PUSAN KYŎNGNAM MATHEMATICAL JOURNAL
Vol. 1, 43~46, 1985

FACTORIZATION OF POLYNOMIALS OVER A DIVISION RING

TAE HOON HYUN AND JAE KEOL PARK

Factorization of polynomials over a division ring will be considered in this short note. In fact, L.H. Rowen[3] refined Wedderburn's method [4] of splitting polynomials. Here we improve again Rowen's result on factorization of polynomials.

We start with following well known

LEMMA 1. Let D be a division rings with the center F. Then for every two-sided ideal I of $D[x]$ there is a monic polynomial $f(x)$ in $F[x]$ such that $I=f(x)D[x]$. Moreover, I is a prime ideal if and only if $f(x)$ is irreducible in $F[x]$.

PROOF. Since $D[x]$ is a principal (left and right) ideal domain, there is a monic polynomial $f(x)$ such that $I = f(x)D[x]$ of least degree. Now for d in $D, r(x) =df(x) -f(x)d$ is in I and the degree of $r(x)$ is less than that of $f(x)$. Hence $r(x)=0$ and so $f(x)$ is in $F[x]$. Straightfowardly, it can be verified that $I=f(x)D[x]$ is prime if and only if $f(x)$ is irreducible in $F[x]$.

LEMMA 2. [2, Theorem 3, p. 179] Let D be a division ring with the center F and let K be a finite algebraic extension field of F. Then there are a division ring A and two positive integers h, m such that

(a) $D \otimes_F K=\mathrm{Mat}_h (A)$.

(b) $K\subset\mathrm{Mat}_m(D)$ as an F-algebra and m is such the smallest positive integer.

(c) $hm = \dim_F K$.

Furthermore, A is the centralizer of K in $\mathrm{Mat}_m(D)$.

Following [1] a right ideal $g(x)D[x]$ is *bounded* if it contains a non-zero two-sided ideal. The sum of all non-zero two-sided ideals contained in $g(x)D[x]$ is thus a two-sided ideal and is called *the bound* of $g(x)D[x]$. We say two polynomials $g_1(x)$ and $g_2(x)$ in $D[x]$ are *right similar* if $D[x]/g_1(x)D[x]$ and $D[x]/g_2(x)D[x]$ are $D[x]$-isomorphic. In this case $g_1(x)D[x]$ and $g_2(x)D[x]$ have the same bound if one of them is bounded. Moreover, $g_1(x)$ and $g_2(x)$ are also left similar. So we just say $g_1(x)$ and $g_2(x)$ are *similar* when they are right similar.

THEOREM 3. Let D be a division ring with the center F and let $p(x)$ be an irreducible monic polynomial in $F[x]$. If $p(u)=0$ for some algebraic element u over F, then for any irreducible decomposition $p(x)=g_1(x)g_2(x)\cdots g_n(x)$ of $p(x)$ in $D[x]$ we have

(a) Every $g_i(x)$ is similar to $g_1(x)$,

(b) $\deg g_1(x)$ (hence all $\deg g_i(x)$) is the smallest positive integer m such that $F[u] \subset \mathrm{Mat}_m(D)$ as an F-algebra,

(c) $D[x]/p(x)D[x]$ is $D[x]$-isomorphic to
$\oplus\sum D[x]/g_i(x)D[x]$
and

(d) $p(x)$ is the minimal polynomial of u.

PROOF. We note that $D[x]/p(x)D[x] = D\otimes_F F[u]$ is simple Artinian. By Lemma 2, there are a division ring A and two positive integers h, m such that $\deg p(x) = hm$, $D[x]/p(x)D[x] = \mathrm{Mat}_h(A)$, and m is the smallest positive integer so that $F[x]/(p(x))$ is F-embedded in $\mathrm{Mat}_m(D)$. Actually there is a minimal right ideal V of the simple Artinian ring $D[x]/p(x)D[x]$ with $\dim_D V=m$ and $F[x]/(p(x))$ is F-embedded in $\mathrm{End}_D(V)$.

Let $V=D[x]/\beta(x)D[x]$ with $p(x)=\alpha(x)\beta(x)$in $D[x]$. Then since V is a minimal right ideal, $\beta(x)D[x]$ is a minimal right ideal of $D[x]$ and so $\beta(x)$ is irreducible in $D[x]$. Now for an irreducible decomposition $p(x)=\beta(x)\beta_2(x)\cdots\beta_k(x)$ in $D[x]$, it can be verified that $\beta(x)D[x]$ and $\beta_i(x)$ have $p(x)D[x]$ as the bound. (see [2], p. 39) So $\beta(x)$ and each $\beta_i(x)$ are similar. In particular, deg $\beta(x)=$deg $\beta_i(x)$ for $i=2,\ldots, k$. Moreover, since deg $\beta(x)=m$ and deg $p(x)=mk$, we have $h=k$.

Now consider the given irreducible decomposition $p(x)=g_1(x)\ldots g_n(x)$ in the assumption. Then obviously $n=k$ and each $g_i(x)D[x]$ has the bound $p(x)D[x]$. So each $g_i(x)$ is similar to $\beta(x)$. Of course deg $g_i(x)=m$ is the smallest positive integer such that $F[x]/(p(x))$ is F-embedded in $\mathrm{Mat}_m(D)$. So we prove (a) and (b).

For (c), recall that the bound of each $g_i(x)D[x]$ is $p(x)D[x]$. Since $p(x)$ is irreducible in $F[x]$, $D[x]/p(x)D[x]$ is $D[x]$-isomorphic to $\oplus\sum D[x]/g_i(x)D[x]$ by [1, Theorem 20, p. 45].

Finally for (d), let I be the ideal of polynomial $f(x)$ in $D[x]$ such that $f(u)=0$. Then $p(x)$ is in I and so I is a non-zero two-sided ideal of $D[x]$. Hence by Lemma 1 there exists a monic polynomial $f_0(x)$ in $F[x]$ such that $I=f_0(x)D[x]$. But since $p(x)$ is irreducible in $F[x]$, we have $p(x)=f_0(x)$ and so $I=p(x)D[x]$. Hence $p(x)$ is the minimal polynomial of u and the proof is completed.

Observing Theorem 3 that every irreducible factor $g(x)$ of $p(x)$ has the same degree m which is the least positive integer such that $F[u]\subset \mathrm{Mat}_m(D)$ as F- algebras, we get following immediately.

COROLLARY 4. [3, Theorem 1.5] Let D be a division ring with the center F and let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(d)=0$ for some element d in D, then $p(x)$ splits into linear factors in $D[x]$ and $p(x)$ is the minimal polynomial of d.

PROOF. In this case since $F[u]\subset D$, we have $m=1$. Hence each $g_i(x)$ is linear in any irreducible decompostion of $p(x)$.

COROLLARY 5. Let D be a division ring with the center F and let $p(x)$ be an irreducible monic polynomial in $F[x]$. If deg $p(x)$ is prime, then either $p(x)$ is irreducible in $D[x]$ or $p(x)$ splits into linear factors in $D[x]$.

References

1. N. Jacobson, The Theory of Rings, Amer. Math. Soc. Survey 2, 1943.
2. N. Jacobson, The Structure of Rings, Amer. Math. Soc. Colloq. Publ. 37, 1964.
3. L. H. Rowen, Central simple algebras, Israel J. Math. 29(1978), 285-301.
4. J. H. Wedderburn, On division algebras, Trans. Amer. Math. Soc. 22(1921), 129-135.

Pusan National Univeresity