Finite Fields and Their Applications 16 (2010) 163–174

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On different families of invariant irreducible polynomials over $\mathbb{F}_2$

Jean Francis Michon, Philippe Ravache *

Université de Rouen, LITIS EA 4108, BP 12 – 76801 Saint-Étienne du Rouvray cedex, France

ARTICLE INFO

Article history:
Received 7 October 2009
Revised 4 January 2010
Available online 12 February 2010
Communicated by D. Panario

Keywords:
Irreducible polynomials
Finite fields
Permutations

ABSTRACT

Using a natural action of the permutation group $\mathfrak{S}_3$ on the set of irreducible polynomials, we attach to each subgroup of $\mathfrak{S}_3$ the family of its invariant polynomials. Enumeration formulas for the trivial subgroup and for one transposition subgroup were given by Gauss (1863) (for prime fields) [1] and Carlitz (1967) (for all finite base fields) [2]. Respectively, they allow to enumerate all irreducible and self-reciprocal irreducible polynomials. In our context, the *last* remaining case concerned the alternating subgroup $\mathfrak{A}_3$. We give here the corresponding enumeration formula restricted to $\mathbb{F}_2$ base field. We wish this will give an interesting basis for subsequent developments analogous to those of Meyn (1990) [3] and Cohen (1992) [4].

1. The action of $\mathfrak{S}_3$ on $\mathbb{P}^1$

The group of permutations of 3 elements (say 1, 2, 3) is a 6 elements non-commutative group. Its subgroups are well known:

- Three cyclic subgroups of order 2, containing respectively the transpositions (12), (23), (13). These subgroups are conjugated.
- One cyclic subgroup of order 3 generated by the “cycle” $c = (123)$. This subgroup is distinguished and called the alternating group $\mathfrak{A}_3$.

* Corresponding author. Fax: +33 (0) 2 32 95 51 87.
E-mail addresses: jean-francis.michon@litislab.fr (J.F. Michon), philippe.ravache@litislab.fr (P. Ravache).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2010.01.004

The group is generated by any set of two transpositions. For example, let us take $u = (12)$ and $v = (23)$ then $uv = c$, $vu = c^2$, and $uvu = vuv = (13)$. These relations form a presentation of $\mathfrak{S}_3$. This presentation is not unique. One finds very often in the literature:

$$U^2 = 1, \qquad V^3 = 1, \qquad UVU = V^2$$

(take $u = U$ and $uv = V$).

In the projective line over $\mathbb{F}_2$, the $\mathbb{F}_2$-rational points can be identified with the set of 3 elements:

$$\mathbb{P}^1(\mathbb{F}_2) = \big\{(0,1), (1,1), (1,0)\big\}.$$

We call these elements respectively $0, 1, \infty$.

The automorphism group of the projective line is the group $PGL_2(\mathbb{F}_2)$. Its $\mathbb{F}_2$-rational elements subset is $PGL_2(\mathbb{F}_2) = GL_2(\mathbb{F}_2)$: the group of invertible 2×2-matrices with coefficients in $\mathbb{F}_2$. $GL_2(\mathbb{F}_2)$ acts as usual on the $\mathbb{F}_2$-vector space $\mathbb{F}_2 \times \mathbb{F}_2$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

with $ad - bc = 1$. Using the projective coordinates we get the classical homographic action

$$(x:1) \to \left(\frac{ax+b}{cx+d} : 1\right) \quad \text{and} \quad \infty \to \left(\frac{a}{c} : 1\right)$$

if the denominators are $\neq 0$. When denominators are 0, we use the ∞ point in the usual way.

