On the tensor product of polynomials over a ring

S. P. Glasby

Dedicated, with much respect, to Laci Kovács

Abstract. Given polynomials a and b over an integral domain R, their tensor product (denoted $a \otimes b$) is a polynomial over R of degree $\deg(a)\deg(b)$ whose roots comprise all products $\alpha\beta$, where α is a root of a, and β is a root of b. This paper considers basic properties of $\otimes$ including how to factor $a \otimes b$ into irreducibles factors, and the direct sum decomposition of the $\otimes$-product of fields.

2000 Mathematics subject classification: 13P05, 13W05

1. Introduction

Let $a_0, \ldots, a_m$ and $b_0, \ldots, b_n$ be indeterminates and let $a = \sum_{i=0}^{m} a_i X^i$ and $b = \sum_{i=0}^{n} b_i X^i$ be polynomials of degree $m \geq 0$ and $n \geq 0$ respectively over the polynomial ring $\mathbb{Z}_{m,n} = \mathbb{Z}[a_0, \ldots, a_m, b_0, \ldots, b_n]$. Let a have roots $\alpha_1, \ldots, \alpha_m$ and b have roots $\beta_1, \ldots, \beta_n$ in the splitting field of a and b over the field of fractions of $\mathbb{Z}_{m,n}$. Then the *tensor product* of a and b is defined to be

$$a \otimes b = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (X - \alpha_i \beta_j).$$

It follows from Theorem 2.1 below that $a \otimes b$ is a polynomial, of degree mn, over $\mathbb{Z}_{m,n}$. The purpose of this paper is to study properties of $\otimes$. We remark that one may define the tensor product of non-zero polynomials over an arbitrary commutative ring R with 1 by using the above definition

and evaluation homomorphisms $\mathbb{Z}_{m,n} \to R$. Most of the theory carries over *mutatis mutandis* to $R[X]$ when R is an integral domain. In Section 3, according to context, the symbols $a_0, \ldots, a_m, b_0, \ldots, b_n$ need to be interpreted as elements of R, and not indeterminants. If R has zero divisors, then the degree of $a \otimes b$ may be less than mn (in which case $a \otimes b = 0$).

The concept of the $\otimes$-product of monic polynomials was introduced by Brawley and Carlitz in 1987 (see [BC87, BB93]) as a special case of a composed product. We find it convenient to define the $\otimes$-product of non-monic polynomials so that, for example, Theorem 2.1 has a nice statement. One motivation for studying the tensor product of polynomials arises from the following problem. Given an $\mathbb{F}G$-module U for a (finite) group G, determine when is it isomorphic to an inner tensor product $V \otimes W$ of $\mathbb{F}G$-modules of smaller dimension (see [LO97]). A necessary condition for this is that the characteristic polynomial of an element of G acting on U can be written as a $\otimes$-product of smaller degree polynomials. Note that if $c(A)$ denotes the characteristic polynomial of a matrix A, then $c(A \otimes B) = c(A) \otimes c(B)$.

The definition of the tensor product on $R[X]$ is closely related to multiplication in the Witt ring $W(R)$ which may be viewed as the set, $1 + XR[[X]]$, of power series with constant term 1 (with appropriate operations of addition and multiplication, see [K73]). In keeping with the motivation for this paper, we will focus on tensor multiplication and factorization in $R[X]$ and not $W(R)$. In Section 2 we study the coefficients of $a \otimes b$, and also show that if R is an integral domain, then the polynomials in $R[X]$ with non-zero constant term form a commutative 'semi-ring' with 1 which has a natural automorphism of order 2. In Section 3 we show how $a \otimes b$ factors into irreducibles, and how this factorization is related to the tensor factorization of fields. In Section 4 we consider the factorization of $a \otimes b$ where both a and b are binomial, or cyclotomic polynomials.

The topic of unique $\otimes$-factorization is not discussed here. It is shown in [BC87] that unique $\otimes$-factorization holds for the set of all irreducible polynomials (excluding X) over a finite field. A shorter proof of this fact is given in [G95]. It is shown in Lemma 3.2(v) that a tensor factorization of a polynomial gives rise to a tensor factorization of a field. The converse

is false. Let $\zeta = (1+i)/\sqrt{2}$ where $i = \sqrt{-1}$. Then ζ is a primitive eighth root of unity, and there are three ways to write the cyclotomic field $\mathbb{Q}(\zeta)$ as a tensor product over $\mathbb{Q}$ of proper subfields:

$$\mathbb{Q}(i) \otimes \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(i) \otimes \mathbb{Q}(\sqrt{-2}), \quad \text{and} \quad \mathbb{Q}(\sqrt{2}) \otimes \mathbb{Q}(\sqrt{-2}).$$

Each factorization shows that ζ can be written as a *sum of products* of elements from the quadratic subfields. However, only in the first two cases can ζ be written as a *product* of elements from the quadratic subfields, namely $\zeta = (1+i)\dfrac{1}{\sqrt{2}} = (1-i)\dfrac{-1}{\sqrt{-2}}$. These two factorizations give rise to $\otimes$-factorizations of the minimal polynomial of ζ over $\mathbb{Q}$:

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

2. Basic properties of $\otimes$

Recall that the *degree* and *weight* of the monomial $\lambda a_0^{k_0} a_1^{k_1} \cdots a_m^{k_m}$ are $\sum_{i=0}^m k_i$ and $\sum_{i=0}^m i k_i$ respectively. We say that a polynomial in several variables has *uniform weight* k if every monomial summand has weight k; we say that it has *uniform degree* k (or is *homogeneous of degree* k) if every monomial summand has degree k. We adopt the convention that $a_k = 0$ if $k > m$, and similarly $b_k = 0$ if $k > n$.

We give an example of the coefficients of $a \otimes b$. A long, but otherwise straightforward, calculation shows that

$$\begin{aligned}(a_0 + a_1X + a_2X^2 + a_3X^3) \otimes (b_0 + b_1X + b_2X^2) = \\ a_0^2b_0^3 - a_0a_1b_0^2b_1X + (a_0a_2b_0b_1^2 + a_1^2b_0^2b_2 - 2a_0a_2b_0^2b_2)X^2 \\ + (3a_0a_3b_0b_1b_2 - a_1a_2b_0b_1b_2 - a_0a_3b_1^3)X^3 \\ + (a_2^2b_0b_2^2 + a_1a_3b_1^2b_2 - 2a_1a_3b_0b_2^2)X^4 - a_2a_3b_1b_2^2X^5 + a_3^2b_2^3X^6.\end{aligned}$$

For a different perspective on computing coefficients of $a \otimes b$, see [S99].

The reader is referred to [M95] for notation and terminology concerning partitions and symmetric polynomials. Denote the set of all partitions $\lambda = (\lambda_1, \ldots, \lambda_m)$ of k with $n \geq \lambda_1 \geq \cdots \geq \lambda_m \geq 0$ by $P_{k,m,n}$, and the dominance partial order on $P_{k,m,n}$ by $\leq$. Given $\lambda \in P_{k,m,n}$ define

$$\lambda'_i = |\{k \mid \lambda_k \geq i\}| \quad \text{and} \quad \widetilde{\lambda}_j = n - \lambda_{m-j+1}$$

for $i = 1, \ldots, n$ and $j = 1, \ldots, m$. Then the conjugate partition, λ', of λ lies in $P_{k,n,m}$ and $\widetilde{\lambda} \in P_{mn-k,m,n}$. It is easy to see, by considering the diagram of a partition, that

$$\widetilde{\lambda}'_i + \widetilde{\lambda}'_{n-i+1} = m \qquad \text{for } i = 1, \ldots, n.$$

Define $b_\lambda = b_{\lambda_1} \cdots b_{\lambda_m}$ and $a_{\lambda'} = a_{\lambda'_1} \cdots a_{\lambda'_n}$. For $i = 0, \ldots, m$, denote by e_i the ith elementary symmetric polynomial in variables $\alpha_1, \ldots, \alpha_m$, and observe that, when evaluated in the splitting field of a,

$$e_i = (-1)^i a_m^{-1} a_{m-i}.$$

Define $e_\mu = e_{\mu_1} \cdots e_{\mu_n}$ for $\mu \in P_{mn-k,n,m}$. Hence, by the previous two displayed equations,

$$\begin{aligned} e_{\widetilde{\lambda}'} = e_{\widetilde{\lambda}'_1} \cdots e_{\widetilde{\lambda}'_n} &= (-1)^{|\widetilde{\lambda}'|} a_m^{-n} \prod_{i=1}^{n} a_{m-\widetilde{\lambda}'_i} \\ &= (-1)^{mn-k} a_m^{-n} \prod_{i=1}^{n} a_{\lambda'_{n-i+1}} = (-1)^{mn-k} a_m^{-n} a_{\lambda'}. \end{aligned}$$

