J. Korean Math. Soc. 22 (1985), No. 2, pp. 117-124

ON THE LEVEL OF IRREDUCIBLE POLYNOMIALS OVER GALOIS FIELDS

DIETMAR GARBE*

1. Introduction

In [3] the author, while working on normal subgroups of the classical modular group Γ, found a connection between a class of non-congruence subgroups of Γ of level m and a certain parameter m of the monic irreducible polynomials over the prime fields $\mathbf{F}_p$.

It is certainly of interest to investigate this parameter. In the present paper we extend that concept, which we call the level of the polynomial, to all Galois fields $\mathbf{F}_q$ $(q=p^f)$. The level turns out to be an analogue of the well known concept of exponent.

There are connections with the theory of cyclotomic fields which has gained new interest in the recent years. We want to stress on the fact that there exist classes of polynomials, indexed by positive integers n with $(n, p)=1$ (namely the cyclotomic polynomials $\Phi_n(x)$ and the below defined $\chi_n(x)$), such that every monic irreducible polynomial over a fixed Galois field $\mathbf{F}_q$ is a divisor of exactly one polynomial of the class. So the index n is a characteristic number of the polynomial, called exponent and level respectively.

This is a phenomenon which is not covered by the Kummer-Dedekind numbertheoretic setting. It belongs to deeper number theory: the theorems 2.1 and 3.5 are statements in the spirit of the Kronecker-Weber theorem.

2. Exponent and cyclotomic polynomials

We recall that the irreducible monic polynomial $f(x)\in\mathbf{F}_q[x]$ is said to belong to the exponent e, if e is the smallest positive integer such that $f(x)$ is a divisor of x^e-1 [1; p. 130].

Received February 10, 1985.
* This research was supported by Deutscher Akademischer Austauschdient (DAAD).

From the well-known relation

$$x^e-1=\prod_{k\mid e}\Phi_k(x) \tag{2.1}$$

($\Phi_k(x)$ the k-th cyclotomic polynomial over $\mathbf{F}_p$)
we get immediately

$$e=\min\ \{n\in\boldsymbol{N}\mid f(x)\mid\Phi_n(x)\}. \tag{2.2}$$

There exist exactly $\frac{\phi(e)}{d}$ different monic irreducible polynomials of degree d in $\mathbf{F}_q[x]$ belonging to the exponent e, and d is then minimal such that

$$q^d\equiv 1 \bmod e.$$

Because of (2.2) $\Phi_e(x)$ decomposes over $\mathbf{F}_q$ into the product of the $\frac{\phi(e)}{d}$ different monic irreducible polynomials of degree d which belong to the exponent e.

Let now q, n be given such that $(q, n)=1$ and let d be the order of q in $\mathbf{Z}_n^*$. If we assume that n is not an exponent for a suitable $f(x)\in\mathbf{F}_q[x]$, then

$$M=\sum_{\substack{e\mid q^d-1\\ e\nmid q^{d_0}-1,\ \text{if } d_0<d}}\frac{\phi(e)}{d} \tag{2.3}$$

would be strictly greater than the number of monic irreducible polynomials of degree d over $\mathbf{F}_q$, which is known to be

$$N=\frac{1}{d}\sum_{n\mid d}\mu\left(\frac{d}{n}\right)q^n. \tag{2.4}$$

But it is routine to check

$$M=N. \tag{2.5}$$

So we have

$$(\Phi_m(x), \Phi_n(x))\sim 1,\ \text{if } (m, q)=(n, q)=1 \text{ and } m\neq n. \tag{2.6}$$

and we have proved the following statement.

THEOREM 2.1. *Every monic irreducible polynomial $f(x)$ of $\mathbf{F}_q[x]$ is a divisor of exactly one of the elements of the set $\{\Phi_n(x)\mid(n, q)=1\}$. The index of this element is the exponent to which $f(x)$ belongs. The $\Phi_n(x)$, $(n, q)=1$, are without repeated factors.*

