are distinct zeros of $f(X)$ in S such that $X-s_i$ is w-irreducible then $f(X)=\Pi_{i=1}^{k}(X-s_{\pi(i)})h_\pi(X)$ where π is an arbitrary permutation of k-letters and $h_\pi(X)\in S[X;\rho,D]$.*

Proof. Dividing $f(X)$ by $X-s_{\pi(1)}$, we have $f(X)=(X-s_{\pi(1)})h_1(X)+t_1$ for some $t_1\in S$. Then w-irreducibility of $X-s_{\pi(1)}$ yields at once $0=f(s_{\pi(1)})=t_1$ in $S[X;\rho,D]/(X-s_{\pi(1)})\cong S$. Therefore we have $f(X)=(X-s_{\pi(1)})h_1(X)$. Next, let $h_1(X)=(X-s_{\pi(2)})h_2(X)+t_2$ for some $t_2\in S$. Then $f(X)=(X-s_{\pi(1)})(X-s_{\pi(2)})h_2(X)+(X-s_{\pi(1)})t_2$. Hence $0=f(s_{\pi(2)})=(s_{\pi(2)}-s_{\pi(1)})t_2$ in $S[X;\rho,D]/(X-s_{\pi(2)})\cong S$. Since $s_{\pi(2)}-s_{\pi(1)}$ is regular by Corollary 1.1 (a), $t_2=0$. Repeating the same procedure, we have $f(X)=\Pi_{i=1}^{k}(X-s_{\pi(i)})h_\pi(X)$.

§ 2. Zeros of polynomials and Galois extensions

Throughout the present section, we assume that $R=S[y]=S\oplus yS\oplus y^2S\oplus\cdots\cdots\oplus y^{n-1}S$ $(n>1)$ be an n-dimensional polynomial simple ring extension over S defined by $S[X;\rho]/(f(X))$ (resp. $S([X;D]/f(X))$, where $f(X)=X^n+\sum_{i=0}^{n-1}X^is_i$ and y is the residue class of X modulo $(f(X))$. Then, $R[X;P]$ with $P=\tilde{y}^{-1}$ can be considered as a polynomial ring containing $S[X;\rho]$ (resp. $R[X;E]$ with $E=I_y$ can be considered as a polynomial ring containing $S[X;D]$). Thus, if we consider $f(X)$ in $R[X;P]$ (resp. $R[X;E]$), y is a zero of $f(X)$ and $X-y$ is w-irreducible in $R[X;P]$ (resp. $R[X;E]$). We call a zero x in R of $h(X)\in S[X;\rho]$ (resp. $R[X;D]$) a *root* in R of $h(X)$ if $X-x$ is w-irreducible in $R[X;P]$ (resp. $R[X;E]$).

Let σ be an S-automorphism of R. Then $y\sigma=yv_\sigma$ if $sy=y(s\rho)$ and $y\sigma=y+v_\sigma$ if $sy=ys+sD$ for some $v_\sigma\in V=V_R(S)$ [4. p. 175].

Theorem 2.1 *Let $R=S[y]\cong S[X;\rho]/(f(X))$.*

(a) *If R is a weakly Galois extension over S with respect to $\mathfrak{G}$ with $y\sigma=yc_\sigma$, $c_\sigma(\neq 1)\in C=V_R(R)$ for each $\sigma\in\mathfrak{G}$, then every w-irreducible polynomial of $S[X;\rho]$ possessing a root x in R has an essentially unique factorization into a product of w-irreducible linear factors in $R[X;P]$. Furthermore, if this is the case, the order of $\mathfrak{G}$ is n.*

(b) *If $f(X)$ has a factorization into $(X-y)(X-yc_1)\cdots\cdots(X-yc_{n-1})$ in $R[X;P]$ such that $c_i\neq c_j$ if $i\neq j$, $c_i(\neq 1)\in C$, then R is weakly Galois over S.*

Proof. Let x be a root in R of a w-irreducible polynomial $h(X)$ of $S[X;\rho]$. Then $h(X)=(X-x)g(X)$ in $R[X;P]$. We set $x=\sum_{k=0}^{n-1}y^ku_k$ $(u_k\in S)$. Then $x\sigma P=\sum_{k=0}^{n-1}(yc_\sigma)^ku_k)P=\sum_{k=0}^{n-1}y^kc^k_\sigma(u_k\rho)=xP\sigma=x\sigma$ since $xP=x$ for each $\sigma\in\mathfrak{G}$ and $s(x\sigma)=(sx)\sigma=(x(s\rho))\sigma=x\sigma\cdot s\rho$. Consequently, $x\sigma$ is a root in R of $h(X)$. Thus $h(X)=\Pi_{\sigma\in\mathfrak{H}}(X-x\sigma)k(X)$ where $\mathfrak{H}=x\,|\,\mathfrak{G}$. Noting here $x\sigma P=x\sigma$ and $x\sigma(X-x\tau)=(X-$