Consider $\nu \in P_{mn-k,m,n}$. In particular ν is an m-tuple. Observe that the symmetric group S_m acts naturally on m-tuples of integers, preserving the total sum of the entries, and define

$$m_\nu(\alpha_1, \ldots, \alpha_m) = \sum \alpha_1^{j_1} \cdots \alpha_m^{j_m}$$

where the sum ranges over all m-tuples $(j_1, \ldots, j_m)$ in the S_m-orbit of ν. Thus $m_\nu(\alpha_1, \ldots, \alpha_m)$ is invariant under permutations of $\{1, \ldots, m\}$, and so is symmetric when regarded as a polynomial in $\alpha_1, \ldots, \alpha_m$. Hence by [M95, I, 2.3] and Möbius inversion, $m_\nu(\alpha_1, \ldots, \alpha_m) = \sum_{\mu \le \nu} \varepsilon_{\nu,\mu} e_{\mu'}$ for some integers $\varepsilon_{\nu,\mu}$ where $\varepsilon_{\nu,\nu} = 1$. These considerations, and the fact that the map $P_{k,m,n} \to P_{mn-k,m,n}$ defined by $\lambda \mapsto \widetilde{\lambda}$ is an order-preserving bijection, tell us that

$$\begin{aligned} m_{\widetilde{\lambda}}(\alpha_1, \ldots, \alpha_m) &= \sum_{\widetilde{\mu} \le \widetilde{\lambda}} \varepsilon_{\widetilde{\lambda},\widetilde{\mu}} e_{\widetilde{\mu}'} = \sum_{\mu \le \lambda} \varepsilon_{\widetilde{\lambda},\widetilde{\mu}} (-1)^{mn-k} a_m^{-n} a_{\mu'} \\ &= a_m^{-n} \sum_{\mu \le \lambda} \gamma^{(k)}_{\lambda,\mu} a_{\mu'} \end{aligned}$$

where $\gamma^{(k)}_{\lambda,\mu} = (-1)^{mn-k} \varepsilon_{\widetilde{\lambda},\widetilde{\mu}}$ satisfies $\gamma^{(k)}_{\lambda,\lambda} = (-1)^{mn-k}$ for each λ, k.

THEOREM 2.1. *If* $a \otimes b = \sum_{k=0}^{mn} c_k X^k$, *then for each* k,

$$c_k = \sum_{\lambda \in P_{k,m,n}} \sum_{\mu \geq \lambda} \gamma_{\lambda,\mu}^{(k)} a_{\lambda'} b_\mu,$$

for some integers $\gamma_{\lambda,\mu}^{(k)}$ *such that* $\gamma_{\lambda,\lambda}^{(k)} = (-1)^{mn-k}$ *for all* $\lambda \in P_{k,m,n}$. *In particular,* c_k *is an element of* $\mathbb{Z}_{m,n}$ *which has uniform degree* n *(respectively* m*) and uniform weight* k *when viewed as a polynomial in* $a_0, \ldots, a_m$ *(respectively* $b_0, \ldots, b_n$*).*

Proof. For each i, the polynomials $(X - \alpha_i) \otimes b$ and $\sum_{j=0}^{n} \alpha_i^{n-j} b_j X^j$ are equal as they have the same roots and leading coefficient. We have

$$\begin{aligned} a \otimes b &= a_m^n \prod_{i=1}^{m} ((X - \alpha_i) \otimes b) = a_m^n \prod_{i=1}^{m} \sum_{j=0}^{n} a_i^{n-j} b_j X^j \\ &= a_m^n \sum_{k=0}^{mn} \left(\sum \alpha_1^{n-j_1} \cdots \alpha_m^{n-j_m} b_{j_1} \cdots b_{j_m} \right) X^k, \end{aligned}$$

where the inner sum is over all m-tuples $(j_1, \ldots, j_m)$ with $0 \leq j_1, \ldots, j_m \leq n$ and $j_1 + \cdots + j_m = k$. Hence

$$a \otimes b = a_m^n \sum_{k=0}^{mn} \left(\sum_{\lambda \in P_{k,m,n}} \left(\sum \alpha_1^{n-j_1} \cdots \alpha_m^{n-j_m} \right) b_\lambda \right) X^k$$

where now the inner sum ranges over all m-tuples $(j_1, \ldots, j_m)$ in the S_m-orbit of the given $\lambda \in P_{k,m,n}$. Thus, by the comments immediately preceding the statement of this theorem,

$$\begin{aligned} a \otimes b &= a_m^n \sum_{k=0}^{mn} \left(\sum_{\lambda \in P_{k,m,n}} m_{\widetilde{\lambda}}(\alpha_1, \ldots, \alpha_m) b_\lambda \right) X^k \\ &= \sum_{k=0}^{mn} \left(\sum_{\lambda \in P_{k,m,n}} \sum_{\mu \leq \lambda} \gamma_{\lambda,\mu}^{(k)} a_{\mu'} b_\lambda \right) X^k, \end{aligned}$$

and the theorem follows quickly. □

The integer $\gamma_{\lambda,\mu}^{(k)}$ is a sum of products of Kosta numbers (see [M95]). Computing tensor products over the ring

$$(\mathbb{Z}/p\mathbb{Z})[a_0, \ldots, a_m, b_0, \ldots, b_n] \cong \mathbb{Z}_{m,n}/p\mathbb{Z}_{m,n}$$

is generally faster than computing in $\mathbb{Z}_{m,n}$, and the intermediate calculations do not involve large integers. Furthermore, if p is chosen so that $-p/2 < \gamma_{\lambda,\mu}^{(k)} < p/2$ holds for all k, λ, μ, then it follows from Theorem 2.1 that one can unambiguously pull back a $\otimes$-product computed in $\mathbb{Z}_{m,n}/p\mathbb{Z}_{m,n}$ to $\mathbb{Z}_{m,n}$. We shall now relate $\otimes$-products in $\mathbb{Z}_{m,n}$ to multiplication in the Witt ring $W(\mathbb{Z})$.

The following technical result allows us to define multiplication, denoted $\odot$, in the Witt ring of $\mathbb{Z}[a_1, a_2, \ldots, b_1, b_2, \ldots]$. Suppose $m > 0$ and ϕ is a homomorphism $\mathbb{Z}_{m,n}[X] \to \mathbb{Z}_{m-1,n}[X]$ mapping a_m to zero and fixing $\mathbb{Z}_{m-1,n}[X]$ elementwise. Then $\phi(a) = \sum_{i=0}^{m-1} a_i X^i$ and $\phi(b) = b$.

PROPOSITION 2.2. *With the above notation:*
(i) $\phi(a \otimes b) = (-1)^n b_0 \, (\phi(a) \otimes \phi(b))$.
(ii) Suppose $a_0 = b_0 = 1$ *and* $R = \mathbb{Z}[a_1, \ldots, a_m, b_1, \ldots, b_n]$. *Then the binary operation* $\odot$ *on* $R[X]$ *defined by* $a \odot b = (-1)^{\deg(a)\deg(b)}(a \otimes b)$ *satisfies* $\phi(a \odot b) = \phi(a) \odot \phi(b)$.

Proof. *(i)* Let $c = a \otimes b$ and $d = \phi(a) \otimes b$. We shall show that

$$\phi(c_k) = (-1)^n b_0 d_k$$

holds for $k = 0, \ldots, (m-1)n$. By Theorem 2.1

$$\phi(c_k) = \sum_{\lambda \in P_{k,m,n}} \sum_{\mu \geq \lambda} \gamma_{\lambda,\mu}^{(k)} \phi(a_{\lambda'}) b_\mu \quad \text{and} \quad d_k = \sum_{\rho \in P_{k,m-1,n}} \sum_{\sigma \geq \rho} \gamma_{\rho,\sigma}^{(k)} a_{\rho'} b_\sigma.$$

The following are equivalent: $\phi(a_{\lambda'}) \neq 0$; $\phi(a_{\lambda'}) = a_{\lambda'}$; $m > \lambda_1'$; $\lambda_m = 0$. If $\mu \geq \lambda$ and $\lambda_m = 0$, then $\mu_m = 0$. Now $\psi: P_{k,m-1,n} \to P_{k,m,n}$ defined by $\psi(\rho_1, \ldots, \rho_{m-1}) = (\rho_1, \ldots, \rho_{m-1}, 0)$ is an order-preserving injective map. Let $\lambda = \psi\rho$ and $\mu = \psi\sigma$ where $\rho, \sigma \in P_{k,m-1,n}$. Then $a_{\lambda'} = a_{\rho'}$ and $b_\mu = b_0 b_\sigma$, so

$$\phi(c_k) = \sum_{\rho \in P_{k,m-1,n}} \sum_{\sigma \geq \rho} \gamma_{\psi\rho,\psi\sigma}^{(k)} a_{\rho'} b_0 b_\sigma.$$

We complete the proof by showing below that $\gamma_{\widetilde{\psi\rho},\widetilde{\psi\sigma}}^{(k)} = \gamma_{\widetilde{\rho},\widetilde{\sigma}}^{(k)}$, or equivalently $\varepsilon_{\widetilde{\psi\rho},\widetilde{\psi\sigma}} = \varepsilon_{\widetilde{\rho},\widetilde{\sigma}}$, holds for $\rho, \sigma \in P_{k,m-1,n}$.