REMARK 2.2. Though the content of theorem 2.1 is likely to be found somewhere in the elder literature, we stated it here because of

the analogy with our later theorem 3.5. A part of the statement of theorem 2.1 is related to Kummer's theorem. In fact, let $(q,n)=1$ and let us asume that we have an algebraic number field k such that there exists a prime ideal p in k of norm q and such that $[K=k(\zeta_n):k]=\phi(n)$, where ζ_n is a primitive n-th root of unity. Then p is unramified in K. The reciprocity isomorphism σ from the Galois group $G(K|k)$ onto $\mathbf{Z}_n^*$ (given by $\sigma(g)=l$, if $g\in G(K|k)$ and $g\zeta_n=\zeta_n^l$) maps the Artin-symbol $\left(\frac{K|k}{p}\right)$ onto $Np=q$. As $d=[\mathcal{O}/\mathcal{P}:o/p]=\left|\left(\frac{K|k}{p}\right)\right|$, the order of q in $\mathbf{Z}_n^*$ is d, and one gets in K the decomposition $p=\prod_{i=1}^{r}\mathcal{P}_i$, where $N\mathcal{P}_i=q^d$, $[K:k]=rd$. As the different is $\mathcal{D}_{K/k}=(\Phi_n'(\zeta_n))$, Kummer's theorem [2;p. 93] implies in $\mathbf{F}_q[x]$ the decomposition $\Phi_n(x)=\prod_{i=1}^{r}f_i(x)$. The $f_i(x)\in\mathbf{F}_q[x]$ are monic irreducible of degree d. But the core of the statement in theorem 2.1 is established by arguments via (2.3), (2.4), (2.5) which are not covered by Kummer's theorem. In the same way theorem 3.5 is related to the fields $k(\zeta_m+\zeta_m^{-1})$.

3. The polynomials $\chi_n(x)$

Let ζ_n be an n-th primitive root of unity over some prime field. We look at $\alpha_n^{(i)}:=\zeta_n^i+\zeta_n^{-i}$ in the n-th cyclotomic field. We define

$$\chi_n(x):=\prod_{\substack{(i,n)=1\\ 1\le i\le\frac{\delta n}{2}}}(x-\alpha_n^{(i)}) \qquad (n\in\mathbf{N}) \tag{3.1}$$

$$\delta:=\begin{cases}2, & \text{if } n=1,2\\ 1, & \text{if } n>2.\end{cases}$$

One can easily prove the following properties of the $\chi_n(x)$:

$$\deg\chi_n(x)=\frac{\delta\phi(n)}{2} \tag{3.2}$$

($\phi(n)$ is Euler's ϕ-function)

$$x^{\frac{\delta\phi(n)}{2}}\chi_n(x+x^{-1})=\chi_n{}^{\delta}(x) \tag{3.3}$$

$$\chi_{2n}(x)=(-1)^{\frac{\delta\phi(n)}{2}}\chi_n(-x) \quad \text{for } n \text{ odd} \tag{3.4}$$

(use (3.3) and the well known formula $\Phi_{2n}(x)=-\Phi_n(-x)$)

$$\chi_p(x)=\sum_{\nu=0}^{\frac{p-1}{2}}(-1)^{\left[\frac{\nu}{2}\right]}\binom{\frac{p-1}{2}-\left[\frac{\nu+1}{2}\right]}{\left[\frac{\nu}{2}\right]}x^{\frac{p-1}{2}-\nu} \quad \text{for prime } p>2 \tag{3.5}$$

($[\nu]$ is the greatest integer not exceeding ν)

$$(3.6)\quad \prod_{\substack{d|n\\ 1\leqslant d\leqslant n}} \chi_d(x+x^{-1})=\frac{(x^n-1)(x^{\varepsilon_n}-1)}{x^{\frac{n+\varepsilon_n}{2}}},\quad \varepsilon_n:=\frac{3+(-1)^n}{2}$$

In the case of characteristic zero we have $\chi_n(x)\in\mathbf{Z}[x]$. $\chi_n(x)$ is irreducible over $\mathbf{Q}$, as χ_n is the minimal polynomial of the algebraic integer $\alpha_n=2\cos\frac{2\pi}{n}$. There exists a connection with the Chebychev polynomials of the 2nd kind

$$U_n(x)=\frac{\sin[(n+1)\cos^{-1}x]}{\sin(\cos^{-1}x)}\in\mathbf{Z}[x].$$

The following lemma gives the decomposition law for the Chebychev polynomials.

LEMMA 3.1. $$U_n(x)=\prod_{\substack{d|2n+1\\ d>2}}\chi_d(2x)$$

Proof. Observe that the relation

$$(3.7)\quad U_n\left(\frac{x}{2}\right)=\prod_{\substack{d|2n+2\\ d>2}}\chi_d(x)$$

follows from the fact that $\chi_d(x)$ is the minimal polynomial of α_d and by comparing the degrees of both sides of (3.7).

COROLLARY. 3.2. *The $U_n(x)$, $n>1$, are reducible over $\mathbf{Z}$*

Using the recursion formula (3.6), it is not difficult to show by induction that for characteristic p the corresponding $\chi_n(x)$ has its coefficients in $\mathbf{F}_p$ and that it is obtained by reducing the characteristic-zero-polynomial $\chi_n(x)$ of $\mathbf{Z}[x]$ modulo p.