$x\tau)x\sigma$, we have $x\sigma \cdot x\tau = x\tau \cdot x\sigma$ for each $\sigma, \tau \in \mathfrak{G}$. Hence $\Pi_{\sigma\in\mathfrak{H}}(X - x\sigma) \in S[X; \rho]$ and is non-vanishing. Now, let $f(X) = \Pi_{\sigma\in\mathfrak{H}}(X - x\sigma)\, g(X) + r(X)$ where $g(X)$, $r(X) \in S[X; \rho]$ and $deg\ r(X) < deg\ \Pi_{\sigma\in\mathfrak{H}}(X - x\sigma)$. Then $\Pi_{\sigma\in\mathfrak{H}}(X - x\sigma)\,(g(X) - k(X)) = r(X)$ and $deg\ \Pi_{\sigma\in\mathfrak{H}}(X - x\sigma)\,(g(X) - k(X)) \geqq deg\ \Pi_{\sigma\in\mathfrak{H}}(X - x\sigma)$ if $g(X) - k(X) \neq 0$. Hence $k(X) = g(X) \in S[X; \rho]$. Therefore, w-irreducibility of $h(X)$ yields $k(X) \in S$. By making use of this fact, we find $f(X) = \Pi_{\sigma\in\mathfrak{G}}(X - y\sigma)$, and hence, the order of $\mathfrak{G}$ have to coincide with n by Lemma 1.2.

(b) Let $f(X) = (X - y)(X - yc_1)\cdots\cdots(X - yc_{n-1})$ in $R[X; P]$. Then the map σ_i defined by $\sum_{k=0}^{n-1}(y^k u_k)\sigma_i = \sum_{k=0}^{n-1} y^k c_i{}^k u_k$ is an S-automorphism of R. For, since yc_i is a root of $f(X)$, σ_i is well defined, and $(sy)\sigma_i = y(s\rho)\sigma_i = yc_i(s\rho) = s\sigma_i y\sigma_i$. Hence σ_i is a ring monomorphism. If $(\sum_{k=0}^{n-1} y^k u_k)\sigma_i = \sum_{k=0}^{n-1} y^k c_i{}^k u_k = 0$, $\sum_{k=0}^{n-1} y^k u_k$ is contained in the kernel of σ_i. Thus $\{(yc_i)^k;\ k = 0, 1, \cdots\cdots n-1\}$ is an S-basis. Consequently, σ_i is an S-automorphism.

Let $\mathfrak{G}$ be the group generated by $\{1, \sigma_1, \cdots\cdots \sigma_{n-1}\}$. If $x = \sum_{k=0}^{n-1} y^k u_k$ is an arbitrary element of $J(\mathfrak{G}, R)$, then $\sum_{k=1}^{n-1} y^k(\sum_{j=0}^{k-1} c_i{}^j)u_k = 0$ for each $i = 1, 2, \cdots\cdots n-1$. This means that

$$(y^{n-1}u_{n-1}, y^{n-2}u_{n-2}\cdots\cdots yu_1)\begin{pmatrix} \sum_{j=0}^{n-2} c_1{}^j & \sum_{j=0}^{n-2} c_2{}^j & \cdots\cdots & \sum_{j=0}^{n-2} c^j{}_{n-1} \\ \sum_{j=0}^{n-3} c_1{}^j & \sum_{j=0}^{n-3} c_3{}^j & \cdots\cdots & \sum_{j=0}^{n-3} c^j{}_{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & 1 & & 1 \end{pmatrix} = 0$$

On the other hand,

$$det\begin{pmatrix} \sum_{j=0}^{n-2} c_1{}^j & \sum_{j=0}^{n-2} c_2{}^j & \cdots\cdots & \sum_{j=0}^{n-2} c^j{}_{n-1} \\ \sum_{j=0}^{n-3} c_1{}^j & \sum_{j=0}^{n-3} c_3{}^j & \cdots\cdots & \sum_{j=0}^{n-3} c^j{}_{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & 1 & & 1 \end{pmatrix} \neq 0$$

shows that $u_{n-1} = u_{n-2} = u_{n-3} = \cdots\cdots = u_1 = 0$, that is $J(\mathfrak{G}, R) = S$.

Corollary 2.1 *Let S be a simple ring with the infinite center Z, and let $R = S[y] \cong S[X; \rho]/(f(X))$.*

(a) *If R/S is Galois and $y\sigma \in yC$ for each $\sigma \in \mathfrak{G}(R/S)$ where $\mathfrak{G}(R/S)$ the S-automorphism group of R, then R/S is outer.*

(b) *If R is a division ring, then R/S is an outer Galois extension if and only if each zero in R of $f(X)$ is a root of $f(X)$. Moreover, if this is the case, every w-irreducible polynomial $h(X)$ of degree m of $S[X; \rho]$ possessing a root x in R has*

an essentially unique factorization into $(X-x)(X-xc_1)\cdots\cdots(X-xc_{m-1})s$ $(s\in S)$ *such that* $c_i\neq c_j$ *if* $i\neq j$ *and* c_i $(\neq 1)\in C$.