Recall that

$$(1) \qquad m_{\widetilde{\sigma}}(\alpha_1,\dots,\alpha_{m-1}) = \sum_{\widetilde{\sigma}\le\widetilde{\rho}} \varepsilon_{\widetilde{\rho},\widetilde{\sigma}}\, e_{\widetilde{\sigma}'}(\alpha_1,\dots,\alpha_{m-1}), \quad \text{and}$$

$$(2) \qquad m_{\widetilde{\psi\sigma}}(\alpha_1,\dots,\alpha_m) = \sum_{\widetilde{\psi\sigma}\le\widetilde{\psi\rho}} \varepsilon_{\widetilde{\psi\rho},\widetilde{\psi\sigma}}\, e_{\widetilde{\psi\sigma}'}(\alpha_1,\dots,\alpha_m).$$

Now $(\widetilde{\psi\sigma})_1 = n$ and

$$\frac{1}{n!}\frac{\partial^n}{\partial {\alpha_m}^n} m_{\widetilde{\psi\sigma}}(\alpha_1,\dots,\alpha_m) = m_{\widetilde{\sigma}}(\alpha_1,\dots,\alpha_{m-1}).$$

Since $\prod_{j=1}^{m}(X-\alpha_j) = \sum_{i\le m}(-1)^i e_i(\alpha_1,\dots,\alpha_m)X^{m-i}$ holds for $m \ge 0$, we see that $e_i(\alpha_1,\dots,\alpha_m)$ equals 0 if $i < 0$, and 1 if $i = 0$. Since $m \ge 1$, it follows that

$$e_i(\alpha_1,\dots,\alpha_m) = e_i(\alpha_1,\dots,\alpha_{m-1}) + e_{i-1}(\alpha_1,\dots,\alpha_{m-1})\alpha_m.$$

Therefore $e_{(\nu_1,\dots,\nu_n)}(\alpha_1,\dots,\alpha_m)$ is a polynomial in α_m of degree $\le n$ and the coefficient of α_m^n is $e_{(\nu_1-1,\dots,\nu_n-1)}(\alpha_1,\dots,\alpha_{m-1})$. Thus

$$\frac{1}{n!}\frac{\partial^n}{\partial {\alpha_m}^n} e_{(\nu_1,\dots,\nu_n)}(\alpha_1,\dots,\alpha_m) = e_{(\nu_1-1,\dots,\nu_n-1)}(\alpha_1,\dots,\alpha_{m-1}).$$

However, it can been seen by considering the diagram of a partition that $(\widetilde{\psi\sigma})'_i - 1 = (\psi\widetilde{\sigma})'_i$ holds for $\sigma \in P_{k,m-1,n}$ and $1 \le i \le n$. Thus

$$(3) \qquad \frac{1}{n!}\frac{\partial^n}{\partial {\alpha_m}^n} m_{\widetilde{\psi\sigma}}(\alpha_1,\dots,\alpha_m) = \sum_{\widetilde{\psi\sigma}\le\widetilde{\psi\rho}} \varepsilon_{\widetilde{\psi\rho},\widetilde{\psi\sigma}}\, e_{(\psi\widetilde{\sigma})'}(\alpha_1,\dots,\alpha_{m-1}).$$

Since $e_{(\psi\widetilde{\sigma})'}(\alpha_1,\dots,\alpha_{m-1}) = e_{\widetilde{\sigma}'}(\alpha_1,\dots,\alpha_{m-1})$, it follows by comparing (1) and (3) that $\varepsilon_{\widetilde{\rho},\widetilde{\sigma}} = \varepsilon_{\widetilde{\psi\rho},\widetilde{\psi\sigma}}$, as desired.

(ii) It follows from (i) that

$$\phi(a\odot b) = (-1)^{mn}\phi(a\otimes b) = (-1)^{(m+1)n}(\phi(a)\otimes\phi(b)) = \phi(a)\odot\phi(b). \quad \square$$

If $a_0 = b_0 = 1$ and $m, n \ge k$, then it follows from Theorem 2.1 and Proposition 2.2(ii) that the coefficient of X^k in $a \odot b$ is an element of $\mathbb{Z}[a_1,\dots,a_k,b_1,\dots,b_k]$ which is independent of m and n. Therefore the

binary operation $\odot$ may be extended to the set of power series with constant term 1 over the ring $\mathbb{Z}[a_1, a_2, \ldots, b_1, b_2, \ldots]$. Let $a = 1 + \sum_{i=1}^{\infty} a_i X^i$ and $T_k(a) = 1 + \sum_{i=1}^{k} a_i X^i$. If $b = 1 + \sum_{i=1}^{\infty} b_i X^i$, then we may define $a \odot b$ by $T_k(a \odot b) = T_k(T_k(a) \odot T_k(b))$ for $k = 1, 2, \ldots$. This gives the multiplication in the Witt ring of $\mathbb{Z}[a_1, a_2, \ldots, b_1, b_2, \ldots]$ (see [K73]). Many properties involving $\odot$-products of power series can be readily deduced from properties of $\otimes$-products of polynomials. Proposition 2.2 may be used to show that the Witt ring $W(R)$ is semi-simple if R is an integral domain of characteristic zero (because $a \otimes a \otimes \cdots \otimes a = 1$ implies that $a = 1$). Henceforth we shall consider polynomials, and not power series, and we revert to our original notation where a and b are polynomials of degrees m and n respectively.

Given the conventions that a non-zero constant polynomial has degree 0 and a non-zero ring element raised to the power zero is 1, it follows that $a \otimes b_0 = b_0^m$. It is straightforward to check that $a \otimes X^n = a_m^n X^{mn}$ and, if $\beta \neq 0$, that $a \otimes (X - \beta) = \beta^m a(X/\beta)$.

THEOREM 2.3. *Let R be an integral domain (with unity). Then the set $R[X]^*$, of non-zero polynomials, is a commutative 'semi-ring' (with unity) with addition corresponding to polynomial multiplication, and multiplication corresponding to $\otimes$. Furthermore, the map $\rho : R[X]^* \to R[X]^*$ defined by*

$$(a\rho)(X) = (-X)^{\deg(a)} a(1/X) = (-1)^{\deg(a)} \sum_{i=0}^{\deg(a)} a_i X^{\deg(a)-i}$$

satisfies $\rho^3 = \rho$ and the restriction of ρ to the sub-semi-ring of polynomials with non-zero constant terms is an automorphism of order 2.

Proof. The term 'semi-ring', means that all the ring axioms hold except possibly for the existence of additive inverses. To prove that $R[X]^*$ is a commutative semi-ring it suffices to prove for $a, b, c \in R[X]^*$ that $a \otimes b = b \otimes a$, $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ and $a \otimes (bc) = (a \otimes b)(a \otimes c)$. Let $\gamma_1, \ldots, \gamma_p$ be the roots of c. The associative law holds as

$$(a \otimes b) \otimes c = (a_m^n b_n^m)^p c_p^{mn} \prod_{i,j,k} (X - (\alpha_i \beta_j)\gamma_k),$$

and this equals

$$a \otimes (b \otimes c) = a_m^{np}(b_n^p c_p^n)^m \prod_{i,j,k}(X - \alpha_i(\beta_j\gamma_k)).$$

The commutative and distributive laws are also easily verified. Note that 1 is the additive identity, and $X-1$ is the multiplicative identity for the semi-ring.

It is not hard to see that $S = \{a \in R[X]^* \mid a_0 \neq 0\}$ is a sub-semi-ring. Also $\rho^3 = \rho$ and $\deg a\rho \leq \deg a$ with equality if and only if $a \in S$. Since $S\rho = S$, ρ defines a bijection of S of order 2. If $a, b \in R[X]^*$, then $(a\rho)(b\rho) = (ab)\rho$ since

$$(a\rho)(b\rho) = (-X)^m a(1/X)(-X)^n b(1/X) = (-X)^{m+n}(ab)(1/X) = (ab)\rho.$$

If $a, b \in S$, we show that $(a \otimes b)\rho = (a\rho) \otimes (b\rho)$. In this case the roots α_i and β_j are non-zero, and hence

$$(a\rho)(X) = (-1)^m a_0 \prod_{i=1}^{m}(X - \alpha_i^{-1}) \quad \text{and} \quad (b\rho)(X) = (-1)^n b_0 \prod_{j=1}^{n}(X - \beta_j^{-1}).$$

Therefore

$$(a\rho) \otimes (b\rho) = a_0^n b_0^m \prod_{i,j}(X - \alpha_i^{-1}\beta_j^{-1}).$$

However, $(a \otimes b)(0) = (-1)^{mn} a_0^n b_0^m$ and so

$$(a \otimes b)\rho = a_0^n b_0^m \prod_{i,j}(X - (\alpha_i\beta_j)^{-1}) = (a\rho) \otimes (b\rho)$$

and ρ restricts to an involutory automorphism of S as claimed. □

Note that ρ does not extend to the Witt ring. Let $a, b \in R[X]^*$ and write $a = X^r\overline{a}$ and $b = X^s\overline{b}$ where $\overline{a}, \overline{b} \in S$. Then

$$(a \otimes b)\rho = (X^{mn-(m-r)(n-s)}\ \overline{a} \otimes \overline{b})\rho = (-1)^{nr+ms-rs}(\overline{a} \otimes \overline{b})\rho$$

and

$$(a\rho) \otimes (b\rho) = ((-1)^r(\overline{a}\rho)) \otimes \big((-1)^s(\overline{b}\rho)\big) = (-1)^{r(n-s)+s(m-r)}\ (\overline{a}\rho \otimes \overline{b}\rho).$$

Thus $(a \otimes b)\rho = (-1)^{rs}(a\rho) \otimes (b\rho)$ and hence ρ is an endomorphism of $R[X]^*$ if $\mathrm{char}(R) = 2$.

