TENSOR PRODUCTS OF POLYNOMIALS

S.P. Glasby

School of Mathematics and Statistics
University of Sydney
N.S.W. 2006, Australia

1 June 1994

Abstract. This paper defines a binary operation $\otimes$ on the set $R[X]^*$ of nonzero polynomials over the integral domain R. The set of polynomials with nonzero constant term is a commutative monoid under $\otimes$ endowed with a natural involution. Let f and g be polynomials over F, the field of fractions of R. We give formulae expressing $f \otimes g$ as a product of irreducible polynomials over F – a problem which we show is similar to writing the tensor product of simple extensions of F as a direct sum of fields. Finally, we consider questions of unique $\otimes$-factorization.

1. Introduction

Given two algebras A and B over a field F, the most obvious way to construct an F-algebra of dimension $\dim_F A \dim_F B$ is to form the tensor product $A \otimes_F B$. If f and g are two polynomials over an integral domain, there are two natural ways to compute a polynomial of degree $\deg f \deg g$. The first involves composing polynomials, while the second it a little known operation which we call the tensor product of polynomials. We start by giving a definition of this binary operation and develop some of its basic properties including finding a connection between tensor product and composition of polynomials. Furthermore, if α, β are elements of an algebraic extension of a field F, we relate the $\otimes$-product $F(\alpha) \otimes_F F(\beta)$ to the factorization of the $\otimes$-product $m_{\alpha/F} \otimes m_{\beta/F}$ of minimum polynomials. Indeed, $F(\alpha) \otimes_F F(\beta)$ can be shown to be the direct sum of compositums of $F(\alpha)$ and $F(\beta)$, and to each summand there corresponds a factor of $m_{\alpha/F} \otimes m_{\beta/F}$ which is a power of an irreducible polynomial. Finally, we consider $\otimes$-factorizations and argue that we should only consider $\otimes$-factorizations of *irreducible* polynomials, and analogously $\otimes$-factorizations of simple algebraic extensions of F. We show that there are unique $\otimes$-factorization theorems (for irreducible polynomials) over some fields, but not for others. This may be seen as an attempt to find a generalized Krull-Schmidt theorem which holds for $\otimes$-products.

1991 *Mathematics Subject Classification.* 12E05, 11T06.

2. Definition of $\otimes$-product

Let R be an integral domain with field of fractions F. A good example to keep in mind is $R = \mathbb{Z}[X_1, \dots, X_n]$ and $F = \mathbb{Q}(X_1, \dots, X_n)$. Let $R[X]^* = R[X]\backslash\{0\}$ denote the set of nonzero polynomials. Given $f(X) = f_m X^m + \cdots + f_1 X + f_0$ and $g(X) = g_n X^n + \cdots + g_1 X + g_0$ in $R[X]^*$ with $f_m \neq 0$ and $g_n \neq 0$, let M denote the splitting field of fg and let $\alpha_1, \dots, \alpha_m$ be the roots of f, and $\beta_1, \dots, \beta_n$ the roots of g in M.

Definition. Let $f, g \in R[X]^*$ be as above. Define $f \otimes g \in M[X]$ to be the following polynomial of degree mn

$$(f \otimes g)(X) = f_m^n g_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (X - \alpha_i \beta_j).$$

Note that if $g(X) = g_0 \neq 0$, then $f \otimes g = g_0^m$. Furthermore, if $f_0 \neq 0$, then

$$(f \otimes g)(X) = f_m^n \prod_{i=1}^{m} \alpha_i^n g(X/\alpha_i) = (-1)^{mn} f_0^n \prod_{i=1}^{m} g(X/\alpha_i).$$

The definition of the tensor product of polynomials (for the case of monic polynomials over a field) occurred in [**1**] where the term "composed product" and the notation $\circ$ were used. We prefer to use the notation $\otimes$ given the connection with the tensor product of fields and matrices mentioned later. The following theorem shows $f \otimes g \in R[X]^*$.

Theorem 1. *Let Y and G be the $n \times n$ matrices*

$$Y = \begin{pmatrix} X & 0 & \cdots & 0 \\ 0 & X & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & g_n X \end{pmatrix} \quad \text{and} \quad G = \begin{pmatrix} 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \\ -g_0 & -g_1 & \cdots & -g_{n-1} \end{pmatrix}.$$

Then

$$(f \otimes g)(X) = \det \begin{pmatrix} Y & -G & 0 & \cdots & 0 \\ 0 & Y & -G & & 0 \\ & & & \ddots & \\ f_0 G & f_1 G & f_2 G & \cdots & f_{m-1} G + f_m Y \end{pmatrix}$$

Hence $f \otimes g \in R[X]$.

Proof. Let

$$C(h) = \begin{pmatrix} 0 & 1 & & 0 \\ \vdots & & \ddots & 0 \\ 0 & 0 & & 1 \\ -h_0 & -h_1 & \cdots & -h_{n-1} \end{pmatrix}$$

denote the companion matrix of the monic polynomial $h(X) = X^n + h_{n-1}X^{n-1} + \cdots + h_0$ and let $\widehat{f}$ and $\widehat{g}$ denote the monic polynomials $f_m^{-1}f$ and $g_n^{-1}g$.

Recall that $C(\widehat{f}) \otimes C(\widehat{g})$ is the $mn \times mn$ matrix which may be identified, using a certain choice of basis, with the $n \times n$ block matrix

$$C(\widehat{f}) \otimes C(\widehat{g}) = (C(\widehat{f})[C(\widehat{g})]_{ij})$$

where $[C(\widehat{g})]_{ij}$ denotes the (i,j)th entry of $C(\widehat{g})$. By considering Jordan canonical forms, one may show that the eigenvalues of $C(\widehat{f}) \otimes C(\widehat{g})$ are $\alpha_i\beta_j, 1 \le i \le m, 1 \le j \le n$. Therefore

$$\prod_{i,j}(X - \alpha_i\beta_j) = \det(XI - C(\widehat{f}) \otimes C(\widehat{g})).$$

Multiplying this equation by $f_m^n g_n^m$ shows

$$(f \otimes g)(X) \;=\; f_m^n g_n^m \begin{vmatrix} XI & -\widehat{G} & 0 & \cdots & 0 \\ 0 & XI & -\widehat{G} & & 0 \\ & & & \ddots & \\ f_0 f_m^{-1}\widehat{G} & f_1 f_m^{-1}\widehat{G} & f_2 f_m^{-1}\widehat{G} & \cdots & f_{m-1}f_m^{-1}\widehat{G} + XI \end{vmatrix}$$

where $\widehat{G} = C(\widehat{g})$. The factor f_m^n may be absorbed into the determinant by multiplying the last n rows by f_m. Similarly, the factor g_n^m may be absorbed by multiplying rows $n, 2m, \ldots, mn$ by g_n. This changes XI and $\widehat{G}$ to Y and G respectively, and completes the proof. $\square$

3. Basic Properties of $\otimes$-product

The following theorem shows, amongst other things, that $R[X]^*$ with the operation $\otimes$, is a commutative monoid. Let S denote the submonoid of $R[X]^*$ comprising polynomials with nonzero constant term, then there are two natural self-inverse maps $f \mapsto f^r$ and $f \mapsto \overline{f}$ on S (actually $f \mapsto f^r$ preserves $\otimes$-multiplication). Define the reverse polynomial f^r of f to be

$$f^r(X) = (-X)^m f(X^{-1}) = (-1)^m(f_0X^m + f_1X^{m-1} + \cdots + f_m).$$

and define $\overline{f}$ to be $\overline{f}(X) = (-1)^m f(-X)$.

Theorem 2. *Let $f, g, h \in R[X]^*$. Then*
(a) $f \otimes g = g \otimes f$
(b) $(f \otimes g) \otimes h = f \otimes (g \otimes h)$
(c) $f \otimes (gh) = (f \otimes g)(f \otimes h)$
(d) $f \otimes X^n = f_m^n X^{mn}$
(e) $f \otimes (X - \beta) = f_m X^m + f_{m-1}\beta X^{m-1} + \cdots + f_0\beta^m = (-X)^m f^r(X^{-1}\beta)$

(f) $f \otimes (X-1) = f$
(g) $(X+1) \otimes (X+1) = X-1$
(h) $\overline{f} = f \otimes (X+1)$, $\overline{\overline{f}} = f$ *and* $\overline{f} \otimes \overline{g} = f \otimes g$
(i) $(f^r)^r = f$ *and* $f^r \otimes g^r = (f \otimes g)^r$ *if* $f, g \in S$
(j) $(\overline{f})^r = (-1)^m \overline{f^r}$.