This article is founded on the isomorphism:

$$GL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3.$$

We easily can explicit this map. We list the elements of $GL_2(\mathbb{F}_2)$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

The corresponding projective transformations are:

$$x \to x,\ x+1,\ \frac{x}{x+1},\ \frac{1}{x},\ \frac{1}{x+1},\ \frac{x+1}{x}$$

and the corresponding permutations of the three points of the projective line are:

$$Id, \quad (01), \quad (1\infty), \quad (0\infty), \quad (01\infty), \quad (0\infty1).$$

2. $\mathfrak{S}_3$ action on irreducible polynomials of $\mathbb{F}_2[X]$

To define a left action of $\mathfrak{S}_3$ on the set

$$\mathcal{I} = \big\{P \in \mathbb{F}_2[X],\ P \text{ irreducible}\big\} \setminus \{X, X+1\}$$

(0 or 1 are not zeros of P), it is sufficient to define it for the two transpositions

$$P^{(01)} = P(X+1),$$
$$P^{(0\infty)} = X^{\deg P} P\left(\frac{1}{X}\right).$$

For ease of notation these previous operations will be written as:

$$P^{+}(X) = P(X+1),$$
$$P^{*}(X) = X^{\deg P} P\left(\frac{1}{X}\right).$$

The polynomial P^* is called the **reciprocal** of P.

Other elements actions are defined by composition. For example the cycle $(01\infty) = (0\infty) \circ (01)$ gives, using left action $P^{\sigma \circ \tau} = (P^{\tau})^{\sigma}$:

$$P^{(01\infty)} = \left(P^{+}\right)^{*}.$$

In the same way we write:

$$P^{(0\infty1)} = P^{(01)(0\infty)} = \left(P^{*}\right)^{+},$$
$$P^{(1\infty)} = P^{(01)(0\infty)(01)} = P^{(0\infty)(01)(0\infty)} = \left(\left(P^{+}\right)^{*}\right)^{+} = \left(\left(P^{*}\right)^{+}\right)^{*}.$$

We shall omit the parentheses in the sequel, like in $((P^{+})^{*})^{+} = P^{+*+}$.

We leave to the reader the easy task of verifying the coherence of the following zoology:

Definition 1. A polynomial $P \in \mathcal{I}$ is called

- **alternate** when it satisfies one of the equivalent conditions

$$P^{*+} = P \quad \Leftrightarrow \quad P^{*} = P^{+};$$

- **self-reciprocal** when $P^* = P$;
- **periodic** when $P^+ = P$;
- **median** when it satisfies one of the equivalent conditions

$$P^{+*+} = P \quad \Leftrightarrow \quad P^{+} \text{ is self-reciprocal} \quad \Leftrightarrow \quad P^{*} \text{ is periodic}.$$

The polynomial $X^2 + X + 1$ is the intersection of any two of these classes.

3. Hexagons

Definition 2. The **hexagon** of $P \in \mathcal{I}$ is the orbit of P:

$$Hex(P) = \left\{P^{\sigma} \mid \sigma \in \mathfrak{S}_3\right\} = \left\{P, P^{*}, P^{+}, P^{*+}, P^{+*}, P^{*+*} = P^{+*+}\right\}.$$

A hexagon is included in $\mathcal{I}$ and has 1, 2, 3 or 6 distinct elements. In each hexagon, all polynomials have the same degree. The degree of a hexagon is the degree of its elements. Consequently we can define the function $hex(n)$ (resp. $h_1(n)$, $h_2(n)$, $h_3(n)$, $h_6(n)$) on integers $\geqslant 2$ as the number of all hexagons (resp. 1, 2, 3, 6 element(s) hexagons) of degree n and we have

$$hex(n) = h_1(n) + h_2(n) + h_3(n) + h_6(n).$$

Our goal is to describe these orbits.

We suppose that $P \in \mathcal{I}$. The n roots of P in the algebraic closure $\overline{\mathbb{F}_2}$ are distinct and conjugated by Frobenius. We can write them

$$g, g^2, \ldots, g^{2^{n-1}}.$$

Any one of them generates the field $\mathbb{F}_{2^n}$.

3.1. 1 element hexagon

A hexagon has only one element if and only if $P = P^* = P^+$. This implies that, if g is a root of P, g^{-1} and $g+1$ are roots too. We have

$$g+1 = g^{2^k} \quad \text{and} \quad g^{-1} = g^{2^l}$$

for two integers $k, l < n$, then

$$g = g^{2^{2k}} = g^{2^{2l}}.$$

The roots of P are distinct and conjugated, then

$$g = g^{2^{2k}} \quad \Rightarrow \quad 2k = 0 \mod n,$$

and for the same reason

$$2l = 0 \mod n,$$

and so

$$k = l = 0 \mod n/2.$$

As we cannot have neither $k = 0$, nor $l = 0$, the only possibility is $k = l = n/2$. Consequently

$$g + 1 = g^{-1}$$

and $P = X^2 + X + 1$.