But in characteristic p the $\chi_n(x)$ are in general not irreducible. (See the following proposition.)

PROPOSITION 3.3. *In $\mathbf{F}_{pf}[x]$, $p>2$, we have $\chi_{pn}(x)=\chi_{p^{p^{n-1}}}(x)=(x-2)^{\frac{p-1}{2}p^{n-1}}$. In $\mathbf{F}_{2f}[x]$ we have $\chi_{2n}(x)=\chi_{2^{2^{n-2}}}(x)=x^{2^{n-2}}$ $(n>1)$.*

Proof. (2.1) implies in the case of characteristic p

$$\Phi_{pn}(x)=\Phi_{p^{p^{n-1}}}(x),$$

and so we get

$$\chi_{pn}(x)=\chi_{p^{p^{n-1}}}(x)\ \text{ for } p>2.$$

The decomposition law of p in $\mathbf{Q}(\alpha_p)$ yields $(p)=\mathfrak{P}^{\frac{p-1}{2}}$, where $\mathfrak{P}$ is a prime ideal in $\mathbf{Z}[\alpha_p]$ such that $N\mathfrak{P}=p$. Kummer's theorem leads to

$$\chi_p(x)\equiv(x-a)^{\frac{p-1}{2}} \mod p.$$

Comparing the coefficients of $x^{\frac{p-1}{2}-1}$ in (3. 5) and in $(x-a)^{\frac{p-1}{2}}$, we get

$$a\equiv 2 \mod p.$$

The proof in the case of characteristic 2 is similar.

Using (2. 6) and (3. 3), we get

PROPOSITION 3. 4. *$(\chi_m(x), \chi_n(x))\sim 1$ in $\mathbf{F}_q[x]$, if $(m, q)=(n, q)=1$ and $m\neq n$.*

Without the presupposition $(m, q)=(n, q)=1$ proposition 3. 4 no longer remains valid, as proposition 3. 3 shows. The reason for this fact becomes obvious, when we look at the following theorem.

THEOREM 3. 5. *Every monic irreducible polynomial $f(x)\in\mathbf{F}_q[x]$ is a divisor of exactly one element $\chi_m(x)$ of the set $\{\chi_n(x)\mid(n, q)=1\}$. The $\chi_n(x)$, $(n, q)=1$, are without repeated factors.*

Proof. According to proposition 3. 4 $f(x)$ is a divisor of at most one $\chi_n(x)$. We consider the special case $q=p$. The decomposition law for $\mathbf{Q}(\alpha_n)$ and Kummer's theorem show that $\chi_n(x)$ decomposes over $\mathbf{F}_p$ into $\frac{\delta\phi(n)}{2d}$ different monic irreducible polynomials of degree d, where d is minimal such that

$$p^d\equiv\pm 1 \mod n.$$

It is a routine matter to check that for fixed d the following analogon of (2. 5) is valid:

$$\sum_{\substack{n\mid p^d\pm 1\\ n\nmid p^{d^*}\pm 1,\ \text{if } d^*<d}}\frac{\delta\phi(n)}{2d}=\frac{1}{d}\sum_{n\mid d}p^n\mu\left(\frac{d}{n}\right). \tag{3.8}$$

But the sum on the right hand side is known to be the number of the monic irreducible polynomials of $\mathbf{F}_p[x]$ of degree d.

Let now $f(x)$ be monic irreducible in $\mathbf{F}_q[x]$ and let $f(x)$ belong to the exponent e. Then by theorem 2. 1 we have

$$\Phi_e(x)\equiv 0 \mod f(x).$$

If

$$\Phi_e(x)=\prod g_i(x)$$

is the decomposition of $\Phi_e(x)$ over $\mathbf{F}_p$ into irreducible factors, then $f(x)$ is a divisor in $\mathbf{F}_q\ [x]$ of one of the $g_i(x)$, say of $g_k(x)$. As

$$\chi_n(x)\equiv 0 \mod g_k(x)$$

for some n according to the first step of the proof, we have

$$\chi_n(x)\equiv 0 \mod f(x).$$

The check of the validity of

$$\sum_{\substack{n\mid q^d\pm 1\\ n\nmid q^{d^*}\pm 1,\ \text{if } d^*<d}} \frac{\delta\phi(n)}{d}=\frac{1}{d}\sum_{n\mid d} q^n\,\mu\left(\frac{d}{n}\right) \tag{3.9}$$

together with lemma 4.2 shows that $\chi_n(x)$ has no repeated factors over $\mathbf{F}_q$, if $(q,n)=1$.