Proof. The proofs of (a), (d), (f) and (g) are immediate consequences of the definition of $\otimes$-products. Consider (b). Let $h(X) = h_p X^p + \cdots + h_1 X + h_0$ have degree p and roots $\gamma_1, \ldots, \gamma_p$. Then

$$(f \otimes g) \otimes h = (f_m^n g_n^m)^p h_p^{mn} \prod_{i,j,k} (X - (\alpha_i \beta_j)\gamma_k)$$

and

$$f \otimes (g \otimes h) = f_m^{np} (g_n^p h_p^n)^m \prod_{i,j,k} (X - \alpha_i(\beta_j \gamma_k)).$$

Therefore $\otimes$ obeys the associative law. A similar argument proves (c), that $\otimes$ distributes over polynomial multiplication.

To prove (e), note that $f \otimes (X - \beta)$ is a polynomial of degree m with roots $\alpha_1\beta, \ldots, \alpha_m\beta$ and leading coefficient f_m. Setting $\beta = -1$ in (e) shows $f \otimes (X+1) = \overline{f}$. By (a), (b), (f) and (g) we have

$$\overline{\overline{f}} = f \otimes (X+1) \otimes (X+1) = f \otimes (X-1) = f$$

and

$$\overline{f} \otimes \overline{g} = f \otimes (X+1) \otimes g \otimes (X+1) = f \otimes (X+1) \otimes (X+1) \otimes g = f \otimes (X-1) \otimes g = f \otimes g.$$

Consider the proof of (i). Since $f, g \in S$, so $f_0 \neq 0$ and $g_0 \neq 0$. Thus the roots α_i and β_j are nonzero, and therefore

$$f^r(X) = (-1)^m f_0 \prod_{i=1}^{m} (X - \alpha_i^{-1}) \quad \text{and} \quad g^r(X) = (-1)^n g_0 \prod_{j=1}^{n} (X - \beta_j^{-1}).$$

Hence

$$(f^r \otimes g^r)(X) = f_0^n g_0^m \prod_{i,j} (X - \alpha_i^{-1} \beta_j^{-1}).$$

It follows from the definition of $\otimes$-product that

$$\begin{aligned}(f \otimes g)(0) &= f_m^n g_n^m (-1)^{mn} (\alpha_1 \cdots \alpha_m)^n (\beta_1 \cdots \beta_n)^m \\ &= f_m^n g_n^m (-1)^{mn} ((-1)^m f_0 f_m^{-1})^n ((-1)^n g_0 g_n^{-1})^m \\ &= (-1)^{mn} f_0^n g_0^m.\end{aligned}$$

Thus

$$(f\otimes g)^r(X) = f_0^n g_0^m \prod_{i,j}(X-(\alpha_i\beta_j)^{-1})$$
$$= (f^r \otimes g^r)(X).$$

Finally, putting $g = X+1$ in $(f\otimes g)^r = f^r \otimes g^r$ shows $(\overline{f})^r = (-1)^m \overline{f^r}$. □

Evaluating tensor products at $X=1$ yields connections with classical quantities such as resultants and discriminants. Recall that the resultant $\mathrm{Res}(f,g)$ is an element of R that is zero if and only if f and g have common roots in M, and the discriminant $D(f)$ is zero if and only if f has repeated roots. Some well-known properties of $\mathrm{Res}(f,g)$ and $D(f)$ such as those below, are proved in [**7**].

$$\mathrm{Res}(f,g) = \det\begin{pmatrix} f_m & f_{m-1} & \cdots & f_0 & & & \\ & \ddots & & & & \ddots & \\ & & f_m & f_{m-1} & & \cdots & f_0 \\ g_n & g_{n-1} & \cdots & g_0 & & & \\ & \ddots & & & & \ddots & \\ & & g_n & g_{n-1} & & \cdots & g_0 \end{pmatrix}$$
$$= f_m^n g_n^m \prod_{i,j}(\alpha_i-\beta_j) = f_m^n \prod_i g(\alpha_i) = (-1)^{mn} g_n^m \prod_j f(\beta_j).$$
$$D(f) = f_m^{-1}\ \mathrm{Res}(f,f') = f_m^{2m-2}\prod_{i<j}(\alpha_i-\alpha_j)^2.$$

The following lemma relates the determinant of the above $(m+n)\times(m+n)$ Sylvester matrix with the $mn\times mn$ determinant in Theorem 1.

Lemma 3. *Let $f,g\in R[X]^*$. If $f_0 \neq 0$, then $\mathrm{Res}(f,g) = (f^r\otimes g)(1)$ and*

$$(f^r\otimes f)(X) = f_0 f_m (X-1)^m(-1)^{m(m-1)/2}h(X) \tag{1}$$

where

$$h(X) = f_m^{2m-2}\prod_{i<j}(\alpha_j X-\alpha_i)(\alpha_j-\alpha_i X)\in R[X]$$

satisfies $h(1) = D(f)$.

Proof.

$$(f^r\otimes g)(X) = ((-1)^m f_0)^n g_n^m \prod_{i,j}(X-\alpha_i^{-1}\beta_j)$$
$$= (f_m\alpha_1\cdots\alpha_m)^n g_n^m \prod_{i,j}(X-\alpha_i^{-1}\beta_j)$$
$$= f_m^n g_n^m \prod_{i,j}(\alpha_i X-\beta_j)$$

When $g = f$, this expression may be rearranged to give (1). Setting $X = 1$ shows $(f^r \otimes g)(1) = \mathrm{Res}(f, g)$. Clearly,

$$h(1) = f_m^{2m-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 = D(f).$$

The proof that $h(X) \in R[X]$ involves considering elementary symmetric polynomials in $\alpha_1, \ldots, \alpha_m$. □

The assumption above that $f_0 \neq 0$ is not problematic given that $\mathrm{Res}(Xf, g) = g_0 \mathrm{Res}(f, g)$. Lemma 3 may be used in conjunction with Theorem 1 and facts such as $(fg)^r = f^r g^r$ and $f^r(1) = (-1)^m f(1)$ to deduce elementary properties of resultants such as $\mathrm{Res}(fg, h) = \mathrm{Res}(f, h)\,\mathrm{Res}(g, h)$ and $\mathrm{Res}(g, f) = (-1)^{mn}\mathrm{Res}(f, g)$.

4. Composites and $\otimes$-products

Let $f, g \in R[X]^*$. Then $f \otimes g$ and the composite polynomials $f \circ g$ and $g \circ f$ have degree mn. Furthermore, the coefficients of these polynomials bear some similarities to one another:

$\sum_{i=0}^{mn} a_i X^i$	a_{mn}	a_{mn-1}	$\cdots$	a_0
$f \otimes g$	$f_m^n g_n^m$	$-f_{m-1} f_m^{n-1} g_{n-1} g_n^{m-1}$	$\cdots$	$(-1)^{mn} f_0^n g_0^m$
$f \circ g$	$f_m g_n^m$	$m\ f_m g_{n-1} g_n^{m-1}$	$\cdots$	$f(g_0)$
$g \circ f$	$f_m^n g_n$	$n\ g_n f_{m-1} f_m^{n-1}$	$\cdots$	$g(f_0)$

It is a pleasant surprise that Theorem 2(e) generalizes to give a connection between tensor products and composites of polynomials. More importantly, this generalization provides a faster method for computing $\otimes$-products than Theorem 1.

Theorem 4. *Let Y, G and $\widehat{G}$ be as in Theorem 1. Then*

$$\begin{aligned} (f \otimes g)(X) &= \det((-Y)^m f^r(Y^{-1}G)) \\ &= g_n^m \det(f_0 \widehat{G}^m + f_1 X \widehat{G}^{m-1} + \cdots + f_m X^m I). \end{aligned} \tag{2}$$

Proof. Note that Y^{-1} is a matrix over $F(X)$, the field of fractions of $R[X]$. (Since $g_n \neq 0$, Y is invertible.) By Theorem 1,

$$(f \otimes g)(X) = \det \begin{pmatrix} Y & -G & 0 & \cdots & 0 \\ 0 & Y & -G & & 0 \\ & & & \ddots & \\ f_0 G & f_1 G & f_2 G & \cdots & f_{m-1}G + f_m Y \end{pmatrix}$$

Postmultiply column 1 by $Y^{-1}G$ and add the result to column 2. Then postmultiply column 2 by $Y^{-1}G$ and add the result to column 3, etc. Then

$$(f \otimes g) = \det \begin{pmatrix} Y & 0 & \cdots & 0 \\ 0 & Y & & 0 \\ & & \ddots & \\ H_1 & H_2 & \cdots & H_m \end{pmatrix}$$

where

$$\begin{aligned} H_i &= Y(f_{i-1}(Y^{-1}G) + \cdots + f_0(Y^{-1}G)^i) \quad \text{if} \quad 1 \le i < m, \quad \text{and} \\ H_m &= Y(f_m I + f_{m-1}(Y^{-1}G) + \cdots + f_0(Y^{-1}G)^m) = (-1)^m Y f^r(Y^{-1}G). \end{aligned}$$

Therefore,

$$(f \otimes g)(X) = \det(Y^{m-1}H_m) = \det((-Y)^m f^r(Y^{-1}G)).$$

Since $Y^{-1}G = X^{-1}\widehat{G}$ and $X^{-1}I$ and $\widehat{G}$ commute, the right-hand side simplifies to $g_n^m \det(f_0\widehat{G}^m + f_1X\widehat{G}^{m-1} + \cdots + f_mX^mI)$. □

Now the complexity of multiplying two $n \times n$ matrices is (for practical purposes) $O(n^3)$, and the complexity of computing an $n\times n$ determinant is $\frac{1}{3}n^3+O(n^2)$. Hence the complexity of computing (2) is $(m+\frac{1}{3})n^3+O(n^2)$. By contrast, the complexity of computing $f\otimes g$ via Theorem 1 is $\frac{1}{3}(mn)^3+O((mn)^2)$. (One practical application of Theorem 4 is to the computation of large degree irreducible polynomials over finite fields, see [**3**].)