The only hexagon with 1 irreducible element is

$$Hex\big(X^2 + X + 1\big).$$

The function value $h_1(n)$ is 0 for $n > 2$ and $h_1(2) = 1$.

3.2. 2 elements hexagons

The orbit of P has two elements if it is invariant under the subgroup $\mathfrak{A}_3$ with 3 elements, more explicitly when

$$P^{*+} = P \quad \text{and} \quad P \neq P^*.$$

Then the orbits of the **alternate** polynomials other than $X^2 + X + 1$ are exactly the 2 elements orbits of our action of $\mathfrak{S}_3$ on $\mathbb{F}_2[X]$. If P is alternate, its orbit is

$$Hex(P) = \big\{P, P^* = P^+\big\}.$$

For example, the degree < 12 alternate polynomials are $X^2 + X + 1$ (which is also self-reciprocal), $X^3 + X + 1$, $X^3 + X^2 + 1$, $X^9 + X + 1$, $X^9 + X^8 + 1$.

Theorem 1. *The alternate polynomials are exactly the irreducible factors of the polynomials*

$$B_k(X) = X^{2^k+1} + X + 1$$

for $k \in \mathbb{N}$.

If P is alternate, then $\deg P \equiv 0 \bmod 3$ *or* $P = X^2 + X + 1$. *If* $\deg P = 3m$, *then* $P|B_m$ *or* $P|B_{2m}$.

Proof. Let g be a root of any irreducible polynomial P, then $1 + 1/g$ is a root of P^{*+}.

Let P be an irreducible factor of a B_k, then $\deg P \geqslant 2$ because 0 and 1 are not roots of B_k. Any root g of P is a root of B_k so

$$g^{2^k} = 1 + \frac{1}{g}.$$

This implies that the set of all roots of P is invariant under the map

$$T : g \to 1 + \frac{1}{g}$$

(defined on $\overline{\mathbb{F}_{2^n}} \setminus \{0, 1\}$), then $P^* = P^+$ and P is alternate.

Reciprocally, if P is alternate and g any of its roots, then

$$g^{2^k} = 1 + \frac{1}{g}$$

for some integer $0 \leqslant k < n = \deg P$. Consequently $P|B_k$.

The transformation T has order 3 and permutes the roots of P because P is alternate. If $\deg P > 3$, no root of P can be fixed by this transformation because in this case we would have

$$g = 1 + \frac{1}{g}$$

and g would be a root of the irreducible $X^2 + X + 1$, which is a contradiction. Consequently the number of roots of P is multiple of 3,

$$\deg P = n \equiv 0 \mod 3.$$

Because $T^3 = I$, we have

$$g^{2^{3k}} = g.$$

This implies that g is an element of the field $\mathbb{F}_{2^{3k}}$ so, if $\deg P = n$

$$\mathbb{F}_{2^n} \subseteq \mathbb{F}_{2^{3k}}.$$

Then

$$3k = 0 \mod n$$

and the bound on k above gives $k = n/3$ or $k = 2n/3$. $\square$

The preceding theorem leads to

Definition 3. Let P be an irreducible alternate polynomial of degree $3m$. If $P|B_m$ we say that the **type** of P is 1. If $P|B_{2m}$ we say that its type is 2.

We don't need to define the type of $P = B_0$.

Proposition 1. *P and P^* have distinct types.*

Proof. Let P be an irreducible alternate polynomial of type 1. The reciprocal P^* is also irreducible alternate of the same degree. Suppose $\deg P = 3m$, then $P|B_m$ and let g be a root of P. We have

$$g^{2^m} = 1 + \frac{1}{g}.$$

Then $h = g^{-1}$ is a root of P^* and

$$\begin{aligned} h^{-2^m} &= 1 + h, \\ h^{2^m} &= \frac{1}{1+h}, \\ h^{2^{2m}} &= \left(\frac{1}{1+h}\right)^{2^m} = \frac{1}{1+h^{2^m}} = 1 + \frac{1}{h}, \end{aligned}$$

hence $B_{2m}(h) = 0$, so $P^*|B_{2m}$.