In practise, one does not use the definition of $a \otimes b$ to compute the tensor product of polynomials. If a and b are monic polynomials and A and B denote their respective companion matrices, then $a \otimes b = \det(XI - A \otimes B)$ provides a practical method to compute $a \otimes b$. A variant of this method, with lower time complexity, is described in [G95]. This fast method is particularly useful for computing in the algebraic closure of a finite field (see [G96]).

3. Factoring $a \otimes b$ into irreducibles

Given $a, b \in \mathbb{Z}_{m,n}[X]$, it is shown in Theorem 3.1 that $a \otimes b \in \mathbb{Z}_{m,n}[X]$ is irreducible. This section is concerned with the factorization of tensor products in $R[X]$, where R is a unique factorization domain. Consider an evaluation homomorphism $\psi\colon \mathbb{Z}_{m,n} \to R$. Now ψ is determined by the values of $a_i\psi$ and $b_j\psi$ in R (we shall assume that $1\psi = 1$), and ψ gives rise to a homomorphism $\mathbb{Z}_{m,n}[X] \to R[X]$, which we also call ψ, that fixes X. Although $a \otimes b \in \mathbb{Z}_{m,n}[X]$ is irreducible, $a\psi \otimes b\psi \in R[X]$ may be reducible. We shall use the notation a_i, b_j to denote (indeterminant) elements of $\mathbb{Z}_{m,n}$, and also to denote elements of R (identified with $a_i\psi, b_j\psi$). One can determine from the context whether a_i, b_j is an element of $\mathbb{Z}_{m,n}$ or R.

THEOREM 3.1. *If $a, b \in \mathbb{Z}_{m,n}[X]$ have degrees $m, n \geq 1$ respectively, then $a \otimes b$ is irreducible over $\mathbb{Z}_{m,n}$.*

Proof. It suffices to prove that for $m, n \geq 1$ there is a commutative ring R and polynomials f and g over R, of degrees m and n respectively, such that $f \otimes g$ is irreducible over R. We shall assume, without loss of generality, that $1 < m \leq n$.

Let $\mathbb{Q}_r$ denote the rth cyclotomic field, and let Φ_r denote the rth cyclotomic polynomial of degree $\phi(r)$, where ϕ is Euler's phi-function. We shall choose r and s so that $\gcd(r, s) = 1$, and note that $\Phi_r \otimes \Phi_s = \Phi_{rs}$. Let $r = p_1^{k_1+1} \cdots p_t^{k_t+1}$ and $m = p_1^{k_1} \cdots p_t^{k_t}$ where the p_i are distinct primes. By Dirichlet's Theorem we may choose a prime s congruent to 1 modulo n and different to $p_1, \ldots, p_t$. Then $\gcd(r, s) = 1$, and $\mathbb{Q}_{rs}$ is the compositum $\mathbb{Q}_r\mathbb{Q}_s$.

Since m divides $\phi(r)$ there is a subfield $\mathbb{K}_m$ of $\mathbb{Q}_r$ satisfying $|\mathbb{Q}_r : \mathbb{K}_m| = m$. Similarly, let $\mathbb{K}_n$ be a subfield of $\mathbb{Q}_s$ satisfying $|\mathbb{Q}_s : \mathbb{K}_n| = n$.

Now $\mathrm{Gal}(\mathbb{Q}_r : \mathbb{Q})$ acts regularly on the roots of Φ_r, and the subgroup $\mathrm{Gal}(\mathbb{Q}_r : \mathbb{K}_m)$ permutes the roots in orbits of length m, hence Φ_r equals $f_1 \cdots f_{\phi(r)/m}$ where each f_i is irreducible over $\mathbb{K}_m$ of degree m. Similarly, $\Phi_s = g_1 \cdots g_{\phi(s)/n}$ where each g_j is irreducible over $\mathbb{K}_n$ of degree n. The following principle may be used to show that $|\mathbb{Q}_{rs} : \mathbb{K}_m\mathbb{K}_n| = mn$: if $\mathbb{K}, \mathbb{L}$ are fields such that $\mathbb{K} : \mathbb{K} \cap \mathbb{L}$ is Galois, then $\mathbb{KL} : \mathbb{L}$ is Galois and $|\mathbb{KL} : \mathbb{L}| = |\mathbb{K} : \mathbb{K} \cap \mathbb{L}|$. Therefore $\Phi_{rs} = h_1 \cdots h_{\phi(rs)/mn}$ where each h_k is irreducible over $\mathbb{K}_m\mathbb{K}_n$ of degree mn. It follows from

$$\prod_{k=1}^{\phi(rs)/mn} h_k = \Phi_{rs} = \Phi_r \otimes \Phi_s = \prod_{i=1}^{\phi(r)/m} \prod_{j=1}^{\phi(s)/n} f_i \otimes g_j$$

that each $f_i \otimes g_j$ equals some h_k. This completes the proof as $\deg(f_i) = m$, $\deg(g_j) = n$ and $f_i \otimes g_j$ is irreducible over $\mathbb{K}_m\mathbb{K}_n$. □

The following notation will hold throughout this section: R is a unique factorization domain, $\mathbb{F}$ is its field of fractions, and $\overline{\mathbb{F}}$ is an algebraic closure of $\mathbb{F}$. Let $a, b \in R[X]$ and consider how $a \otimes b$ factors into irreducible factors over R. Since $(fg) \otimes h = (f \otimes h)(g \otimes h)$, we shall assume that a and b are irreducible over R. By Gauss' Lemma, the irreducible factors of $a \otimes b$ are the same (up to constant multiples) as those over $\mathbb{F}$. We shall assume henceforth that a and b are monic and irreducible over $\mathbb{F}$. As a shorthand we write $a = m_{\alpha/\mathbb{F}}$, $b = m_{\beta/\mathbb{F}}$ where the notation $m_{\alpha/\mathbb{F}}$ denotes the minimum polynomial of α over $\mathbb{F}$.

LEMMA 3.2. *Let $\alpha, \beta \in \overline{\mathbb{F}}^\times$, and let $m_{\alpha/\mathbb{F}}, m_{\beta/\mathbb{F}}$ denote the minimum polynomials of α, β over $\mathbb{F}$, respectively. The following are necessary conditions for $m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}}$ to be irreducible over $\mathbb{F}$:*
(i) $|\mathbb{F}(\alpha\beta) : \mathbb{F}| = mn$,
(ii) $m_{\beta/\mathbb{F}}$ *is irreducible over* $\mathbb{F}(\alpha)$, *and* $m_{\alpha/\mathbb{F}}$ *is irreducible over* $\mathbb{F}(\beta)$,
(iii) $\mathbb{F}(\alpha) \cap \mathbb{F}(\beta) = \mathbb{F}$,
(iv) $|\mathbb{F}(\alpha, \beta) : \mathbb{F}(\alpha)| = n$ *and* $|\mathbb{F}(\alpha, \beta) : \mathbb{F}(\beta)| = m$,
(v) $\mathbb{F}(\alpha)\mathbb{F}(\beta) = \mathbb{F}(\alpha, \beta) = \mathbb{F}(\alpha\beta)$ *and* $\mathbb{F}(\alpha, \beta) \cong \mathbb{F}(\alpha) \otimes_{\mathbb{F}} \mathbb{F}(\beta)$.
Condition (i) is also sufficient.

Proof. Consider Figure 1 below. Let $D = \mathbb{F}(\alpha) \cap \mathbb{F}(\beta)$ and $d = |D : \mathbb{F}|$. Since $m_{\beta/\mathbb{F}}$ is irreducible over $\mathbb{F}$ of degree n, $|\mathbb{F}(\beta) : \mathbb{F}| = n$ and similarly $|\mathbb{F}(\alpha) : \mathbb{F}| = m$. Therefore $|\mathbb{F}(\alpha) : D| = m/d$ and $|\mathbb{F}(\beta) : D| = n/d$. Since $m_{\alpha/\mathbb{F}(\beta)}$ divides $m_{\alpha/D}$, it follows that

$$|\mathbb{F}(\alpha,\beta) : \mathbb{F}(\beta)| = \deg m_{\alpha/\mathbb{F}(\beta)} \leq \deg m_{\alpha/D} = |\mathbb{F}(\alpha) : D| = m/d,$$

and similarly $|\mathbb{F}(\alpha,\beta) : \mathbb{F}(\alpha)| \leq n/d$.

