Bull. Korean Math. Soc. **23**(1986), No. 2, pp. 103-111

REMARKS ON FINITE FIELDS III

SHINWON KANG

In [2] and [3], the Shinwon polynomial $S_n(x)$ of order n is defined and studied in some details. In this paper we will define the general Shinwon polynomial $S_n(a, x)$ and the Dickson polynomial $D_n(a, x)$ of the second kind of order n which is a slightly changed form of the Dickson polynomial $g_n(a, x)$, and show that $D_n(a, x)$ is closely related to $S_n(a, x)$.

Let a and b be given integers. A sequence $s_0, s_1, \ldots$ of elements of Z satisfying the relation

$$s_{n+2}=as_{n+1}+bs_n \text{ for } n=0, 1, \ldots \tag{1}$$

is called a *second order homogeneous linear recurring sequence* in Z. With this homogeneous linear recurring sequence we associate the 2×2 matrix A over $\boldsymbol{Z}$ defined by $A=\begin{bmatrix}0 & b\\ 1 & a\end{bmatrix}$. The polynomial $f(x)=\det\begin{bmatrix}x & b\\ 1 & x-a\end{bmatrix}=x^2-ax-b$ is called the *characteristic polynomial of the sequence.* The vector (s_n, s_{n+1}) is called the *n-th state vector of the homogeneous linear recurring sequence.* The state vector (s_0, s_1) is also refered to as the initial state vector. Since $(s_{n+1}, s_{n+2})=(s_n, s_{n+1})\begin{bmatrix}0 & b\\ 1 & a\end{bmatrix}$ for all $n\geqslant 0$, we have that $(s_n, s_{n+1})=(s_0, s_1)A^n$ for $n=0, 1, \ldots,$ by induction on n ([4]).

LEMMA 1. *If a and b are integers and $A=\begin{bmatrix}0 & b\\ 1 & a\end{bmatrix}$, then*

$$A^n=\begin{bmatrix}bs_{n-2}(a, b) & bs_{n-1}(a, b)\\ s_{n-1}(a, b) & s_n(a, b)\end{bmatrix} \quad \textit{for } n=2, 3, \ldots$$

where $S_0(a, b)=1$ *and* $S_n(a, b)=\sum_{i=0}^{[n/2]}\binom{n-i}{i}a^{n-2i}b^i$ *for* $n=1, 2, \ldots$

Proof. We will prove the lemma by induction on n.

$$A^2=\begin{bmatrix}0 & \mathrm{b}\\ 1 & \mathrm{a}\end{bmatrix}^2=\begin{bmatrix}b & ba\\ a & b+a^2\end{bmatrix}=\begin{bmatrix}bs_0(a, b) & bS_1(a, b)\\ S_1(a, b) & S_2(a, b)\end{bmatrix}.$$

Suppose that the lemma is true for all integers less than n. Then

Received November 20, 1985.

$$A^n = A^{n-1}\cdot A = \begin{bmatrix} bS_{n-3}(a,b) & bS_{n-2}(a,b) \\ S_{n-2}(a,b) & S_{n-1}(a,b)\end{bmatrix}\begin{bmatrix} 0 & b \\ 1 & a\end{bmatrix}$$
$$= \begin{bmatrix} bS_{n-2}(a,b) & b^2S_{n-3}(a,b)+abS_{n-2}(a,b) \\ S_{n-1}(a,b) & bS_{n-2}(a,b)+aS_{n-1}(a,b)\end{bmatrix}.$$

According to the following identity

$$S_n(a,b) = aS_{n-1}(a,b) + bS_{n-2}(a,b)$$

which follows from the property of the binomial coefficients:

$$\binom{n-r}{r} = \binom{n-r-1}{r} + \binom{n-r-1}{r-1}, \quad [n/2] \geqslant r \geqslant 1$$

we have that

$$A^n = \begin{bmatrix} bS_{n-2}(a,b) & bS_{n-1}(a,b) \\ S_{n-1}(a,b) & S_n(a,b)\end{bmatrix}.$$

So the lemma is true for all integers $n \geqslant 2$.

THEOREM 1. *If* $s_0, s_1 \ldots$ *is a homogeneous linear recurring sequence in* $\boldsymbol{Z}$ *satisfying* (1), *then* $s_n = s_0 bS_{n-2}(a,b) + s_1 S_{n-1}(a,b)$, *for* $n \geqslant 2$.

Proof. By the above lemma, we have that

$$(s_n, s_{n+1}) = (s_0, s_1)\begin{bmatrix} bS_{n-2}(a,b) & bS_{n-1}(a,b) \\ S_{n-1}(a,b) & S_n(a,b)\end{bmatrix}.$$

This means that

$$s_n = s_0 bS_{n-2}(a,b) + s_1 S_{n-1}(a,b), \quad \text{for } n \geqslant 2.$$

DEFINITION. Let a and b be any integers.