The demonstration for a type 2 polynomial follows the same lines. □

For example $P = B_1 = X^3 + X + 1$ is alternate. Then $P^* = X^3 + X^2 + 1$ is a factor of

$$B_2 = \left(X^2 + X + 1\right)\left(X^3 + X^2 + 1\right).$$

Proposition 1 implies the following:

Corollary 1. *Among all the alternate polynomials of degree $3m$, half of them divides B_m, while the other half divides B_{2m}.*

Proposition 2. *B_k has no multiple roots.*

Proof. We have $B_k(X) = X^{2^k+1} + X + 1$ and its derivative $B_k'(X) = X^{2^k} + 1 = (X+1)^{2^k}$. Since $B_k(1) \neq 0$ then $B_k(X)$ and $B_k'(X)$ have no common root so B_k has no multiple roots. □

Proposition 3. *$(X^2 + X + 1)|B_k$ if and only if k is even.*

Proof. Let α be a root of $X^2 + X + 1$ then $\alpha^3 = 1$. We have $2^k + 1 = (-1)^k + 1$. If k is even $B_k(\alpha) = \alpha^2 + \alpha + 1 = 0$, and if k is odd $B_k(\alpha) = \alpha$. □

Theorem 2. *Let P be an irreducible polynomial of degree $3m$ then $P|B_k$ if and only if the three conditions are fulfilled*:

- *P is alternate*;
- *$m|k$*;
- *$\frac{k}{m} \bmod 3$ is equal to the type of P.*

Proof. We prove first that the conditions are necessary.

We know from Theorem 1 that P is alternate. Using the same arguments as above, all the roots of B_k are in $\mathbb{F}_{2^{3k}}$, and the smallest field containing the roots of P is $\mathbb{F}_{2^{3m}}$. If $P|B_k$ this implies $\mathbb{F}_{2^{3m}} \subseteq \mathbb{F}_{2^{3k}}$ and $m|k$.

Let us write $k = ml$ for some integer l, and let g be a root of P then, if P is of type 1:

$$g^{2^m} = 1 + \frac{1}{g} = g^{2^k} = g^{2^{ml}}.$$

Because all the $3m$ roots of P are distinct and from properties of Frobenius operator we have

$$m = ml \mod 3m$$

then

$$l = 1 \mod 3.$$

If P is of type 2, then

$$g^{2^{2m}} = 1 + \frac{1}{g} = g^{2^k} = g^{2^{ml}}$$

and $l = 2 \bmod 3$ for the same reasons.

We prove now that the properties are sufficient.

Let $P \in \mathcal{I}$ be an alternate polynomial of degree $3m$. Suppose that the type of P is t and $k = lm$ with $l = t \bmod 3$, then for any root g of P:

$$g^{2^k} = g^{2^{lm}} = g^{2^{tm}} = 1 + \frac{1}{g}.$$

The last equality is a consequence of the definition of the type. Then g is always a root of B_k and $P|B_k$. $\square$

We give two simple examples:

For $k = 2$: $B_2 = X^5 + X + 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$. The alternate irreducible factor $X^3 + X^2 + 1$ corresponds to $m = 1$ and its type is 2. We verify easily that its type is 2 because, if g is a root of this factor, then

$$g^{2^2} = 1 + \frac{1}{g}.$$

For $k = 3$: $B_3 = X^9 + X + 1$. From our Theorem 2, only $m = 3$ can give irreducible factors (of type 1) of B_3 and such irreducible factor will have degree $3 \cdot 3 = 9$. So B_3 is alternate, irreducible and of type 1.