As $\alpha\beta$ is a root of $m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}}$, it follows that $m_{\alpha\beta/\mathbb{F}}$ divides $m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}}$. Thus $m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}}$ is irreducible if and only if $\deg m_{\alpha\beta/\mathbb{F}} = mn$, or equivalently $|\mathbb{F}(\alpha\beta) : \mathbb{F}| = mn$. Hence (i) is both necessary and sufficient.

Suppose henceforth that $m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}}$ is irreducible. It follows from Figure 1 that

$$mn = |\mathbb{F}(\alpha\beta) : \mathbb{F}| \leq |\mathbb{F}(\alpha,\beta) : \mathbb{F}| \leq (m/d)(n/d)d = mn/d.$$

Therefore $d = 1$, $\mathbb{F}(\alpha)\mathbb{F}(\beta) = \mathbb{F}(\alpha,\beta) = \mathbb{F}(\alpha\beta)$, $|\mathbb{F}(\alpha,\beta) : \mathbb{F}(\alpha)| = n$ and $|\mathbb{F}(\alpha,\beta) : \mathbb{F}(\beta)| = m$. To conclude the proof, we note that the $\mathbb{F}$-algebra homomorphism $\mathbb{F}(\alpha) \otimes_{\mathbb{F}} \mathbb{F}(\beta) \to \mathbb{F}(\alpha,\beta)$ given by $\alpha \otimes 1 \mapsto \alpha$ and $\beta \otimes 1 \mapsto \beta$ is an isomorphism (as the domain and the codomain have dimension mn).□

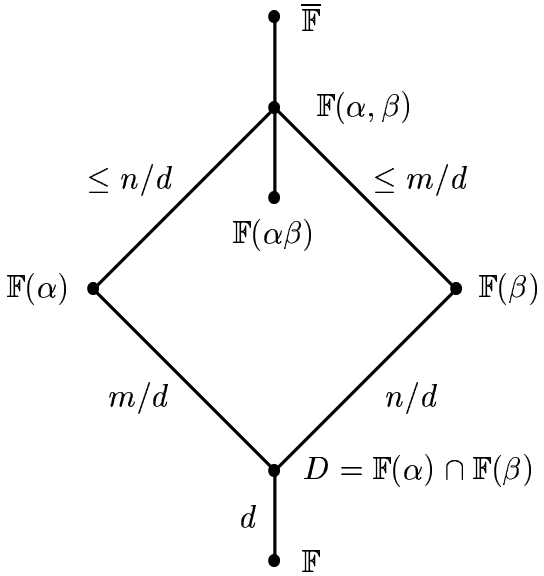

Figure 1. Subfields of $\mathbb{F}(\alpha,\beta)$ and degrees of field extensions

LEMMA 3.3. *(i) The characteristic polynomial of the $\mathbb{F}$-algebra homomorphism $\mathbb{F}(\alpha) \otimes \mathbb{F}(\beta) \to \mathbb{F}(\alpha) \otimes \mathbb{F}(\beta) : x \mapsto x(\alpha \otimes \beta)$ is $m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}}$.*
(ii) The $\mathbb{F}$-algebra homomorphism $\mathbb{F}(\alpha, \beta) \to \mathbb{F}(\alpha, \beta) : x \mapsto x\alpha\beta$ has characteristic polynomial $m_{\alpha\beta/\mathbb{F}}^{|\mathbb{F}(\alpha,\beta):\mathbb{F}(\alpha\beta)|}$.
(iii) If $|\mathbb{F}(\alpha) : \mathbb{F}|\,|\mathbb{F}(\beta) : \mathbb{F}| = |\mathbb{F}(\alpha, \beta) : \mathbb{F}|$, then $\mathbb{F}(\alpha) \otimes \mathbb{F}(\beta) \to \mathbb{F}(\alpha, \beta)$ given by $\alpha \otimes 1 \mapsto \alpha$ and $1 \otimes \beta \mapsto \beta$ is an $\mathbb{F}$-algebra isomorphism and $m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}} = m_{\alpha\beta/\mathbb{F}}^{|\mathbb{F}(\alpha,\beta):\mathbb{F}(\alpha\beta)|}$.

Proof. Both (i) and (ii) follow from the fact that the characteristic polynomial of the map $\mathbb{F}(\gamma) \to \mathbb{F}(\gamma)$ given by $x \mapsto x\gamma$ is $m_{\gamma/F}$. The map given in part (iii) is a surjective homomorphism, and by comparing dimensions, it must be an isomorphism. This isomorphism shows that the maps in (i) and (ii) are similar and hence have equal characteristic polynomials. That is, $m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}} = m_{\alpha\beta/\mathbb{F}}^{|\mathbb{F}(\alpha,\beta):\mathbb{F}(\alpha\beta)|}$. □

THEOREM 3.4. *Let $\alpha, \beta \in \overline{\mathbb{F}}$. Let $m_{\alpha/\mathbb{F}}$ be separable over $\mathbb{F}$, and suppose that it factors over $\mathbb{F}(\beta)$ as $m_{\alpha/\mathbb{F}} = \prod_{i=1}^{d} m_{\alpha_i/\mathbb{F}(\beta)}$. Then*

$$m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}} = \prod_{i=1}^{d} m_{\alpha_i\beta/\mathbb{F}}^{|\mathbb{F}(\alpha_i,\beta):\mathbb{F}(\alpha_i\beta)|} \quad \textit{and} \quad \mathbb{F}(\alpha) \otimes_{\mathbb{F}} \mathbb{F}(\beta) \cong \bigoplus_{i=1}^{d} \mathbb{F}(\alpha_i, \beta)$$

Furthermore, the polynomials $m_{\alpha_i/\mathbb{F}(\beta)}$ are distinct and the fields $\mathbb{F}(\alpha_i, \beta)$, $i = 1, \ldots, d$, are separable over $\mathbb{F}(\beta)$.

Proof. Since $m_{\alpha/\mathbb{F}}$ is separable, the polynomials $m_{\alpha_i/\mathbb{F}(\beta)}$ are distinct. Hence it follows from [HB82, II, 1.4(a)] that

$$\mathbb{F}(\alpha) \otimes_{\mathbb{F}} \mathbb{F}(\beta) \cong \bigoplus_{i=1}^{d} \mathbb{F}(\alpha_i, \beta),$$

where the $\mathbb{F}(\alpha_i, \beta)$ are separable over $\mathbb{F}(\beta)$. A precise description of the above isomorphism is obtained from the proofs of II, 1.4(a) and (c) in [HB82]. The images of $\alpha \otimes 1$ and $1 \otimes \beta$ in $\mathbb{F}(\alpha_i, \beta)$ are α_i and β respectively; and hence $\alpha \otimes \beta$ has image $\alpha_i\beta$. The factorization of $m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}}$ now follows from Lemma 3.3(i) and (ii). □

THEOREM 3.5. *Let $\alpha, \beta \in \overline{\mathbb{F}}$ and $D = \mathbb{F}(\alpha) \cap \mathbb{F}(\beta)$. Suppose that $m_{\alpha/\mathbb{F}}$ equals $\prod_{i=1}^{d} m_{\alpha_i/\mathbb{F}(\beta)}$ and $\mathbb{F}(\alpha) : \mathbb{F}$ is Galois. Then d equals $|D : \mathbb{F}|$ and divides $\gcd(|\mathbb{F}(\alpha) : \mathbb{F}|, |\mathbb{F}(\beta) : \mathbb{F}|)$, and $m_{\alpha_i/\mathbb{F}(\beta)}$ equals $m_{\alpha_i/D}$ and has degree $|\mathbb{F}(\alpha, \beta) : \mathbb{F}(\beta)| = |D(\alpha) : D|$ for $i = 1, \ldots, d$.*

Proof. Since $\mathbb{F}(\alpha) : \mathbb{F}$ is Galois, $\mathbb{F}(\alpha_i) = \mathbb{F}(\alpha)$ and hence $\mathbb{F}(\alpha_i, \beta) = \mathbb{F}(\alpha, \beta)$ for each i. We show below that d equals $|D : \mathbb{F}|$.