4. The level of the irreducible monic polynomials over $\mathbf{F}_q$

DEFINITION 4.1. Let $f(x)\in\mathbf{F}_q[x]$ be irreducible monic. We now call the parameter m of theorem 3.5 the *level of* $f(x)$.

LEMMA 4.2. *Let ζ_n be a primitive n-th root of unity over the prime field of $\mathbf{F}_q$, $(q,n)=1$, and let $\alpha_n := \zeta_n+\zeta_n^{-1}$. Then $[\mathbf{F}_q(\alpha_n):\mathbf{F}_q]$ is the smallest positive integer d such that*

$$q^d\equiv\pm 1 \ \textit{mod}\ n.$$

Proof. $\mathbf{F}_q(\alpha_n)$ is a Galois field with $G(\mathbf{F}_q(\alpha_n)\,|\,\mathbf{F}_q)=\langle x\to x^q\rangle$. So $[F_q(\alpha_n):F_q]$ is the smallest positive integer d such that $\alpha_n{}^{q^d}=\alpha_n$, i.e.,

$$\zeta_n{}^{q^d+1}-1=\zeta_n{}^2(1-\zeta_n{}^{-q^d-1}).$$

This implies the assertion.

THEOREM 4.3. *Let $f(x)\in\mathbf{F}_q[x]$ be irreducible monic. The following statements hold true:*

a. *$f(x)$ has level m, iff every root of $f(x)$ is a root of $\chi_m(x)$.*

b. *If m is the level of $f(x)$, then $\deg f(x)$ is the smallest positive integer d such that $q^d\equiv\pm 1$ mod m.*

c. *All polynomials of $\mathbf{F}_q[x]$ of level m have the same degree.*

d. *The level of $f(x)$ is a divisor of $q^{\deg f(x)}\pm 1$.*

e. *If $(m,q)=1$, then there exist exactly $\dfrac{\delta\phi(m)}{2d}$ monic irreducible polynomials in $\mathbf{F}_q[x]$ of level m, where d is the smallest positive integer such that $q^d\equiv\pm 1$ mod m. (They have degree d.)*

f. *If* $f(x)$ *has level* m, *then* $\delta\phi(m)\equiv 0 \bmod 2deg f(x)$.

g. *As levels of the irreducible monic polynomials in* $\mathbf{F}_q[x]$ *of degree* d *occur exactly those positive integers which are divisors of* $q^d\pm 1$, *but not of* $q^{d^*}\pm 1$, *if* $d^*<d$.

Proof. a follows from the definition. b is a consequence of lemma 4.2. c and d follow from b. e is a consequence of (3.9) and of lemma 4.2. f follows from e. g is a consequence of b and of (3.9).

As an illustration we give the level m (and the exponent e) of all irreducible polynomials over $\mathbf{F}_2$, $\mathbf{F}_3$, and $\mathbf{F}_5$ up to a certain low degree d, namely $d=5, 3, 2$ respectively. If the irreducible polynomial has the form

$$f(x)=x^d+a_1x^{d-1}+\ldots+a_d,$$

$f(x)$ is described in the table by the sequence $a_1a_2\ldots a_d$.

$\mathbf{F}_2$			$\mathbf{F}_3$			$\mathbf{F}_5$		
$f(x)$	e	m	$f(x)$	e	m	$f(x)$	e	m
0		1	0		4	0		4
1	1	3	1	2	1	1	2	3
11	3	5	2	1	2	2	4	2
011	7	9	01	4	8	3	4	1
101	7	7	12	8	5	4	1	6
0011	15	17	22	8	10	02	8	12
1001	15	15	021	26	26	03	8	8
1111	5	17	022	13	13	11	3	24
00101	31	31	102	13	28	12	24	13
01001	31	31	112	13	7	23	24	26
01111	31	33	121	26	13	24	12	13
10111	31	11	201	26	28	33	24	13
11011	31	33	211	26	14	34	12	26
11101	31	11	222	13	26	41	6	24
						42	24	26

References

1. A. A. Albert, *Fundamental Concepts of Higher Algebra*, The University of Chicago Press, Chicago, 1956.
2. J. W. S. Cassels and A. Froehlich (eds.), *Algebraic Number Theory*, Academic Press, London, 1967.

3. D. Garbe, *Ueber eine Klasse von arithmetisch definierbaren Normalteilern der Modulgruppe*, Math. Ann. **235** (1978), pp. 195–215.

Pusan National University
Pusan 607, Korea