The sequence $\{s_n\} = \{S_n(a,b)\}$ for $n=0, 1, 2, \ldots$ is called the *Shinwon sequence of the first kind with respect to a and b.*

The sequence $s_0 = 2$, $s_1 = a$, $s_{n+2} = as_{n+1} + bs_n$ for $n=0, 1, \ldots$ is called the *Shinwon sequence of the second kind with respect to a and b* and is denoted by $\{s_n\} = \{D_n(a,b)\}$.

On putting $a=b=1$ in $S_n(a,b)$ and $D_n(a,b)$ respectively, we have the interesting results: the sequence $\{S_n(1,1)\} = \{F_{n+1}\}$ for $n=0, 1, \ldots$ is the Fibonacci sequence and the sequence $\{D_n(1,1)\} = \{L_n\}$ for $n=0, 1, \ldots,$ is the Lucas sequence. Since the sequence $\{D_n(a,b)\}$ is a homogeneous linear recurring sequence in $\boldsymbol{Z}$ satisfying (1), by the Theorem 1, $D_n\ (a,b)$ is of the form

$$D_n(a,b) = 2bS_{n-2}(a,b) + aS_{n-1}(a,b), \quad \text{for } n \geqslant 2.$$

Simple calculation shows that for $n \geqslant 2$,

$$D_n(a,b)=2b\sum_{i=0}^{[(n-2)/2]}\binom{n-2-i}{i}a^{n-2-2i}b^i$$
$$+a\sum_{i=0}^{[(n-1)/2]}\binom{n-1-i}{i}a^{n-1-2i}b^i$$
$$=\sum_{i=0}^{[n/2]}\frac{n}{n-i}\binom{n-i}{i}a^{n-2i}b^i.$$

THEOREM 2. *If* α *and* β *are the roots of the characteristic polynomial* $f(x)=x^2-ax-b$ *of the sequence* $\{S_n(a,b)\}$ *(or, equivalently* $\{D_n(a,b)\}$*), then*

$$S_n(a,b)=\alpha^n+\alpha^{n-1}\beta+\ldots+\alpha\beta^{n-1}+\beta^n$$
$$D_n(a,b)=\alpha^n+\beta^n.$$

Proof. We will prove the theorem by induction on n.

$$S_0(a,b)=1$$
$$D_0(a,b)=2$$
$$S_1(a,b)=a=\alpha+\beta$$
$$D_1(a,b)=a=\alpha+\beta.$$

Suppose that the theorem is true for all integers less than n. Then

$$S_n(a,b)=aS_{n-1}(a,b)+bS_{n-2}(a,b)$$
$$=(\alpha+\beta)(\alpha^{n-1}+\alpha^{n-2}\beta+\ldots+\alpha\beta^{n-2}+\beta^{n-1})$$
$$-\alpha\beta(\alpha^{n-2}+\alpha^{n-3}\beta+\ldots+\alpha\beta^{n-3}+\beta^{n-2})$$
$$=\alpha^n+\alpha^{n-1}\beta+\ldots+\alpha\beta^{n-1}+\beta^n.$$
$$D_n(a,b)=aD_{n-1}(a,b)+bD_{n-2}(a,b)$$
$$=(\alpha+\beta)(\alpha^{n-1}+\beta^{n-1})-\alpha\beta(\alpha^{n-2}+\beta^{n-2})$$
$$=\alpha^n+\beta^n.$$

So, the theorem is true for all integers.

LEMMA 2. *For all integers* $n\geqslant r\geqslant 2$ *we have that*

$$S_n(a,b)=S_{r-1}(a,b)S_{n-r+1}(a,b)+bS_{r-2}(a,b)S_{n-r}(a,b)$$
$$D_n(a,b)=S_{r-1}(a,b)D_{n-r+1}(a,b)+bS_{r-2}(a,b)D_{n-r}(a,b).$$

Proof. $(S_n(a,b),S_{n+1}(a,b))=(1,a)A^n=(1,a)A^{n-r}\cdot A^r$

$$=(S_{n-r}(a,b),S_{n-r+1}(a,b))\begin{bmatrix}bS_{r-2}(a,b) & bS_{r-1}(a,b)\\ S_{r-1}(a,b) & S_r(a,b)\end{bmatrix}.$$ So,

$$S_n(a,b)=S_{r-1}(a,b)S_{n-r+1}(a,b)+bS_{r-2}(a,b)S_{n-r}(a,b)$$
$$(D_n(a,b),D_{n+1}(a,b))=(2,a)A^n=(2,a)A^{n-r}\cdot A^r$$
$$=(D_{n-r}(a,b),D_{n-r+1}(a,b))\begin{bmatrix}bS_{r-2}(a,b) & bS_{r-1}(a,b)\\ S_{r-1}(a,b) & S_r(a,b)\end{bmatrix}.$$

So, $D_n(a,b)=S_{r-1}(a,b)D_{n-r+1}(a,b)+bS_{r-2}(a,b)D_{n-r}(a,b)$.