We can now settle our main result, which is a simple consequence of Theorem 2:

Theorem 3. *Consider $h_2(3m)$ with $m \geqslant 1$, i.e., half of the number of alternate irreducible polynomials of degree $3m$. Then for any $k \geqslant 1$:*

$$2^k - (-1)^k = \sum_{\substack{d|k \\ \frac{k}{d} \not\equiv 0 \bmod 3}} 3d h_2(3d). \tag{1}$$

Proof. Let EB_k be the set of all the polynomials of degree $\geqslant 3$ dividing B_k, then from Proposition 2

$$EB_k = \bigcup_{\substack{d|k \\ \frac{k}{d}\equiv 1 \bmod 3}} E_1(3d) \cup \bigcup_{\substack{d|k \\ \frac{k}{d}\equiv 2 \bmod 3}} E_2(3d),$$

with $E_1(3d)$ (resp. $E_2(3d)$) the set of all irreducible alternate polynomials of degree $3d$ and type 1 (resp. type 2) dividing B_k. Then, taking the degrees, we have

$$\sum_{Q\in EB_k} \deg Q = \sum_{\substack{d|k \\ \frac{k}{d}\equiv 1 \bmod 3}} 3d\,Card\big(E_1(3d)\big) + \sum_{\substack{d|k \\ \frac{k}{d}\equiv 2 \bmod 3}} 3d\,Card\big(E_2(3d)\big).$$

Corollary 1 implies

$$\begin{aligned}\sum_{Q\in EB_k} \deg Q &= \sum_{\substack{d|k \\ \frac{k}{d}\equiv 1 \bmod 3}} 3dh_2(3d) + \sum_{\substack{d|k \\ \frac{k}{d}\equiv 2 \bmod 3}} 3dh_2(3d) \\ &= \sum_{\substack{d|k \\ \frac{k}{d}\not\equiv 0 \bmod 3}} 3dh_2(3d).\end{aligned}$$

Moreover, from Proposition 3 we know that

$$\begin{aligned}\sum_{Q\in EB_k} \deg Q &= \begin{cases} 2^k - 1 & \text{if } k \text{ is even,} \\ 2^k + 1 & \text{if } k \text{ is odd} \end{cases} \\ &= 2^k - (-1)^k,\end{aligned}$$

which concludes our proof. $\square$

As we saw previously, a hexagon with two elements in the set of irreducible polynomials of degree $3m$ in $\mathbb{F}_2[X]$ is made of two alternate polynomials, so the number of these hexagons is equal to $h_2(3m)$.

Using Möbius inversion with characters (see Appendix A) on (1) we can give a formula for computing $h_2(3m)$:

Theorem 4. *The number $h_2(n)$ of hexagons with two elements of given degree $n \geqslant 2$ is* 0 *if $n \not\equiv 0 \bmod 3$, else with $n = 3m$*:

$$h_2(3m) = \frac{1}{3m} \sum_{\substack{d|m \\ d\not\equiv 0 \bmod 3}} \mu(d)\big(2^{m/d} - (-1)^{m/d}\big). \tag{2}$$

Proof. To obtain h_2 from the preceding theorem, we use elementary results about Dirichlet's characters and convolution. Short explanations are given in Appendix A.

Let us define the arithmetic functions:

$$f(m) = 2^m - (-1)^m,$$

$$g(m) = 3mh_2(3m)$$

for any $m \geqslant 1$. Let χ_3 be the principal Dirichlet's character modulo 3 (see Appendix A), then the formula (1) can be written as

$$f(m) = \sum_{\substack{d|m \\ d \not\equiv 0 \bmod 3}} g\left(\frac{m}{d}\right) = \sum_{d|m} \chi_3(d) g\left(\frac{m}{d}\right)$$

or, using Dirichlet's convolution, we obtain

$$f = \chi_3 * g.$$

Consequently

$$\mu\chi_3 * f = g.$$

This last equality gives (2). $\square$

The first values of h_2 are

$3m$	3	6	9	12	15	18	21	24	27	30
$h_2(3m)$	1	0	1	1	2	3	6	10	19	33

Eventually, we give a bound for $h_2(3m)$:

Corollary 2. *For integer $m \geqslant 1$:*

$$\left|3mh_2(3m) - 2^m\right| \leqslant 2^{\lfloor m/2 \rfloor + 1} + \lfloor m/2 \rfloor - 1.$$

Proof. From formula (1) we have

$$3mh_2(3m) = 2^m - (-1)^m + \sum_{\substack{d|m,\, d \geqslant 2 \\ d \not\equiv 0 \bmod 3}} \mu(d)\left(2^{m/d} - (-1)^{m/d}\right).$$