5. Tensor Products of Power Series

The $\otimes$-product of two monic polynomials is again monic. If f and g are two power series whose constant terms are 1, it is natural to normalize their tensor product so its constant term is also 1. Towards this end define the binary operation $\odot$ on *polynomials* by $f \odot g = (-1)^{mn} f \otimes g$. If $f_0 = g_0 = 1$ and $m, n \ge k$, then the coefficient of X^k in $f \odot g$ is a polynomial in $f_1, \ldots, f_k, g_1, \ldots, g_k$. The polynomials when $k = 0, 1, 2, 3$ are

$$1,\ -f_1g_1,\ f_1^2g_2-2f_2g_2+f_2g_1^2, \text{ and } (-f_1^3-3f_3+3f_1f_2)g_3-f_1f_2g_1g_2+3f_3g_1g_2-f_3g_1^3,$$

respectively. If $1+XR[[X]]$ denotes the set of power series (with coefficients from R) and constant term 1, then the binary operation $\odot$ extends naturally to $1+XR[[X]]$. (If $f \in 1 + XR[[X]]$, let $\widehat{f}_k$ denote the polynomial $1 + \sum_{i=1}^k f_iX^i$. Then the coefficients of $1, X, \ldots, X^k$ of $f \odot g$ are defined to be the same as $\widehat{f}_k \odot \widehat{g}_k$.)

If $\oplus$ denotes multiplication in the abelian group $1 + XR[[X]]$, then $1 + XR[[X]]$ becomes a ring with addition $\oplus$ and multiplication $\odot$. Indeed, $1 + XR[[X]]$ is an integral domain where zero and one are the power series 1 and $1-X$, respectively (cf. [**5**]). The polynomials in $1+XR[[X]]$ form a subring. We shall show that for certain choices of R this subring is a unique factorization domain.

Given $f, g \in 1+XR[[X]]$, it can be difficult in practice to compute $f \odot g$. It is quite easy to show that

$$(1-rX) \odot \sum_{i=0}^{\infty} f_i X^i = \sum_{i=0}^{\infty} f_i (rX)^i \quad \text{and} \quad (1-X^m)^{-1} \odot (1-X^n)^{-1} = (1-X^e)^d$$

where $(1-X^m)^{-1}$ denotes the power series $\sum_{i=0}^{\infty} X^{mi}$, $e = \mathrm{lcm}(m,n)$ and $d = \gcd(m,n)$ (see Section 8). If the characteristic of R is zero and $r, \rho \in R$, one may define $(1-rX)^{\rho}$ and e^{rX} to be $\sum_{i=0}^{\infty} \binom{\rho}{i}(rX)^i$ and $\sum_{i=0}^{\infty}(rX)^i/i!$ where $\binom{\rho}{i} = \rho(\rho-1)\cdots(\rho-i+1)/i!$. Given $r, s, \rho, \sigma \in R$ one may prove

$$e^{rX} \odot e^{sX} = e^{-rsX},\ (1-rX)^{\rho} \odot (1-sX)^{\sigma} = (1-rsX)^{\rho\sigma} \text{ and } (1-rX)^{\rho} \odot e^{sX} = e^{rs\rho X}.$$

We shall omit these proofs and return to considering polynomials.

6. Field Extensions

A natural and fundamental question is: How does $f \otimes g$ factor into irreducibles over F? It follows from the law $f \otimes (gh) = (f \otimes g)(f \otimes h)$, that it is sufficient to answer this question when both f and g are irreducible over F.

Let α be one of $\alpha_1, \ldots, \alpha_m$ and β one of $\beta_1, \ldots, \beta_n$. Denote the minimum polynomial of α over F by $m_{\alpha/F}$ or, when there is no confusion over the field, by m_α. Henceforth assume that $f = m_\alpha$ and $g = m_\beta$ are irreducible over F and monic. In general, $m_\alpha \otimes m_\beta$ is reducible. For example, if $\alpha \notin F$, and $\beta = \alpha^{-1}$.

If $m_\alpha \otimes m_\beta$ is irreducible, then it equals $m_{\alpha\beta/F}$. Therefore $[F(\alpha\beta) : F] = mn$ holds, and one may deduce from the following diagram

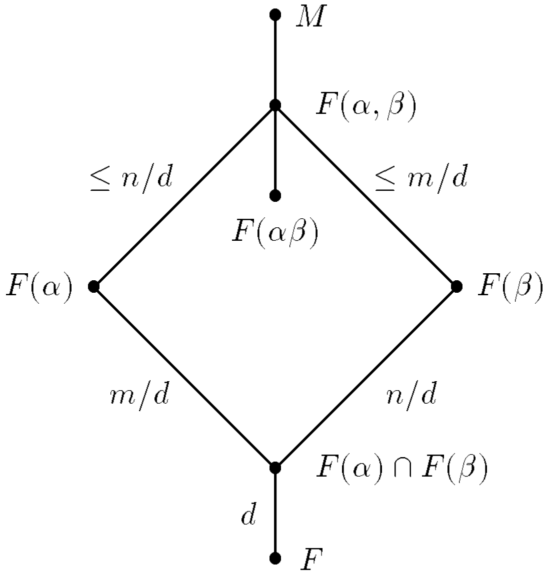

Figure 1. Subfields of $F(\alpha,\beta)$ and degrees of field extensions

that $F(\alpha)\cap F(\beta) = F$, $F(\alpha,\beta) = F(\alpha\beta)$, $[F(\alpha,\beta) : F(\alpha)] = n$ and $[F(\alpha,\beta) : F(\beta)] = m$. The following theorem is now straightforward to prove.

Theorem 5. *The following are equivalent*
(a) $m_{\alpha/F}\otimes m_{\beta/F}$ *is irreducible over* F*,*
(b) $[F(\alpha\beta) : F] = mn$*,*
(c) $m_{\beta/F}$ *is irreducible over* $F(\alpha)$*,*
(d) $m_{\alpha/F}$ *is irreducible over* $F(\beta)$*.*

In general, it is hard to determine whether $m_\alpha\otimes m_\beta$ equals $m_{\alpha\beta}$. However, if $[F(\alpha,\beta) : F] = mn$, this happens precisely when $F(\alpha,\beta) = F(\alpha\beta)$.

Theorem 6. *If* $[F(\alpha,\beta) : F] = mn$*, then*

$$(m_{\alpha/F}\otimes m_{\beta/F})(X) = m_{\alpha\beta/F}(X)^{[F(\alpha,\beta):F(\alpha\beta)]}.$$

Proof. Let $f = m_{\alpha/F}$ and $g = m_{\beta/F}$. Then $f_m = g_n = 1$, so $f = \widehat{f}$, $g = \widehat{g}$ and $G = \widehat{G}$. Now $1,\beta,\ldots,\beta^{n-1}$ is a basis for $F(\beta)$ over F. Since $[F(\alpha,\beta) : F] = mn$, it follows from Figure 1 that $1,\alpha,\ldots,\alpha^{m-1}$ is a basis for $F(\alpha,\beta)$ over $F(\beta)$. Hence

$$1,\beta,\ldots,\beta^{n-1},\alpha,\alpha\beta,\ldots,\alpha\beta^{n-1},\ldots,\alpha^{m-1},\alpha^{m-1}\beta,\ldots,\alpha^{m-1}\beta^{n-1}$$

is a basis for $F(\alpha,\beta)$ over F. Relative to this basis, multiplication by $\alpha\beta$ has matrix

$$\begin{pmatrix} 0 & G & 0 & \cdots & 0 \\ 0 & 0 & G & & 0 \\ & & & \ddots & \\ -f_0G & -f_1G & -f_2G & \cdots & -f_{m-1}G \end{pmatrix}$$

where $G = C(g)$. The above matrix equals $C(f) \otimes C(g)$, and its characteristic polynomial equals $m_{\alpha\beta/F}(X)^{[F(\alpha,\beta):F(\alpha\beta)]}$. Since $m_{\alpha\beta/F}$ is monic, Theorem 1 gives the desired result. $\square$

Corollary 7. *If $[F(\alpha,\beta) : F] = mn$ and $m_{\alpha/F} \otimes m_{\beta/F}$ is square-free, then $m_{\alpha/F} \otimes m_{\beta/F}$ is irreducible over F.*

The hypothesis $[F(\alpha,\beta) : F] = mn$ holds automatically in the case when m and n are coprime. The following theorem has as a corollary, the well-known and important fact that if F is a finite field and $\gcd(m,n) = 1$, then $m_{\alpha/F} \otimes m_{\beta/F}$ is irreducible over F of degree mn (see [**3**]).