Now $D(\alpha) = \mathbb{F}(\alpha)$ and $D(\alpha) : D$ is Galois. Furthermore, $D(\alpha, \beta) : D(\beta)$ is Galois with group isomorphic, via restriction, to $\mathrm{Gal}(D(\alpha) : D)$. Now $\mathrm{Gal}(\mathbb{F}(\alpha) : \mathbb{F})$ acts regularly on the roots of $m_{\alpha/\mathbb{F}}$ and hence so too does the subgroup $\mathrm{Gal}(D(\alpha) : D)$. If Δ_i is the orbit of a root α_i of $m_{\alpha/\mathbb{F}}$ under $\mathrm{Gal}(D(\alpha) : D)$, then $|\Delta_i| = |D(\alpha) : D|$. Hence $m_{\alpha/\mathbb{F}}$ factors over D into $|D : \mathbb{F}|$ irreducible polynomials each of degree $|D(\alpha) : D|$. Moreover, $\Delta_i\beta$ is the orbit of $\alpha_i\beta$ under $\mathrm{Gal}(D(\alpha, \beta) : D(\beta))$ so $m_{\alpha_i\beta/D(\beta)} = m_{\alpha_i/D} \otimes (X - \beta)$ and thus $m_{\alpha_i/D} = m_{\alpha_i/D(\beta)}$. Since $D(\beta) = \mathbb{F}(\beta)$ it follows that $d = |D : \mathbb{F}|$ and $m_{\alpha_i/D(\beta)}$ has degree

$$|D(\alpha_i) : D| = |D(\alpha) : D| = |\mathbb{F}(\alpha, \beta) : \mathbb{F}(\beta)|.$$

It is clear that d divides $\gcd(|\mathbb{F}(\alpha) : \mathbb{F}|, |\mathbb{F}(\beta) : \mathbb{F}|)$. □

It is worth noting that the polynomials $m_{\alpha_i\beta/\mathbb{F}}$, $i = 1, \ldots, d$, appearing in Theorem 3.4 need not be distinct even though the $m_{\alpha_i/\mathbb{F}(\beta)}$ are distinct. For example, if $\alpha = \beta$ is a primitive fifth root of unity and $\mathbb{F} = \mathbb{Q}$, then $d = 4$ and the values of $m_{\alpha_i\beta/\mathbb{F}}$ are $X - 1, m_{\alpha/\mathbb{F}}, m_{\alpha/\mathbb{F}}$ and $m_{\alpha/\mathbb{F}}$.

LEMMA 3.6. *Let $\alpha, \beta \in \overline{\mathbb{F}}$ and let A and B denote the set of roots of $m_{\alpha/\mathbb{F}}$ and of $m_{\beta/\mathbb{F}}$ respectively. Suppose that $\mathbb{F}(\alpha)$ and $\mathbb{F}(\beta)$ are Galois over $\mathbb{F}$ and $m_{\alpha/\mathbb{F}}$ is irreducible over $\mathbb{F}(\beta)$. Then $\mathbb{F}(\alpha) \otimes_{\mathbb{F}} \mathbb{F}(\beta)$ is isomorphic to the field $\mathbb{F}(\alpha, \beta)$. Furthermore, $\mathbb{F}(\alpha, \beta) : \mathbb{F}$ is Galois with group isomorphic (as a permutation group) to $\mathrm{Gal}(\mathbb{F}(\alpha) : \mathbb{F}) \times \mathrm{Gal}(\mathbb{F}(\beta) : \mathbb{F})$ acting on $A \times B$ with product action.*

Proof. It follows from Theorem 3.4 that $d = 1$ and $\mathbb{F}(\alpha) \otimes \mathbb{F}(\beta) \cong \mathbb{F}(\alpha, \beta)$. Then, by Theorem 3.5, $\mathbb{F}(\alpha) \cap \mathbb{F}(\beta) = \mathbb{F}$ so all of the assertions hold by [L80, VIII Theorem 5]. □

We introduce some notation used in Theorem 3.7 below. A positive integer s is called an *exponent* of a polynomial a if $a(X) = b(X^s)$ for some polynomial b. If $a \neq a_0$, then a has a *greatest exponent* denoted $\mathrm{ge}(a)$. This is a multiple of every exponent of a and equals $\gcd\{i \mid a_i \neq 0\}$. If $a \neq X^m$ or a_0 and $a = a \otimes (X - \rho)$ where $\rho \neq 0$, then the (multiplicative) order of ρ is finite and divides $\mathrm{ge}(a)$.

Given an abelian group G, let $\Omega_n(G)$ denote the subgroup $\{g \in G \mid g^n = 1\}$ of G.

THEOREM 3.7. *Suppose that* $\alpha, \beta \in \overline{\mathbb{F}}$, $\alpha, \beta \notin \mathbb{F}$ *and* $\mathbb{F}(\alpha)$ *and* $\mathbb{F}(\beta)$ *are Galois over* $\mathbb{F}$.
(*i*) *Then* $\mathbb{F}(\alpha, \beta)$ *and* $D = \mathbb{F}(\alpha) \cap \mathbb{F}(\beta)$ *are Galois over* $\mathbb{F}$, *and* $\mathrm{Gal}(\mathbb{F}(\alpha, \beta) : \mathbb{F})$ *is isomorphic to the pull-back of* $\mathrm{Gal}(\mathbb{F}(\alpha) : \mathbb{F})$ *and* $\mathrm{Gal}(\mathbb{F}(\beta) : \mathbb{F})$ *identifying* $\mathrm{Gal}(D : \mathbb{F})$.
(*ii*) *Suppose* $m_{\alpha/\mathbb{F}} = \prod_{i=1}^{d} m_{\alpha_i/D}$. *Then* $d = |D : \mathbb{F}|$ *and*

$$m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}} = \prod_{i=1}^{d} (m_{\alpha_i \beta/\mathbb{F}})^{e f_i},$$

$e = |D(\alpha, \beta) : D(\alpha\beta)|$ *and* $f_i = |D(\alpha_i \beta) : \mathbb{F}(\alpha_i \beta)|$ *for each* i. *Moreover,* e *divides* $|\Omega_g(D^\times)|$ *where* $g = \gcd(\mathrm{ge}(m_{\alpha/D}), \mathrm{ge}(m_{\beta/D}))$, f_i *divides* d *and*

$$e f_i \deg m_{\alpha_i \beta/\mathbb{F}} = (\deg m_{\alpha/\mathbb{F}})(\deg m_{\beta/\mathbb{F}})/d \quad \textit{for each} \quad i.$$

Proof. (*i*) This is a generalization of [L80, VIII Theorem 5] which is presumably known. Let $\mathbb{K}_1 = \mathbb{F}(\alpha)$ and $\mathbb{K}_2 = \mathbb{F}(\beta)$ be Galois extensions of $\mathbb{F}$ with groups G_1 and G_2 respectively. Then the compositum $\mathbb{K}_1\mathbb{K}_2 = \mathbb{F}(\alpha, \beta)$ is Galois over $\mathbb{F}$ and its group, G, is a *pull-back* of G_1 and G_2 as described below. Let $\pi_i : G \to G_i$ be the epimorphism defined by $\sigma\pi_i = \sigma|\mathbb{K}_i$. Let $N_1 = \ker(\pi_2)$ and $N_2 = \ker(\pi_1)$. Since $N_1 \cap N_2$ is trivial, the map $\theta : G \to G_1 \times G_2$ defined by $\sigma\theta = (\sigma|\mathbb{K}_1, \sigma|\mathbb{K}_2)$ is a monomorphism. It follows from the Galois correspondence (Figure 2 below)

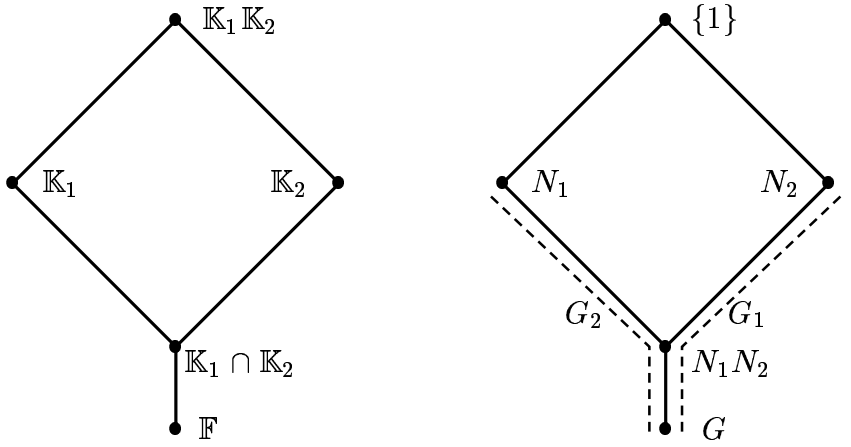

Figure 2. Galois correspondence and the pull-back $G_1 \times_\phi G_2$

that the fixed field of the normal subgroup N_1N_2 is $\mathbb{K}_1 \cap \mathbb{K}_2$, and the Galois group of $\mathbb{K}_1 \cap \mathbb{K}_2$ over $\mathbb{F}$ is $G/N_1N_2 \cong G_1/N_1^* \cong G_2/N_2^*$ where $N_i^* = \pi_i(N_i)$ is isomorphic to N_i. Furthermore, the map $\phi : G_1/N_1^* \to G_2/N_2^*$ given by $(\sigma|\mathbb{K}_1)N_1^* \mapsto (\sigma|\mathbb{K}_2)N_2^*$ for $\sigma \in G$, is a well-defined isomorphism. But G is isomorphic to $G\theta$, and a little thought shows that $G\theta$ equals the pull-back

$$G_1 \times_\phi G_2 = \{(\sigma_1, \sigma_2) \in G_1 \times G_2 \mid (\sigma_1 N_1^*)\phi = \sigma_2 N_2^*\}.$$