Proof. (a) The order of $\mathfrak{G}(R/S)$ is n by Theorem 2.1 (a). Hence the order of $\tilde{V}=[V^*:C^*]\leqq n$. Now if we note that V is a simple ring possessing infinitely many elements, $V=C$ by a generalized Scott's Theorem [5. Lemma 1].

(b) The number of distinct zeros $\{x_\alpha\}$ in R of $f(X)$ such that $x_\alpha P=x_\alpha$ is either infinite or at most n [3. Theorem 6]. Hence if each zero in R of $f(X)$ is a root of $f(X)$, we have $f(X)=\Pi_{\sigma\in\mathfrak{G}(R/S)}(X-y\sigma)$. Thus the assertion is an immediate consequence of (a). The converse is clear.

Theorem 2.2 *Let* $R=S[y]\cong S[X;D]/(f(X))$.

(a) *If* R *is a weakly Galois extension over* S *with respect to* $\mathfrak{G}$ *with* $y\sigma=y+c_\sigma$, $c_\sigma(\neq 0)\in C$, *for each* $\sigma\in\mathfrak{G}$, *then every* w*-irreducible polynomial of* $S[X;D]$ *possessing a root in* R *has a non-zero constant term and an essentially unique factorization into a product of* w*-irreducible linear factors in* $R[X;E]$. *Furthermore, if this is the case, the order of* $\mathfrak{G}$ *is* n.

(b) *Let* $\chi(S)\geqq n$ *or* $\chi(S)=0$ *and* $V\neq Z$. *Then* R/S *is an outer Galois extension if and only if* w*-irreducible polynomial* $h(X)$ *of degree* m *of* $S[X;D]$ *possessing a root* x *in* R *has an essentially unique factorization* $(X-x)\cdot(X-(x+c_1))\cdots\cdots(X-(x+c_{m-1}))$ s $(s\in S)$ *such that* $c_i\neq c_j$ if $i\neq j$, c_i $(\neq 0)\in C$.

Proof. (a) The proof is quite similar to that of Theorem 2.1 (a).

(b) If $\chi(S)\geqq n$ or $\chi(S)=0$ and $V\neq Z$, then $V=C$ by [4. Theorem 2.2]. Thus there exists an element $t\in S$ such that $y-t\in C$ and $\{(y-t)^k;\ k=0,1,\cdots\cdots n-1\}$is an S-basis for R. If $(y-t)^n+(y-t)^{n-1}u_{n-1}+\cdots\cdots+u_0=0$ $(u_k\in S)$, then $g(X)=(X-t)^n+\sum_{k=0}^{n-1}(X-t)^ku_k=X^n+\sum_{k=0}^{n-1}X^kw_k$ $(w_k\in S)$ is w-irreducible in $S[X;D]$ and it possesses a root y in R. Hence $g(X)=(X-y)(X-(y+c_1))\cdots\cdots(X-(y+c_{n-1}))$ in $R[X;E]$. Then the map σ_i defined by $\sum_{k=0}^{n-1}(y^ka_k)\ \sigma_i=\sum_{k=0}^{n-1}(y+c_i)^k\ a_k$ $(a_k\in S)$ is an S-auotomorphism of R. Hence $(y-t)\sigma_i=(y-t)d_i$ for some $d_i\in C$ since $y-t$ is contained in C. Hence we can see that $J(\mathfrak{G},R)=S$ by similar methods to that of Theorem 2.1 (b) if $\mathfrak{G}$ is the group generated by $\{1,\sigma_1,\cdots\cdots\sigma_{n-1}\}$. Therefore $R=S[C]$ is an outer Galois extension over S. Conversely, if R/S is outer Galois, $y\sigma=y+c_\sigma$, $c_\sigma\in C$ for each $\sigma\in\mathfrak{G}(R/S)$. Hence the assertion is clear from (a).

References

[1] COHN, P. M. : On a class of binomial extensions, Illinois J. of Math., Vol. 10 (1966), 418–424.

[2] JACOBSON, N. : *The Theory of Rings*, Providence, 1943.

[3] GORDON, B. and T. S. MOTZKIN : On the zeros of polynomials over division rings, Trans. of A. M. S., Vol. 116 (1965), 218–226.

[4] KISHIMOTO, K. : On polynomial extensions of simple rings, J. of Fac. Sci. Hokkaido Univ. Ser. I., Vol. 19 (1966), 169–180.

[5] TOMINAGA, H. : A note on conjugates II, Math. J. of Okayama Univ., Vol. 9 (1959), 1–3.