Theorem 8. *Let $d = \gcd(m,n)$ and $e = \mathrm{lcm}(m,n)$. Suppose that M:F is Galois where $\Gamma(M : F)$ is cyclic and generated by η. Then*

$$m_{\alpha/F} \otimes m_{\beta/F} = h_0 h_1 \cdots h_{d-1}$$

where h_k is a polynomial over F of degree e. Furthermore, $h_k(X) = p_k(X)^{e_k}$ where $p_k(X)$ is irreducible of degree e_k, and e_k divides d. (In particular, when $m_{\alpha/F} \otimes m_{\beta/F}$ is square-free, the polynomials $h_k(X)$ are irreducible and pairwise coprime.)

Proof. Set $\alpha_i = \alpha\eta^i$ and $\beta_i = \beta\eta^i$. Then α_i, $i = 0, \ldots, m-1$, are distinct and $\alpha_m = \alpha_0$, and similarly β_i, $i = 0, \ldots, n-1$, are distinct and $\beta_n = \beta_0$. Therefore $m_{\alpha/F}$, $m_{\beta/F}$ and $m_{\alpha/F} \otimes m_{\beta/F}$ equal

$$\prod_{i=0}^{m-1}(X - \alpha_i), \quad \prod_{i=0}^{n-1}(X - \beta_i) \quad \text{and} \quad \prod_{i=0}^{m-1}\prod_{j=0}^{n-1}(X - \alpha_i\beta_j)$$

respectively. Define h_k to be the polynomial $h_k(X) = \prod_{i=0}^{e-1}(X - \alpha_i\beta_{i+k})$ where the subscripts for α (respectively β) are read modulo m (respectively n). Since $(\alpha_{e-1}\beta_{e-1+k})\eta = \alpha_e\beta_{e+k} = \alpha_0\beta_k$, it follows that $h_k(X) \in F[X]$. In addition, $h_k = h_{k+d}$. Note that if $M, N \in \mathbb{Z}$ satisfy $Mm + Nn = d$, then

$$\alpha_{Mm+i}\beta_{Mm+i+k} = \alpha_{Mm+i}\beta_{d-Nn+i+k} = \alpha_i\beta_{i+k+d}.$$

Furthermore, $m_{\alpha/F} \otimes m_{\beta/F} = h_0 h_1 \cdots h_{d-1}$. (Note that $h_0 h_1 \cdots h_{d-1}$ has $de = mn$ roots, counting multiplicities. Also, $\alpha_i\beta_j$ is a root of h_{j-i}, and if $j - i \equiv k \pmod{d}$ where $0 \le k < d$, then $h_{j-i} = h_k$.)

In general, the roots $\alpha_i\beta_j$, $1 \le i \le m$, $1 \le j \le n$, are not all distinct (i.e. $m_{\alpha/F} \otimes m_{\beta/F}$ is not square-free). Let $E = e_k$ be the smallest positive integer such that $\alpha_E\beta_{E+k} = \alpha_0\beta_k$. It follows that $\alpha_{i+E}\beta_{i+E+k} = \alpha_i\beta_{i+k}$ holds for all i, and $\alpha_{i+f}\beta_{i+f+k} \ne \alpha_i\beta_{i+k}$ for $1 \le f < E$. Thus the roots of h_k fall into orbits of length

e_k and so $h_k(X) = p_k(X)^{e_k}$ where $p_k(X) = \prod_{i=0}^{e_k-1}(X - \alpha_i\beta_{i+k})$ is the minimum polynomial of $\alpha_0\beta_k$. Thus $p_k(X)$ is irreducible over F.

We now show that if $d = 1$, then $m_{\alpha/F} \otimes m_{\beta/F}$ is irreducible over F. It suffices to prove that the $\alpha_i\beta_j$, $1 \le i \le m$, $1 \le j \le n$, are all distinct. Suppose that two are equal, say $\alpha_i\beta_j = \alpha_k\beta_\ell$. Thus $\alpha_i\alpha_k^{-1} = \beta_\ell\beta_j^{-1} = \lambda$ lies in the fixed field of η^m and of η^n. Hence λ lies in the fixed subfield of η, i.e. in F. Thus $\alpha_i = \lambda\alpha_k$ or $\alpha_0 = \lambda\alpha_{k-i}$, and similarly $\beta_0 = \lambda\beta_{j-\ell}$. Thus $\alpha_0 = \lambda^m\alpha_{m(k-i)} = \lambda^m\alpha_0$ and $\beta_0 = \lambda^n\beta_0$. Therefore, $\lambda^m = \lambda^n = 1$ and so $\lambda = 1$. Because the roots of m_α and m_β are distinct, this shows that $i \equiv k \pmod{m}$ and $j \equiv \ell \pmod{n}$, as desired.

Now let $f_k(X) = \prod_{i=0}^{m/d-1}(X - \alpha_{di+k})$ and $g_k(X) = \prod_{i=0}^{n/d-1}(X - \beta_{di+k})$. Then f_k and g_k are irreducible over the fixed subfield K of η^d. Furthermore,

$$m_{\alpha/F} = f_0 f_1 \cdots f_{d-1} \quad \text{and} \quad m_{\beta/F} = g_0 g_1 \cdots g_{d-1}$$

and $f_d = f_0$ and $g_d = g_0$. Since $\deg f_i = m/d$ and $\deg g_j = n/d$ are coprime, it follows from the previous paragraph that the $f_i \otimes g_j$ are irreducible over K of degree $(m/d)(n/d) = e/d$ and $m_{\alpha/F} \otimes m_{\beta/F} = \prod_{i,j} f_i \otimes g_j$ has d^2 irreducible factors over K. Suppose that p_k factors as a product of r_k irreducible factors over K. Then $\deg p_k = r_k e/d$. However, $e = e_k \deg p_k$ so $e_k r_k = d$. $\square$

The polynomials $h_0, h_1, \ldots, h_{d-1}$ in Theorem 8 need not be distinct. For example, if $\alpha = \beta$, then $e = d = m$ and $h_k = h_{-k}$. Furthermore, the exponents e_k may be greater than 1. For example, if $\alpha = \beta$ and m is even, then

$$h_{m/2}(X) = \left(\prod_{i=0}^{m/2-1} (X - \alpha_i\alpha_{i+m/2}) \right)^2 .$$

Also, if $\alpha = \beta$ and $x\eta = x^2$ for all $x \in M$, then $h_0(X) = m_{\alpha/F}(X)$, so $e_0 = 1$.

7. Tensor Products of Fields

We relate the problem of factoring $m_{\alpha/F} \otimes m_{\beta/F}$ into irreducible factors over F to the problem of writing $F(\alpha) \otimes F(\beta)$ as as a direct sum of fields.

Let $m_{\alpha/F}(X) = \prod_{i=1}^m (X - \alpha_i)$ and $m_{\beta/F}(X) = \prod_{i=1}^n (X - \beta_i)$ be separable polynomials over F. (Note that an irreducible polynomial is automatically separable if the characteristic of F does not divide its degree, or if F is finite.) Let M be the splitting field of the separable polynomial $m_\alpha m_\beta$. Then $M : F$ is a Galois extension. Let A and B denote the diagonal matrices $A = \mathrm{diag}(\alpha_1, \ldots, \alpha_m)$ and $B = \mathrm{diag}(\beta_1, \ldots, \beta_n)$ over M. Consider the F-algebra monomorphism

$$\phi : F(\alpha) \otimes_F F(\beta) \longrightarrow M_{mn}(M) \quad \text{defined by} \quad \sum_{i,j} a_{i,j}\alpha^i \otimes \beta^j \mapsto \sum_{i,j} a_{i,j} A^i \otimes B^j$$

where $a_{i,j} \in F$.

Recall that

$$A^k \otimes B^\ell = \mathrm{diag}(\alpha_1^k \beta_1^\ell, \ldots, \alpha_m^k \beta_1^\ell, \ldots, \alpha_1^k \beta_n^\ell, \ldots, \alpha_m^k \beta_n^\ell).$$

Let $\phi_i : F(\alpha) \otimes_F F(\beta) \longrightarrow M$ map x to the ith diagonal entry of $x\phi$. Then $\mathrm{im}\,\phi_{(j-1)m+i} = F(\alpha_i, \beta_j)$. If $\sigma \in \Gamma(M : F)$, then σ permutes the roots of m_α and m_β, and so permutes the fields $F(\alpha_i, \beta_j)$. Now $\Gamma(M : F)$ acts transitively on the roots of m_β, and so by renumbering $\alpha_1, \ldots, \alpha_m$ if necessary, we may assume that the orbit representatives of the fields $F(\alpha_i, \beta_j)$, $1 \le i \le m$, $1 \le j \le n$, under $\Gamma(M : F)$ are $F(\alpha_1, \beta), \ldots, F(\alpha_s, \beta)$. Thus $s \le m$ (and similarly $s \le n$).