(*ii*) Now $D(\alpha) : D$ is Galois and $D(\alpha) \cap D(\beta) = D$, therefore $m_{\alpha/D}$ is irreducible over $D(\beta)$. Since $D(\beta) : D$ is also Galois it follows from Lemma 3.6 that $D(\alpha) \otimes D(\beta)$ is isomorphic to the field $D(\alpha, \beta)$, and $m_{\alpha/D} \otimes m_{\beta/D}$ equals $(m_{\alpha\beta/D})^e$ where e is the order of the stabilizer of $\alpha\beta$ in $\mathrm{Gal}(D(\alpha, \beta) : D)$. If the element (σ, τ) of $\mathrm{Gal}(D(\alpha) : D) \times \mathrm{Gal}(D(\beta) : D)$ stabilizes $\alpha \otimes \beta$, then there exists a $\rho \in D^\times$ such that $\alpha\sigma = \rho\alpha$ and $\beta\tau = \rho^{-1}\beta$. The map from the stabilizer of $\alpha \otimes \beta$ to $D^\times$ given by $(\sigma, \tau) \mapsto \rho$ is a monomorphism, since if $\rho = 1$ then both σ and τ are the identity automorphism. The image of this homomorphism is cyclic of order e. By the remarks preceding this theorem e divides $g = \gcd(\mathrm{ge}(m_{\alpha/D}), \mathrm{ge}(m_{\beta/D}))$ and hence divides $|\Omega_g(D^\times)|$.

By Theorem 3.5, $d = |D : \mathbb{F}|$. By Theorem 3.4

$$m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}} = \prod_{i=1}^{d} m_{\alpha_i\beta/\mathbb{F}}^{|\mathbb{F}(\alpha_i,\beta):\mathbb{F}(\alpha_i\beta)|} = \prod_{i=1}^{d} m_{\alpha_i\beta/\mathbb{F}}^{e|D(\alpha_i\beta):\mathbb{F}(\alpha_i\beta)|}$$

since $e = |D(\alpha, \beta) : D(\alpha\beta)| = |\mathbb{F}(\alpha_i, \beta) : D(\alpha_i\beta)|$ for each i. The remaining claims of the theorem are immediate upon comparing degrees of field extensions. □

Suppose that $\mathbb{F}(\alpha,\beta):\mathbb{F}$ is *cyclic* (that is, is Galois with a cyclic group). Then $\mathbb{F}(\alpha):\mathbb{F}$ and $\mathbb{F}(\beta):\mathbb{F}$ are also cyclic and it follows from Theorem 3.7(i) that $|\mathbb{F}(\alpha,\beta):\mathbb{F}(\alpha)|$ and $|\mathbb{F}(\alpha,\beta):\mathbb{F}(\beta)|$ are coprime (otherwise $\mathbb{F}(\alpha,\beta):\mathbb{F}(\alpha)\cap\mathbb{F}(\beta)$ is not cyclic). Thus $d=\gcd(m,n)$ where $m=\deg m_{\alpha/\mathbb{F}}$ and $n=\deg m_{\beta/\mathbb{F}}$, and by Theorem 3.7($ii$), $ef_i\deg m_{\alpha_i\beta/\mathbb{F}}=\operatorname{lcm}(m,n)$ holds for $i=1,\dots,d$. It follows from Theorems 3.4 and 3.7(ii) that

$$\mathbb{F}_{q^m}\otimes_{\mathbb{F}}\mathbb{F}_{q^n}\cong\bigoplus_{i=1}^{\gcd(m,n)}\mathbb{F}_{q^{\operatorname{lcm}(m,n)}}$$

(compare with [HB82, 1.4(b)]). Moreover, g divides $\gcd(m/d,n/d)=1$ so $g=e=1$ and $m_{\alpha/\mathbb{F}}\otimes m_{\beta/\mathbb{F}}$ is irreducible if and only if $d=1$.

LEMMA 3.8. *Let $\mathbb{F}(\alpha)$ and $\mathbb{F}(\beta)$ be Galois over $\mathbb{F}$, and suppose P is a normal p-subgroup of $\operatorname{Gal}(\mathbb{F}(\alpha,\beta):\mathbb{F})$ such that every element of order p in P fixes α or β. Then $|P|$ divides $\deg m_{\alpha\beta/\mathbb{F}}$.*

Proof. Since $G=\operatorname{Gal}(\mathbb{F}(\alpha,\beta):\mathbb{F})$ acts transitively on the roots of $m_{\alpha\beta/\mathbb{F}}$, and the orbits of the normal subgroup P have equal size, it suffices to show that one orbit has $|P|$ elements. This follows if each non-trivial $\sigma\in P$ does not fix $\alpha\beta$. Assume without loss of generality that σ has order p, and hence by our assumption $\alpha\sigma=\alpha$ or $\beta\sigma=\beta$. Assume that $\beta\sigma=\beta$. Then $\alpha\sigma\neq\alpha$, otherwise σ has order 1, not p. Thus $(\alpha\beta)\sigma\neq\alpha\beta$, and assuming that $\alpha\sigma=\alpha$ gives the same conclusion. □

More can be said about the integers f_i in Theorem 3.7(ii) in the case when $\operatorname{Gal}(\mathbb{F}(\alpha,\beta):\mathbb{F})$ is cyclic.

PROPOSITION 3.9. *Suppose $\alpha,\beta\in\overline{\mathbb{F}}$, $\mathbb{F}(\alpha,\beta):\mathbb{F}$ is cyclic and $m=\deg m_{\alpha/\mathbb{F}}$ and $n=\deg m_{\beta/\mathbb{F}}$. Suppose that p is prime, and let $|m|_p$ denote the largest power of p dividing m. If $m_{\alpha/\mathbb{F}}=\prod_{i=1}^{d}m_{\alpha_i/D}$, where $D=\mathbb{F}(\alpha)\cap\mathbb{F}(\beta)$ and $|m|_p\neq|n|_p$, then $|D(\alpha,\beta):D(\alpha\beta)|=1$, and for each i, $|f_i|_p=1$ and $\max\{|m|_p,|n|_p\}=|\deg m_{\alpha_i\beta/\mathbb{F}}|_p$. In particular, if $|m|_p\neq|n|_p$ for each prime divisor p of mn, then $m_{\alpha/\mathbb{F}}\otimes m_{\beta/\mathbb{F}}$ is a product of $\gcd(m,n)$ irreducible polynomials over $\mathbb{F}$ each of degree $\operatorname{lcm}(m,n)$.*

Proof. It was shown in the remarks preceding Lemma 3.8 that $D(\alpha,\beta)$ equals $D(\alpha\beta)$, $d=\gcd(m,n)$ and $f_i\deg m_{\alpha_i\beta/\mathbb{F}}=\operatorname{lcm}(m,n)$. Suppose $|m|_p\neq|n|_p$.

Without loss of generality assume $|m|_p < |n|_p$. If P_1 is the Sylow p-subgroup of $\mathrm{Gal}(\mathbb{F}(\alpha) : \mathbb{F})$ and P_2 is the Sylow p-subgroup of $\mathrm{Gal}(\mathbb{F}(\beta) : \mathbb{F})$, then the Sylow p-subgroup of $\mathrm{Gal}(\mathbb{F}(\alpha, \beta) : \mathbb{F})$ is isomorphic (by 3.7(i)) to the pull-back

$$P_1 \times_\theta P_2 = \{(\sigma_1, \sigma_2) \in P_1 \times P_2 \mid (\sigma_1 N_1)\theta = \sigma_2 N_2\},$$

where N_i is a normal subgroup of P_i ($i = 1, 2$) and $\theta\colon P_1/N_1 \to P_2/N_2$ is an isomorphism. Since $P_1 \times_\theta P_2$ is cyclic, it follows that $N_1 = \{1\}$ and $P_1 \times_\theta P_2 \cong P_2$. As any element of $P_1 \times_\theta P_2$ of order p fixes α, Lemma 3.8 shows that $|P_2|$ divides $\deg m_{\alpha_i \beta/\mathbb{F}}$ for each i. Since $|P_2| = |n|_p = |\operatorname{lcm}(m, n)|_p$, it follows from Theorem 3.7(ii) that $|f_i|_p = 1$. Hence if $|m|_p \neq |n|_p$ for each prime divisor p of $\operatorname{lcm}(m, n)$, then $f_i = 1$ and $\deg m_{\alpha_i \beta/\mathbb{F}} = \operatorname{lcm}(m, n)$ for each i. □

The main idea behind Proposition 3.9 holds more generally. Suppose that $\mathbb{F}(\alpha) : \mathbb{F}$ and $\mathbb{F}(\beta) : \mathbb{F}$ are Galois and P_1, P_2 are Sylow p-subgroups of the respective Galois groups. A Sylow p-subgroup of $\mathrm{Gal}(\mathbb{F}(\alpha, \beta) : \mathbb{F})$ is isomorphic (by Theorem 3.7(i)) to a pull-back $P_1 \times_\theta P_2$ where $\theta\colon P_1/N_1 \to P_2/N_2$ is an isomorphism. Suppose that each element (σ_1, σ_2) of order p in $P_1 \times_\theta P_2$ has $\sigma_1 = 1$ or $\sigma_2 = 1$, or equivalently lies in the subgroup $N_1 \times \{1\}$ or $\{1\} \times N_2$. Then by Lemma 3.8

$$|P_1 \times_\theta P_2| = \max\{|P_1|, |P_2|\} = |\deg m_{\alpha_i \beta/\mathbb{F}}|_p$$

and p does not divide $|D(\alpha, \beta) : D(\alpha\beta)|$ or f_i for any i.