Hence

$$\begin{aligned}\left|3mh_2(3m) - 2^m\right| &\leqslant 1 + \sum_{1 \leqslant i \leqslant \lfloor m/2 \rfloor} \left(2^i + 1\right) \\ &\leqslant 1 + 2\left(2^{\lfloor m/2 \rfloor} - 1\right) + \lfloor m/2 \rfloor = 2^{\lfloor m/2 \rfloor + 1} + \lfloor m/2 \rfloor - 1. \qquad \square\end{aligned}$$

3.3. 3 elements hexagons

The results of this section are well known because, as we shall see below, this case is connected to the **self-reciprocal irreducible (sri)** polynomials. We refer to [4], [3] or [5] for more details and proofs.

Each of the polynomials in a 3 elements orbit $Hex(P)$ is invariant by one of the 3 subgroups of order 2 in $\mathfrak{S}_3$. In other words each 3 elements orbit is the orbit of a sri-polynomial of $\mathcal{I}$ (we recall that $X + 1$ is discarded from $\mathcal{I}$).

Conversely, if $P \in \mathcal{I}$ is a sri-polynomial, then:

$$Hex(P) = \left\{P, P^+, P^{+*}\right\},$$

P^+ is invariant by (1∞) action and P^{+*} is invariant by (01) action (it is a periodic polynomial).

The degree of a sri-polynomial P is even, because the inverse of the roots of P are also roots.

We emphasize on the fact that over $\mathbb{F}_2$ the sri-polynomials set plays exactly the same role as periodic or median polynomials. Nevertheless sri-polynomials draw much more attention, and a lot of work were devoted to them, because they are easy to recognize by visual inspection of their coefficients.

Theorem 5. *(See Meyn [3].)*

i) *Each sri-polynomial of degree* $2n$ $(n \geqslant 1)$ *over* $\mathbb{F}_2$ *is a factor of the polynomial*

$$H_n(X) = X^{2^n+1} + 1.$$

ii) *Each irreducible factor of degree* $\geqslant 2$ *of* H_n *is a sri-polynomial of degree* $2d$*, where* d *divides* n *such that* n/d *is odd.*

Corollary 3. *The median* (*resp. periodic*) *irreducible polynomials in* $\mathcal{I}$ *are the irreducible factors of*

$$X^{2^k} + X^{2^k-1} + 1 \ \big(\textit{resp. } X^{2^k} + X + 1\big) \quad k \geqslant 1.$$

Proof. We get the polynomial $X^{2^k} + X^{2^k-1} + 1$ (resp. $X^{2^k} + X + 1$) applying the transformation $+$ (resp. $+*$) on $X^{2^k+1} + 1$. $\square$

Theorem 6. *(See Carlitz [2].) The number of degree* $2m$ $(m \geqslant 1)$ *sri-polynomials in* $\mathbb{F}_2[X]$ *is*

$$S(2m) = \frac{1}{2m} \sum_{d|m,\, d \text{ odd}} \mu(d) 2^{\frac{m}{d}}$$

where μ *is the Möbius function.*

We refer to [5] for a demonstration of Carlitz formula in the same spirit as our paper.

Following our definitions,

$$h_3(n) = S(n) \quad \text{for } n \text{ even}, \ n > 2$$

and $h_3(n) = 0$ for all other values of n. The case $n = 2$ corresponds to the polynomial $X^2 + X + 1$ which gives a 1 element orbit.

The first values of h_3 and S are

$2m$	2	4	6	8	10	12	14	16	18	20
$h_3(2m)$	0	1	1	2	3	5	9	16	28	51
$S(2m)$	1	1	1	2	3	5	9	16	28	51

The value $S(1) = 1$ could be added: it corresponds to the polynomial $X + 1$ (which is not in our set $\mathcal{I}$). The sequence $S(n)$ $(n \geqslant 1)$ is registered as the sequence A48 in [6].