Let $E_{(j-1)m+i}$ denote the field $F(\alpha_i, \beta_j)$. Suppose that $\beta_1 = \beta$ and consider the F-algebra homomorphism $\Phi : F(\alpha) \otimes_F F(\beta) \longrightarrow \oplus_{i=1}^s E_i$ defined by $x\Phi = (x\phi_1, \ldots, x\phi_s)$. If $x \in \ker \Phi$, then $x \in \ker \phi_i$ for $1 \le i \le s$ and so $x \in \ker \phi_i$ for $1 \le i \le mn$. Thus $x \in \ker \phi = \{0\}$ and so Φ is injective. Now $\mathrm{im}\,\Phi$ is an F-subalgebra of $\oplus_{i=1}^s E_i$ and so it is semisimple. By the Wedderburn-Artin theorem $\mathrm{im}\,\Phi$ is isomorphic to a direct sum of some of the fields E_i, $1 \le i \le s$. Now $\mathrm{im}\,\Phi$ projects onto each summand E_i and so if $\mathrm{im}\,\Phi$ were a proper F-subalgebra of $\oplus_{i=1}^s E_i$, then it follows that there is an F-isomorphism $E_i \longrightarrow E_j$ where $i \ne j$ and $1 \le i, j \le s$. Since $M : F$ is normal, such an F-isomorphism can be extended to an F-automorphism of M mapping E_i to E_j. This is a contradiction as $E_1, \ldots, E_s$, come from different orbits under $\Gamma(M : F)$. Hence Φ is an F-isomorphism.

Consider the characteristic polynomial of the transformation induced by multiplication by $(\alpha \otimes \beta)\Phi$ on $\oplus_{i=1}^s E_i$. By Theorem 6 it equals $m_{\alpha_i\beta}(X)^{e_i}$ where $e_i = [F(\alpha_i, \beta), F(\alpha_i\beta)]$. Therefore $m_\alpha \otimes m_\beta = \prod_{i=1}^s m_{\alpha_i\beta}(X)^{e_i}$, and we have proved

Theorem 9. *Let $m_{\alpha/F}$ and $m_{\beta/F}$ be separable polynomials and let M be the splitting field of $m_{\alpha/F} m_{\beta/F}$. Let $F(\alpha_1, \beta), \ldots, F(\alpha_s, \beta)$ be the representatives of different orbits of $\{F(\alpha_i, \beta_j) \mid 1 \le i \le m, 1 \le j \le n\}$ under $\Gamma(M : F)$. Then*

$$F(\alpha) \otimes_F F(\beta) \cong \bigoplus_{i=1}^{s} F(\alpha_i, \beta) \quad \text{and} \quad m_\alpha \otimes m_\beta = \prod_{i=1}^{s} m_{\alpha_i\beta}(X)^{e_i}$$

where $e_i = [F(\alpha_i, \beta), F(\alpha_i\beta)]$.

The polynomials $m_{\alpha_i\beta}(X)$, $1 \le i \le s$, in Theorem 9 need not be distinct as the following example shows.

Example. Suppose that q is a prime-power and that p is a prime such that $\mathrm{ord}_q(p) = p-1$ (i.e. p has order $p-1$ modulo q). Then $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ is irreducible over $F = \mathbb{F}_q$ and $\mathbb{F}_{q^p} = F(\alpha)$ where α is a root of $\Phi_p(X)$. Thus

$m_{\alpha/F} = \Phi_p$ and

$$F(\alpha) \otimes_F F(\alpha) \cong \bigoplus_{i=1}^{p-1} F(\alpha^i, \alpha) = \bigoplus_{i=1}^{p-1} F(\alpha).$$

Furthermore, $e_i = [F(\alpha^i, \alpha) : F(\alpha^{i+1})]$ equals 1 if $i \neq p-1$ and $p-1$ otherwise, and $m_{\alpha^{i+1}/F}(X) = m_{\alpha/F}(X)$ if $i \neq p-1$ and $X-1$ otherwise.

Let A be an F-algebra with 1, and let B and C be F-subalgebras (with the same 1) of A. Suppose that B and C generate A as an F-algebra, $\dim_F A = \dim_F B \dim_F C$ and $bc = cb$ for all $b \in B$ and $c \in C$. Then the map $B \otimes_F C \longrightarrow A$ defined by $b \otimes c \mapsto bc$ is an F-algebra isomorphism. In this case A is called an *internal tensor product* of B and C, and one can show that $B \cap C$ equals $F \cdot 1$.

Theorem 10. *Let $D = F(\alpha) \cap F(\beta)$ and suppose that the extensions $F(\alpha) : D$ and $D : F$ are both Galois. Then $F(\alpha) \otimes_F F(\beta)$ is isomorphic to a direct sum of $[D : F]$ copies of the field $F(\alpha, \beta)$.*

Proof. Note that $F(\alpha)$, $F(\beta)$ and $F(\alpha, \beta)$ are equal to $D(\alpha)$, $D(\beta)$ and $D(\alpha, \beta)$ respectively. Since $D(\alpha) : D$ is Galois, so is $D(\alpha, \beta) : D(\beta)$ and

$$\Gamma(D(\alpha, \beta) : D(\beta)) \cong \Gamma(D(\alpha) : D).$$

Thus $[D(\alpha, \beta) : D(\beta)] = [D(\alpha) : D]$ and so $[D(\alpha, \beta) : D] = [D(\alpha) : D][D(\beta) : D]$. By the above remarks $D(\alpha, \beta)$ is an internal $\otimes$-product $D(\alpha) \otimes_D D(\beta)$.

Since $D(\alpha) : D$ and $D : F$ are Galois, so is $D(\alpha) : F$. Let $\sigma \in \Gamma(D(\alpha) : F)$ and consider the F-algebra homomorphism

$$\phi_\sigma : F(\alpha) \otimes_F F(\beta) \longrightarrow D(\alpha\sigma, \beta) \quad \text{defined by} \quad \sum a_{i,j} \alpha^i \otimes \beta^j \mapsto \sum a_{i,j} (\alpha\sigma)^i \beta^j$$

where $a_{i,j} \in F$. Clearly $\operatorname{im} \phi_\sigma = D(\alpha\sigma, \beta) = D(\alpha, \beta)$ as $\alpha\sigma \in D(\alpha)$. Therefore $\ker \phi_\sigma$ is a maximal ideal of $F(\alpha) \otimes_F F(\beta)$. By Theorem 9, $F(\alpha) \otimes_F F(\beta)$ is a direct sum of s fields and so has precisely s maximal ideals. We shall prove that each maximal ideal has the form $\ker \phi_\sigma$ for some $\sigma \in \Gamma(D(\alpha) : F)$.

Let τ be an element of the subgroup $\Gamma(D(\alpha) : D)$ of $\Gamma(D(\alpha) : F)$. Let $\tau' \in \Gamma(D(\alpha, \beta) : D(\beta))$ be the extension of τ that fixes β. Then $\phi_\sigma \circ \tau' = \phi_{\sigma\tau}$ and so $\ker \phi_{\sigma\tau} = \ker \phi_\sigma$. Suppose now that $\sigma, \tau \in \Gamma(D(\alpha) : F)$ lie in different left cosets of $\Gamma(D(\alpha) : D)$. Then $\sigma^{-1}\tau \notin \Gamma(D(\alpha) : D)$ and so there exists a $\delta \in D$ such that $\delta\sigma^{-1}\tau \neq \delta$. Hence $1 \otimes \delta - \delta\sigma^{-1} \otimes 1$ lies in $\ker \phi_\sigma$ but not in $\ker \phi_\tau$. Thus the number, s, of maximal ideals is at least $[D : F]$ (as each coset of $\Gamma(D(\alpha) : D)$ in $\Gamma(D(\alpha) : F)$ gives rise to a different maximal ideal of the form $\ker \phi_\sigma$). We have thus shown that $\oplus_{i=1}^{[D:F]} D(\alpha, \beta)$ is a quotient of $F(\alpha) \otimes_F F(\beta)$. By counting dimensions, we see that $F(\alpha)\otimes_F F(\beta)\cong\oplus_{i=1}^{[D:F]}D(\alpha,\beta)$. Note that

$$\begin{aligned}\dim_F \bigoplus_{i=1}^{[D:F]} D(\alpha,\beta) &= [D:F][D(\alpha,\beta):F]\\ &= [D:F][D(\alpha):D][D(\beta):D][D:F]\\ &= [D(\alpha):F][D(\beta):F]\\ &= \dim_F F(\alpha)\otimes_F F(\beta).\end{aligned}$$

This concludes the proof. □

An immediate corollary of Theorem 10 is that $\mathbb{F}_{q^m}\otimes_{\mathbb{F}_q}\mathbb{F}_{q^n}\cong\mathbb{F}_{q^e}\oplus\cdots\oplus\mathbb{F}_{q^e}$ where $e=\mathrm{lcm}(m,n)$ and there are $d=\gcd(m,n)$ summands.