4. ⊗-products of binomials and cyclotomic polynomials

In this section we give some examples of how $m_{\alpha/\mathbb{F}} \otimes m_{\beta/\mathbb{F}}$ factors over $\mathbb{F}$.

LEMMA 4.1. *Suppose that $\mathbb{F}$ is an arbitrary field, $a, b \in \mathbb{F}$ are non-zero, and $d = \gcd(m, n)$ where m, n are positive integers. Then*

$$(X^m - a) \otimes (X^n - b) = (X^{mn/d} - a^{n/d} b^{m/d})^d \tag{6}$$

and $(X^m - a) \otimes (X^n - b)$ is irreducible over $\mathbb{F}$ if and only if $X^m - a$ and $X^n - b$ are irreducible over $\mathbb{F}$ and $d = 1$.

Proof. Suppose first that $\mathrm{char}(\mathbb{F})$ does not divide mn. Then there exist $\zeta_m, \zeta_n \in \overline{\mathbb{F}}$ with multiplicative orders m and n respectively. Let $\alpha, \beta \in \overline{\mathbb{F}}$ be roots of $X^m - a$ and $X^n - b$ respectively. Then the roots of $X^m - a$, $X^n - b$ and $(X^m - a) \otimes (X^n - b)$ are distinct and have the form $\alpha\zeta_m^i$, $\beta\zeta_n^j$, $\alpha\beta\zeta_m^i\zeta_n^j$ respectively where $i = 1, \ldots, m$ and $j = 1, \ldots, n$. Each of the mn roots $\alpha\beta\zeta_m^i\zeta_n^j$ has multiplicity d and satisfies $(\alpha\beta\zeta_m^i\zeta_n^j)^{mn/d} = a^{n/d}b^{m/d}$ and so (6) holds. Consider now the case when $\mathrm{char}(\mathbb{F}) = p$ divides mn. Let $m = rs$ and $n = tu$ where $r = |m|_p$ and $t = |n|_p$. This case follows from the previous case by considering

$$(X^s - a^{1/r})^r \otimes (X^u - b^{1/t})^t$$

over the field $\mathbb{F}(a^{1/r}, b^{1/t})$.

Suppose that $(X^m - a) \otimes (X^n - b)$ is irreducible over $\mathbb{F}$. Then $d = 1$ and it follows from the distributive law that both $X^m - a$ and $X^n - b$ are irreducible over $\mathbb{F}$. Conversely, suppose that $X^m - a$ and $X^n - b$ are irreducible over $\mathbb{F}$ and $d = 1$. Let M and N be integers satisfying $Mm + Nn = 1$. Since $(\alpha\beta)^{Mm} = \alpha^{Mm}\beta^{1-Nn} = a^M b^{-N}\beta$, we see $\beta \in \mathbb{F}(\alpha\beta)$. Similarly, $\alpha \in \mathbb{F}(\alpha\beta)$ so $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\alpha\beta)$. Hence $|\mathbb{F}(\alpha\beta) : \mathbb{F}| = mn$ and by Lemma 3.2, the tensor product $(X^m - a) \otimes (X^n - b)$ is irreducible over $\mathbb{F}$. □

It is well-known (see [L80, VIII, Theorem 16], for example) which binomials are irreducible over $\mathbb{F}$. We remark that if $\gcd(m, n) = 1$, then the binomial $X^{mn} - c$ can be tensor factored as $(X^m - a) \otimes (X^n - b)$ where $a = c^N$, $b = c^M$ and $M, N \in \mathbb{Z}$ satisfy $Mm + Nn = 1$. This follows from (6) as $a^n b^m = c^{Mm+Nn} = c$.

Setting $a = b = 1$ in (6) shows that

$$(X^m - 1) \otimes (X^n - 1) = (X^{\mathrm{lcm}(m,n)} - 1)^{\gcd(m,n)}.$$

Now $X^m - 1 = \prod_{r|m} \Phi_r$ and $X^n - 1 = \prod_{s|n} \Phi_s$ are factorizations over $\mathbb{Q}$ into (irreducible) cyclotomic polynomials. Hence $\prod_{r|m,\, s|n} \Phi_r \otimes \Phi_s$ equals $\prod_{t|\mathrm{lcm}(m,n)} \Phi_t^{\gcd(m,n)}$ and so $\Phi_r \otimes \Phi_s$ is a product of certain Φ_t where t divides $\mathrm{lcm}(m, n)$. This factorization may be determined from the following facts:

$$\Phi_r \otimes \Phi_s = \Phi_{rs} \qquad \text{if} \qquad \gcd(r, s) = 1, \tag{7}$$

while if r and s are powers of the same prime p and $r \leq s$, then

$$\Phi_r \otimes \Phi_s = \begin{cases} (\Phi_1 \Phi_p \cdots \Phi_{r/p})^{\phi(r)} \Phi_r^{\phi(r)-r/p} & \text{if } r = s, \\ \Phi_s^{\phi(r)} & \text{if } r < s. \end{cases} \tag{8}$$

The proof of (7) is straightforward, and (8) follows by considering the equation $\rho\sigma = \tau$ where ρ, σ, τ are roots of unity of prime power order such that $|\rho|$ properly divides $|\sigma|$ (and so $|\sigma| = |\tau|$).

Let $r = r_1 \cdots r_k$ and $s = s_1 \cdots s_k$, where r_i and s_i are powers of p_i, and $p_1, \ldots, p_k$ are distinct primes. A formula for the factorization over $\mathbb{Q}$ of $\Phi_r \otimes \Phi_s$ into irreducible factors is quite complicated if $r_i = s_i$ for some i. Suppose that $r_i \neq s_i$ for each i. Then

$$\Phi_r \otimes \Phi_s = \bigotimes_{i=1}^{k} \Phi_{r_i} \otimes \Phi_{s_i} = \bigotimes_{i=1}^{k} \Phi_{\mathrm{lcm}(r_i,s_i)}^{\phi(\gcd(r_i,s_i))} = \Phi_{\mathrm{lcm}(r,s)}^{\phi(\gcd(r,s))}$$

(see Proposition 3.9). More generally, if $t = t_1 \cdots t_k$ where $t_i = \mathrm{lcm}(r_i, s_i)$ when $r_i \neq s_i$, and t_i is a proper divisor of r_i when $r_i = s_i$, then the largest power of Φ_t dividing $\Phi_r \otimes \Phi_s$ is $\phi(\gcd(r, s))$.

Acknowledgments

I am most grateful to L.G. Kovács for comments and discussions which, amongst other things, led to an improved version of Theorem 3.4. I would like to thank David Easdown for many suggestions including a shorter proof of Theorem 2.1. I am grateful to the referee and the others who commented on earlier drafts.

References

[BB93] J.V. Brawley and D. Brown, 'Composed products and module polynomials over finite fields', *Discrete Math.* **117** (1993), 41–56.

[BC87] J.V. Brawley and L. Carlitz, 'Irreducibles and the composed product for polynomials over a finite field', *Discrete Math.* **65** (1987), 115–139.

[G96] S.P. Glasby, 'Computing in the algebraic closure of a finite field', (Research Report 96-14, University of Sydney).

[G95] ————, 'Tensor products of polynomials', (Research Report 95-04, University of Sydney).

[HB82] B. Huppert, N. Blackburn, *Finite groups II* (Springer, Berlin, 1982).

[K73] Donald Knutson, *λ-rings and the representation theory of the symmetric group*, Lecture Notes in Math. 308 (Springer, Berlin, 1973).

[L80] Serge Lang, *Algebra* (Addison–Wesley, 1980).

[LO97] C.R. Leedham-Green and E.A. O'Brien, 'Recognising tensor products of matrix groups', *Internat. J. Algebra and Comput. (5)* **7** (1997), 541–559.

[M95] I.G. Macdonald, *Symmetric functions and Hall polynomials, 2nd Ed.* (Clarendon, Oxford, 1995).

[S99] R. Schwingel, 'The tensor product of polynomials', *Experiment. Math. (4)* **8** (1999), 395–397.

Department of Mathematics

Central Washington University

WA 98926-7424, USA

E-mail: glasbys@cwu.edu