3.4. 6 elements hexagons

A famous formula of Gauss [1] gives the number $I(n)$ of irreducible polynomials of degree n in $\mathbb{F}_2[X]$:

$$I(n) = \frac{1}{n} \sum_{d|n} \mu(d) 2^{\frac{n}{d}}. \tag{3}$$

From (3) and the enumerations formulas we obtain the number of 6 elements hexagons of degree n, for $n \geqslant 2$:

$$h_6(n) = \frac{1}{6}\big[I(n) - h_1(n) - 2h_2(n) - 3h_3(n)\big].$$

4. Conclusion

We gather the different results of previous sections in a short table, starting from $n = 2$ because we excluded the polynomials of degree 1 from our enumerations:

n	h_1	h_2	h_3	h_6	*hex*	$I(n)$
2	1	0	0	0	1	1
3	0	1	0	0	1	2
4	0	0	1	0	1	3
5	0	0	0	1	1	6
6	0	0	1	1	2	9
7	0	0	0	3	3	18
8	0	0	2	4	6	30
9	0	1	0	9	10	56
10	0	0	3	15	18	99
11	0	0	0	31	31	186
12	0	1	5	53	59	335
13	0	0	0	105	105	630
14	0	0	9	189	198	1161
15	0	2	0	363	365	2182
16	0	0	16	672	688	4080
17	0	0	0	1285	1285	7710
18	0	3	28	2407	2438	14532
19	0	0	0	4599	4599	27594
20	0	0	51	8704	8755	52377

The sequence *hex* is A11957 [6]. It appears very unexpectedly in a 1981 work of T.J. McLarnan about packing atoms in chemistry [7,8].

The new sequences h_2 and h_6 are now registered as A165920 and A165921 [6].

Appendix A

For the article to be self contained we give a quick explanation of (more or less) known results on Möbius inversion with Dirichlet's characters.

An **arithmetic function** is a map $f : \mathbb{N} - \{0\} \to \mathbb{Z}$.

For two given arithmetic functions $f, g : \mathbb{N} - \{0\} \to \mathbb{Z}$ one defines their (Dirichlet's) **convolution** as

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

for any integer $n \geqslant 1$. The convolution is associative, commutative, distributive on the sum, and the arithmetical function

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{else} \end{cases}$$

is the neutral element of the convolution.

The **Möbius function identity**

$$\sum_{d|n} \mu(d) = \delta(n)$$

can be translated as

$$1 * \mu = \delta.$$

In other words, μ is the inverse of the constant function 1. The **Möbius inversion formula** is an immediate consequence of it:

$$f = 1 * g \quad \Rightarrow \quad g = f * \mu.$$

Let us consider the **principal** Dirichlet's character modulo n:

$$\chi_n(a) = \begin{cases} 1 & \text{if } (a,n) = 1, \\ 0 & \text{if } (a,n) \neq 1. \end{cases}$$

Given two arithmetical functions f and g, we write fg the pointwise multiplication of the two functions.

Proposition 4. *For any prime number p, and arithmetical functions f, g:*

$$(f\chi_p) * (g\chi_p) = (f * g)\chi_p.$$

The demonstration is straightforward. In particular, taking $f = 1$ and $g = \mu$, we obtain

Corollary 4.

$$\chi_p * (\mu\chi_p) = \delta\chi_p = \delta.$$

The inverse of χ_p for convolution is $\mu\chi_p$.

References

[1] C.F. Gauss, Disquisitiones generales de congruentiis. Werke II, 1863, pp. 220–221; our thanks to http://gdz.sub.uni-goettingen.de/en/gdz/.
[2] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, J. Reine Angew. Math. 227 (1967) 212–220.
[3] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Engrg. Comm. Comput. 1 (1990) 43–53.
[4] S.D. Cohen, The explicit construction of irreducible polynomials over finite fields, Des. Codes Cryptogr. 2 (1992) 169–174.
[5] H. Meyn, W. Götz, Self-reciprocal polynomials over finite fields, Publ. I.R.M.A. Strasbourg 413 (S-21) (1990) 82–90.
[6] N.J.A. Sloane, The on-line encyclopedia of integer sequences, 2009; http://www.research.att.com/~njas/sequences/.
[7] T.J. McLarnan, Z. Krist. 155 (1981) 269–291.
[8] N.J.A. Sloane, Parthasarathy Nambi, Integer sequences related to chemistry, Poster to be presented at the Amer. Chem. Soc. National Meeting, San Francisco, 2006.