8. Some Examples

It is of interest to know which binomials in $F[X]$ are irreducible (c.f. [**2**]). This question can be reduced to binomials of prime-power degree using tensor products as the following argument shows.

Let X^m-a, X^n-b be binomials over F (so a and b are nonzero). If $d=\gcd(m,n)$, then it is straightforward to prove

$$(X^m-a)\otimes(X^n-b)=(X^{mn/d}-a^{n/d}b^{m/d})^d. \tag{3}$$

Now consider the binomial $X^r-c\in F[X]$. Suppose that r is not a prime power. Let $r=mn$ where $\gcd(m,n)=1$ and $m,n>1$. There exist integers M and N such that

$$Mm+Nn=1.$$

Then $c=c^{Mm+Nn}=a^nb^m$ where $a=c^N$ and $b=c^M$. Therefore,

$$(X^m-a)\otimes(X^n-b)=X^r-c.$$

Thus a necessary condition for X^r-c to be irreducible over F is that both X^m-a and X^n-b are irreducible over F. We show that this condition is also sufficient.

Suppose $\gcd(m,n)=1$ and α and β are roots of X^m-a and X^n-b respectively. Since $(\alpha\beta)^{Mm}=\alpha^{Mm}\beta^{1-Nn}=a^Mb^{-N}\beta$, we see $\beta\in F(\alpha\beta)$. Similarly, $\alpha\in F(\alpha\beta)$ so $F(\alpha,\beta)=F(\alpha\beta)$. Hence $[F(\alpha\beta):F]=mn$ and by Theorem 5, $(X^m-a)\otimes(X^n-b)$ is irreducible over F.

The next question to ask is: Which binomials $X^{p^m}-a$, where p is a prime, are irreducible over F? This is answered in [**6**, VIII, Theorem 16]. If p is an odd prime or $p^m=2$, then $X^{p^m}-a$ is irreducible if and only if $a\notin F^p$ (i.e. a is not a

pth power). If 4 divides p^m, then $X^{2^m} - a$ is irreducible if and only if $a \notin -4F^4$ (i.e. $a \neq -4b^4$ for all $b \in F$). Hence, one can completely classify the irreducible binomials. (With more work one can factor binomials into irreducible factors.)

Putting $a = b = 1$ in (3) shows $(X^m - 1) \otimes (X^n - 1) = (X^e - 1)^d$ where $e = \operatorname{lcm}(m,n)$. Thus the tensor product $\Phi_m \otimes \Phi_n$ of two cyclotomic polynomials is a product of certain Φ_r where r divides e. This factorization may be determined from the following facts

$$\Phi_m \otimes \Phi_n = \Phi_{mn} \qquad \text{if} \qquad \gcd(m,n) = 1, \tag{4}$$

and if p is a prime and $m \geq n$, then

$$\Phi_{p^m} \otimes \Phi_{p^n} = \begin{cases} (X^{p^n} - 1)^{\phi(p^n)}/\Phi_{p^n}(X)^{p^{n-1}} & \text{if } m = n, \\ \Phi_{p^m}(X)^{\phi(p^n)} & \text{if } m > n. \end{cases} \tag{5}$$

(Here ϕ denotes Euler's totient function.) The proof of (4) is straightforward, and (5) follows from the fact that the if α has order p^m and β has order p^n where $m > n$, then $\alpha\beta$ has order p^m.

By using (4) and (5) and the factorization $X^{p^n} - 1 = \prod_{i=0}^n \Phi_{p^i}(X)$, we may obtain factorizations of the form $\Phi_m \otimes \Phi_n = \prod \Phi_r^{e_r}$. For example,

$$\begin{aligned} \Phi_{60} \otimes \Phi_{40} &= (\Phi_4 \otimes \Phi_3 \otimes \Phi_5) \otimes (\Phi_8 \otimes \Phi_5) \\ &= (\Phi_8 \otimes \Phi_4) \otimes \Phi_3 \otimes (\Phi_5 \otimes \Phi_5) \\ &= \Phi_8^2 \otimes \Phi_3 \otimes \Phi_1^4 \Phi_5^3 \\ &= (\Phi_8 \otimes \Phi_3 \otimes \Phi_1)^8 (\Phi_8 \otimes \Phi_3 \otimes \Phi_5)^6 \\ &= \Phi_{24}^8 \Phi_{120}^6 \end{aligned}$$

Taking the degree of both sides gives identities such as

$$\phi(60)\phi(40) = 8\phi(24) + 6\phi(120).$$

9. Uniqueness of $\otimes$-factorizations

Let $U(R)$ denote the group of units of R, and $U(R[X]^*)$ the group of $\otimes$-units in $R[X]^*$. We call $f \in R[X]^*$ a $\otimes$-*unit* if there exists a $g \in R[X]^*$ such that $f \otimes g = X - 1$.

Lemma 10. *Every $f \in U(R[X]^*)$ may be uniquely written as $f = \alpha(X - \beta)$ where $\alpha, \beta \in U(R)$. Indeed, the map*

$$U(R[X]^*) \longrightarrow U(R) \times U(R) \quad \textit{defined by} \quad f \longmapsto (\alpha, \beta)$$

is a isomorphism.

The proof of this lemma is omitted as it is straightforward. We call $f \in R[X]^*$ $\otimes$-*irreducible* if f is not a $\otimes$-unit and $f = g \otimes h$ implies that g or h is a $\otimes$-unit. We call $f, g \in R[X]^*$ $\otimes$-*associates* if there is an $h \in U(R[X]^*)$ such that $f = g \otimes h$. There are two obvious questions to ask about $\otimes$-factorizations:

(F1) Can every $f \in R[X]^*$ which is not a $\otimes$-unit be factored as a $\otimes$-product of $\otimes$-irreducibles?

(F2) Are such factorizations unique? (That is, are the $\otimes$-irreducibles in one $\otimes$-factorization, up to order, $\otimes$-associates of the other?)

Now $R[X]^*$ does not satisfy (F1) as $1 \otimes 1 = 1$, $X \otimes X = X$ and 1 and X are not $\otimes$-units. For this reason we consider the following submonoid of $R[X]^*$

$$T = \{f \in R[X]^* \mid \deg f \geq 1 \quad \text{and} \quad f_0 \neq 0\}.$$

We show in Theorem 12 that T has property (F1) if R is a unique factorization domain.

Lemma 11. *(a) If $f \in R[X]^*$ is monic and $f = g \otimes h$ holds in $R[X]^*$, then there exist monic $\widehat{g}, \widehat{h} \in R[X]^*$ such that $f = \widehat{g} \otimes \widehat{h}$.*
(b) $^-$ and ^{r} respect $\otimes$-units, and $\otimes$-irreducibles with nonzero constant terms.
(c) If m is prime and $f_m, f_0 \in U(R)$, then f is $\otimes$-irreducible.
(d) If m is prime, f_m is irreducible in R and $f_0 \in U(R)$, then f is $\otimes$-irreducible.

Proof. (a) The leading term of $f = g \otimes h$ is $1 = g_n^p h_p^n$. Thus $g_n, h_p \in U(R)$, so setting $\widehat{g} = g_n^{-1} g$ and $\widehat{h} = h_p^{-1} h$ shows $\widehat{g} \otimes \widehat{h} = (g_n^{-p} h_p^{-n})(g \otimes h) = f$.
(b) This follows from Theorem 2(h) and (i).
(c) Suppose $f = g \otimes h$. Then $f_m = g_n^p h_p^n$ and $f_0 = (-1)^{np} g_0^p h_0^n$. Since $f_m, f_0 \in U(R)$, so $g_n, h_p, g_0, h_0 \in U(R)$. Since $m = np$ is prime, we may assume without loss of generality that $n = 1$. Therefore, $g \in U(R[X]^*)$ by Lemma 10, and hence f is $\otimes$-irreducible.
(d) This proof is similar to that of (c) and hence is omitted. □

Theorem 12. *If R is a unique factorization domain, then every element of T, which is not a unit, may be $\otimes$-factored as a product of $\otimes$-irreducibles.*

Proof. Let $f \in T$ and suppose $f_m = \varepsilon p_1 \cdots p_r$ and $f_0 = \eta q_1 \cdots q_s$ where $\varepsilon, \eta \in U(R)$ and the p_i and q_j are irreducible in R. Because R is a unique factorization domain, the quantity $d(f) = m + r + s$ is an invariant of f. Furthermore, $d(f) = 1$ if and only if $m = 1$ and $r = s = 0$. That is, if and only if $f \in U(R[X]^*)$. In addition, if $f = g \otimes h$, then $d(f) \geq d(g)$ with equality if and only if $h \in U(R[X]^*)$.

Our proof uses induction on $d(f)$. It is vacuously true if $d(f) = 1$. Suppose now $d(f) > 1$. If f is $\otimes$-irreducible, then the result is true. If not, then there exist

$g, h \in R[X]^*$ such that $f = g \otimes h$ where $d(g) < d(f)$ and $d(h) < d(f)$. The proof now follows from the inductive hypothesis. $\square$

There seems to be little connection between irreducible elements of $R[X]$ and $\otimes$-irreducible elements of $R[X]^*$. For example, if m is prime $(X-1)^m$ is reducible in $R[X]$ but is $\otimes$-irreducible by Lemma 11 (c). Conversely, if m is odd $(X^m - 2) \otimes (X^2+1) = X^{2m} + 4$ is irreducible in $\mathbb{Z}[X]$, but is clearly $\otimes$-reducible in $\mathbb{Z}[X]^*$.

Unfortunately Theorem 12 can not be strengthened to conclude that T has unique $\otimes$-factorization. The following example shows unique $\otimes$-factorization fails whenever $U(R) \neq \{1\}$.

Example. Let $\gamma \in U(R)$ have prime order p, or let γ have infinite order and let p be an arbitrary prime. Let q be a prime different to p and consider the $\otimes$-factorizations

$$\prod_{i=0}^{p-1}(X-\gamma^i) \otimes \prod_{j=0}^{q-1}(X-\gamma^{pj}) = \prod_{i=0}^{q-1}(X-\gamma^i) \otimes \prod_{j=0}^{p-1}(X-\gamma^{qj}) = \prod_{i=0}^{pq-1}(X-\gamma^i).$$

By Lemma 11 (c) the $\otimes$-factors of degree p and q are $\otimes$-irreducible. Since $p \neq q$, the polynomials of degree p and q are not $\otimes$-associates. Suppose the two polynomials of degree q are $\otimes$-associates. Then there is some $\varepsilon(X-\eta) \in U(R[X]^*)$ such that

$$\varepsilon(X-\eta) \otimes \prod_{i=0}^{q-1}(X-\gamma^i) = \prod_{i=0}^{q-1}(X-\gamma^{pi}).$$

Thus $\eta = \gamma^{pi}$ and $\eta\gamma = \gamma^{pj}$ where $0 \leq i, j < q$ and $i \neq j$. Therefore $\gamma^{p(j-i)} = \gamma$. This is impossible when γ has infinite order, and when γ has order p.

Because of this example and the identity $(fg) \otimes h = (f \otimes h)(g \otimes h)$, it seems unproductive to consider unique $\otimes$-factorization of reducible polynomials. Henceforth consider the $\otimes$-factorization of irreducibles. Now if $m_{\gamma/F} = f \otimes g$, then both f and g are irreducible. Hence, we may write $m_{\gamma/F} = m_{\alpha/F} \otimes m_{\beta/F}$ where $\gamma = \alpha\beta$. If $m_{\alpha/F}$ has degree m and $m_{\beta/F}$ has degree n, then $m_{\gamma/F}$ has degree mn and $F(\gamma)$ is an internal tensor product $F(\alpha) \otimes_F F(\beta)$ because $F(\alpha)F(\beta) = F(\gamma)$ and $[F(\gamma) : F] = mn$.

We shall investigate unique $\otimes$-factorization for finite fields. Although Theorems 13 and 14 were first proved by Brawley and Carlitz [**1**], their proofs were somewhat long and indirect. We offer shorter elementary proofs.

Theorem 13. *Let $F = \mathbb{F}_q$. If $m_{\gamma/F} = m_{\alpha/F} \otimes m_{\beta/F}$ is $\otimes$-reducible over F where $m = \deg m_{\alpha/F}$ and $n = \deg m_{\beta/F}$ are > 1, then $\deg m_{\gamma/F} = mn$, $\gcd(m,n) = 1$ and the order of γ divides $(q^m-1)(q^n-1)/(q-1)$. Conversely, if $\deg m_{\gamma/F} = mn$ where $\gcd(m,n) = 1$, and the order of γ divides $(q^m-1)(q^n-1)/(q-1)$, then* *there exist* $\alpha, \beta \in F(\gamma)$ *such that* $m_{\gamma/F} = m_{\alpha/F} \otimes m_{\beta/F}$ *and* $\deg m_{\alpha/F} = m$ *and* $\deg m_{\beta/F} = n$.

Proof. Suppose that $m_\gamma = m_\alpha \otimes m_\beta$ is $\otimes$-reducible where $\gamma = \alpha\beta$ and $m = \deg m_\alpha$, $n = \deg m_\beta$ are > 1. Then $\deg m_\gamma = mn$ where $m = \deg m_\alpha$ and $n = \deg m_\beta$. The lattice of subfields of $F(\gamma)$ is isomorphic to the lattice of divisors of mn and hence $\gcd(m, n) = 1$. Furthermore, it follows from $\gamma = \alpha\beta$ that the order of γ divides $\operatorname{lcm}(q^m - 1, q^n - 1) = (q^m - 1)(q^n - 1)/(q - 1)$.

Conversely, suppose that $\deg m_\gamma = mn$ where $\gcd(m, n) = 1$, and the order of γ divides $(q^m - 1)(q^n - 1)/(q - 1)$. Let Q_r be an abbreviation for $(q^r - 1)/(q - 1)$. Then $\gcd(Q_r, Q_s) = Q_{\gcd(r,s)}$. Thus there exist $M, N \in \mathbb{Z}$ such that $MQ_m + NQ_n = 1$. Set $\alpha = \gamma^{NQ_n}$ and $\beta = \gamma^{MQ_m}$. Then $\alpha\beta = \gamma^{MQ_m + NQ_n} = \gamma$ and

$$\alpha^{q^m - 1} = \gamma^{N(q^m - 1)(q^n - 1)/(q - 1)} = 1,$$

so $\alpha \in \mathbb{F}_{q^m}$. Similarly, $\beta \in \mathbb{F}_{q^n}$. Now $\deg m_\alpha$ divides m, $\deg m_\beta$ divides n and $m_\alpha \otimes m_\beta$ divides m_γ. Since m_γ is irreducible over F, $m_\gamma = m_\alpha \otimes m_\beta$ and so $\deg m_\alpha = m$ and $\deg m_\beta = n$. □

When cancellation laws hold, it is standard to prove that unique factorization holds by showing that the notions of "prime" and "irreducible" coincide. In general, cancellation laws do not hold. If $F = \mathbb{Q}$, and $f \otimes g = f \otimes h$ is irreducible, then it does not imply that g and h are $\otimes$-associate. For example, the factorizations $e^{2\pi i/8} = (1 + i)\frac{1}{\sqrt{2}} = (1 - i)\frac{i}{\sqrt{2}}$ give rise to the $\otimes$-factorizations

$$X^4 + 1 = (X^2 - 2X + 2) \otimes (X^2 - 1/2) = (X^2 - 2X + 2) \otimes (X^2 + 1/2)$$

over $\mathbb{Q}$. However, $X^2 - 1/2$ and $X^2 + 1/2$ are not $\otimes$-associate over $\mathbb{Q}$. (Indeed, unique $\otimes$-factorization fails over $\mathbb{Q}$!) As a consequence of Theorem 14, the above cancellation law holds for finite fields, however, we can not use this fact to prove

Theorem 14. *Every irreducible polynomial over* $\mathbb{F}_q$ *can be uniquely* $\otimes$*-factored into* $\otimes$*-irreducibles.*

Proof. As we are interested only in $\otimes$-factorizations of irreducible polynomials, we define a polynomial in $R[X]^*$ to be $\otimes$-*prime* if it is not a $\otimes$-unit, and if it is a $\otimes$-factor of $f \otimes g$ where $f \otimes g$ is irreducible, then it is a $\otimes$-factor of f or g. If f is $\otimes$-prime, then it is certainly $\otimes$-irreducible. (Let $R = \mathbb{F}_q$. If $f = g \otimes h$, then $g = f \otimes g_1$ or $h = h_1 \otimes f$. Thus $f = f \otimes g_1 \otimes h$ or $f = g \otimes h_1 \otimes f$ so g or h is a $\otimes$-unit.) Unique $\otimes$-factorization of irreducibles will follow once we prove that an irreducible $\otimes$-irreducible polynomial is $\otimes$-prime. (Suppose that $f_1 \otimes \cdots \otimes f_r = g_1 \otimes \cdots \otimes g_s$ are two $\otimes$-factorizations of an irreducible polynomial h into $\otimes$-irreducibles. Then f_1 is a $\otimes$-associate of some g_i. Similarly, f_2 is a $\otimes$-associate of some g_j. If $i = j$, then $f_1 \otimes f_1$ is a $\otimes$-factor of h. This is impossible as $f_1 \otimes f_1$ is reducible. Thus $i \neq j$ and we may show that $r = s$ and each f_i is a $\otimes$-associate of a unique g_j.)

Suppose that m_α is $\otimes$-irreducible and $m_\alpha \otimes m_\beta = m_\gamma \otimes m_\delta = m_\varepsilon$ is irreducible where $\alpha\beta = \gamma\delta$. Let a, b, c, d denote the degrees of $m_\alpha, m_\beta, m_\gamma, m_\delta$ respectively. Then by Theorem 13, $ab = cd$ and $\gcd(a, b) = \gcd(c, d) = 1$. Assume, without loss of generality, that $\gcd(a, c) > 1$. We consider two cases: when $\gcd(a, c) = a$ and $\gcd(a, c) < a$.

Case (i) $\gcd(a, c) = a$. First suppose that $a = c$. Then $b = d$ and $\lambda = \beta/\delta = \gamma/\alpha \in \mathbb{F}_{q^a} \cap \mathbb{F}_{q^b} = \mathbb{F}_q$. Thus $\gamma = \alpha\lambda$, so $m_\gamma = m_\alpha \otimes m_\lambda = m_\alpha \otimes (X - \lambda)$ and m_α is a $\otimes$-factor of m_γ as desired.

Assume now that $c = ar$ where $r > 1$. Since $c = \gcd(ab, c) = \gcd(a, c)\gcd(b, c)$, it follows that $r = \gcd(b, c)$ and $\gcd(a, r) = 1$. Thus there exist $C, D \in \mathbb{Z}$ such that $CQ_c + DQ_d = 1$. By the above comments, we may assume, without loss of generality, that

$$\gamma = \varepsilon^{DQ_d} \quad \text{and} \quad \delta = \varepsilon^{CQ_c}. \tag{6}$$

The order of ε divides $e = \operatorname{lcm}(q^a - 1, q^b - 1)$ and $f = \operatorname{lcm}(q^c - 1, q^d - 1)$ and hence divides $\gcd(e, f)$. However,

$$\begin{aligned} \gcd(e, f) &= (q-1)\gcd(e/(q-1), f/(q-1)) = (q-1)\gcd(Q_aQ_b, Q_cQ_d) \\ &= (q-1)\gcd(Q_a, Q_c)\gcd(Q_b, Q_c)\gcd(Q_a, Q_d)\gcd(Q_b, Q_d) \\ &= (q-1)Q_aQ_rQ_d = (q^a-1)(q^r-1)(q^d-1)/(q-1)^2. \end{aligned}$$

It follows from (6) that $\gamma^{(q^a-1)(q^r-1)/(q-1)} = \varepsilon^{D(q^a-1)(q^r-1)(q^d-1)/(q-1)^2} = 1$. Hence by Theorem 13, $m_\gamma = m_\rho \otimes m_\sigma$ where $\deg m_\rho = r$ and $\deg m_\sigma = a$. Since m_α and m_σ have the same degree, m_α is a $\otimes$-factor of m_σ and hence of m_γ, as desired.

Case (ii) $\gcd(a, c) < a$. This case never arises. If it did, an argument similar to the previous case would show that m_α is $\otimes$-reducible – a contradiction. $\square$

While it is true that $\otimes$-factorizations of $m_{\gamma/F}$ give rise to $\otimes$-factorizations of $F(\gamma)$, the converse is false.

Theorem 15. *The cyclotomic polynomial* Φ_{3^k} *is* $\otimes$*-irreducible over* $\mathbb{Q}$ *for all* $k \geq 1$.

Proof. Let $\zeta_n = e^{2\pi i/n}$ be a primitive nth root of 1. Then $\mathbb{Q}(\zeta_n) : \mathbb{Q}$ is Galois with Galois group isomorphic to the group $U(\mathbb{Z}_n)$ of order $\phi(n)$. Let $n = 3^k$ and $\zeta = \zeta_n$. Then $U(\mathbb{Z}_n) \cong C_2 \times C_{3^{k-1}}$ is isomorphic to a direct product of cyclic groups of order 2 and 3^{k-1}. The only possible factorization of $\phi(n) = 2 \cdot 3^{k-1}$ as a product with coprime factors is, 2 times 3^{k-1}. Hence the only possible $\otimes$-factorization of $\mathbb{Q}(\zeta)$ is, $\mathbb{Q}(\omega) \otimes \mathbb{Q}(\theta)$ where $\omega = \zeta^{n/3}$ and $\theta = \zeta + \zeta^{-1}$. If Φ_n were $\otimes$-reducible, then there exist $\alpha, \beta \in \mathbb{Q}(\zeta)$ such that $\zeta = \alpha\beta$, $\mathbb{Q}(\alpha) = \mathbb{Q}(\omega)$ and $\mathbb{Q}(\beta) = \mathbb{Q}(\theta)$. Replacing α, β by $\alpha\mu^{-1}, \beta\mu$ where $\mu \in \mathbb{Q}$ if necessary, we may assume that α may be written in the form $\alpha = \lambda + \omega$ where $\lambda \in \mathbb{Q}$.

Now $(\alpha\beta)^n = \zeta^n = 1$ and so $\alpha^n = \beta^{-n} \in \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$. Consider $\alpha^n = \sum_{i=0}^n \binom{n}{i}\lambda^i\omega^{n-i}$. If $i \equiv 1 \pmod 3$, then $\omega^{n-i} = \omega^2 = -1-\omega$ and if $i \equiv 2 \pmod 3$, then $\omega^{n-i} = \omega$. Writing $(\lambda+\omega)^n$ in the form $\sigma + \tau\omega$ where $\sigma, \tau \in \mathbb{Q}$ shows

$$\tau = \sum_{i\equiv 1 \pmod 3} -\binom{n}{i}\lambda^i + \sum_{i\equiv 2 \pmod 3} \binom{n}{i}\lambda^i = \sum_{i\equiv 1 \pmod 3} -\binom{n}{i}\lambda^i + \binom{n}{i+1}\lambda^{i+1}.$$

Since when $0 < i < n$, the largest power of 3 dividing $n-i$ is the largest power of 3 dividing i, it follows that n divides $\binom{n}{i}$ if $n \equiv 1, 2 \pmod 3$. Hence the above polynomial in λ has the form $\tau = n\lambda a(\lambda)$ where

$$a(\lambda) = -1 + a_1\lambda - a_3\lambda^3 + a_4\lambda^4 - \cdots + \lambda^{n-1} \quad \text{and} \quad a_i = \frac{1}{n}\binom{n}{i+1}$$

are positive integers. Now the only possible *rational* roots of $a(\lambda)$ are ± 1, because $a(\lambda)$ is monic and $a(0) = -1$. It is clear that $a(-1) < 0$. Also, $a(1) = 0$ because $\binom{n}{i} = \binom{n}{n-i}$ and, if $i \equiv 1 \pmod 3$, then $n - i \equiv 2 \pmod 3$. Since $\lambda \in \mathbb{Q}$ satisfies $n\lambda a(\lambda) = 0$, it follows that $\lambda = 0, 1$. Hence $\alpha = \lambda + \omega = \omega, -\omega^2$ and $\beta = \zeta\alpha^{-1} = \zeta^{1-n/3}, -\zeta^{1-2n/3}$. This is a contradiction, as then $\mathbb{Q}(\beta) = \mathbb{Q}(\zeta) \neq \mathbb{Q}(\theta)$. Hence Φ_{3^k} is $\otimes$-irreducible over $\mathbb{Q}$ for all $k \geq 1$. $\square$

It is shown in [**4**] that, if n is odd, the $\otimes$-factorization of $\Phi_n(X)$ over $\mathbb{Q}$ into $\otimes$-irreducibles is the same as the factorization of n into prime-powers.

Acknowledgements

I am most grateful to L.G. Kovács for comments and discussions which, amongst other things, lead to an improved version of Theorem 8. I would also like to thank A.M. Nelson for comments relating to Theorem 10.

References

1. J.V. Brawley and L. Carlitz, *Irreducibles and the composed product for polynomials over a finite field*, Discrete Mathematics **65** (1987), 115–139.

2. D. Gay and W.Y. Vélez, *On the degree of the splitting field of an irreducible binomial*, Pacific J. Math. **78** (1978), 117–120.

3. S.P. Glasby, *Computing efficiently with cyclic Galois extensions*, in prep.

4. S.P. Glasby, *Unique tensor factorization of irreducible projective representations over $\mathbb{Q}$ of cyclic groups*, in prep.

5. Donald Knutson, *λ-Rings and the Representation Theory of the Symmetric Goup*, Lecture Notes in Matematics 308, Springer-Verlag, 1973.

6. Serge Lang, *Algebra*, Addison–Wesley, 1980.

7. B.L. van der Waerden, *Algebra Vol. 1*, Frederick Ungar, 1970.