LEMMA 3. *For all positive integers n and r, we have that*

$$S_{nr-1}(a,b)\equiv 0 \pmod{S_{r-1}(a,b)}.$$

Proof. Straightforward calculation shows that

$$\begin{aligned}S_{nr-1}(a,b)&=\alpha^{nr-1}+\alpha^{nr-2}\beta+\ldots+\alpha\beta^{nr-2}+\beta^{nr-1}\\&=(\alpha^{r-1}+\alpha^{r-2}\beta+\ldots+\alpha\beta^{r-2}+\beta^{r-1})\cdot\\&\quad(\alpha^{(n-1)r}+\alpha^{(n-2)r}\beta^r+\ldots+\alpha^r\beta^{(n-2)r}+\beta^{(n-1)r})\\&=S_{r-1}(a,b)f(a,b)\end{aligned}$$

where $f(a,b)=\alpha^{(n-1)r}+\alpha^{(n-2)r}\beta^r+\ldots+\alpha^r\beta^{(n-2)r}+\beta^{(n-1)r}$ is a symmetric polynomial in α and β which means that $f(a,b)$ is a polynomial in a and b.

LEMMA 4. *For all positive integers n and r we have that*

$$D_{n(2r+1)}(a,b)\equiv 0 \pmod{D_n(a,b)}.$$

Proof.
$$\begin{aligned}D_{n(2r+1)}(a,b)&=\alpha^{n(2r+1)}+\beta^{n(2r+1)}\\&=(\alpha^n+\beta^n)(\alpha^{2rn}-\alpha^{(2r-1)n}\beta^n+\ldots-\alpha^n\beta^{(2r-1)n}+\beta^{2rn})\\&=D_n(a,b)g(a,b)\end{aligned}$$

where $g(a,b)=\alpha^{2rn}-\alpha^{(2r-1)n}\beta^n+\ldots-\alpha^n\beta^{(2r-1)n}+\beta^{2rn}$ is a symmetric polynomial in α and β which means that $g(a,b)$ is a polynomial in a and b.

LEMMA 5. *Suppose that p is an odd prime and a and b are not divisible by p. Then we have that*

$$S_{p-1}(a,b)\equiv(a^2+4b)^{(p-1)/2} \pmod p$$
$$D_p(a,b)\equiv a \pmod p$$

Proof. Since $\binom{p-1}{r}=\dfrac{(p-1)\cdots(p-r)}{r!}\equiv(-1)^r \pmod p$

we have that

$$\begin{aligned}S_{p-1}(a,b)&=\alpha^{p-1}+\alpha^{p-2}\beta+\ldots+\alpha\beta^{p-2}+\beta^{p-1}\\&\equiv\alpha^{p-1}-\binom{p-1}{1}\alpha^{p-2}\beta+\ldots-\binom{p-1}{p-2}\alpha\beta^{p-2}+\beta^{p-1}\\&=(\alpha-\beta)^{p-1}=[(\alpha-\beta)^2]^{(p-1)/2}\\&=(a^2+4b)^{(p-1)/2} \pmod p.\end{aligned}$$

$$\begin{aligned}D_p(a,b)&=\alpha^p+\beta^p\equiv(\alpha+\beta)^p\\&=a^p\equiv a \pmod p.\end{aligned}$$

LEMMA 6. *Suppose that p is an odd prime and a and b are not divisible by p. Then we have that*

$$S_p(a,b)\equiv a[S_{p-1}(a,b)+a^{p-1}](p+1)/2$$
$$\equiv[bS_{p-2}(a,b)-a^p](p-1)\pmod p.$$

Proof. It follows from the following properties:

$$2\binom{p-r}{r}\equiv\binom{p-r-1}{r}\pmod p$$
$$\binom{p-r}{r}\equiv(p-1)\binom{p-r-1}{r-1}\pmod p$$

where $1\leqslant r\leqslant(p-1)/2$.

LEMMA 7. *For every positive integer n*

$$S_{2n-1}(a,b)=S_{n-1}(a,b)D_n(a,b).$$

Proof. $S_{2n-1}(a,b)=S_{n-1}(a,b)(\alpha^n+\beta^n)=S_{n-1}(a,b)D_n(a,b)$.

LEMMA 8. *For all positive integers $n\geqslant 2$ and any non-zero integers a and b, $D_n(a,b)$ does not contain the $S_r(a,b)$ as a factor for $1<r\leqslant n$.*

Proof. Suppose that $D_n(a,b)=S_r(a,b)f(a,b)$ where $f(a,b)\in\boldsymbol{Z}$ is a polynomial in a and b. Then

$$\alpha^n+\beta^n=(\alpha^r+\alpha^{r-1}\beta+\dots+\alpha\beta^{r-1}+\beta^r)f(a,b).$$

If we put $\alpha=\beta=1$, then we have that $2=(r+1)f(a,b)$.
Since $f(a,b)\in\boldsymbol{Z}$, this is impossible.

If we replace b by an indeterminate x in $S_n(a,b)$ and $D_n(a,b)$ respectively, then we obtain the polynomials which are defined on $\boldsymbol{Z}$, namely

$$S_n(a,x)=\sum_{i=0}^{[n/2]}\binom{n-i}{i}\,a^{n-2i}x^i\quad n\geqslant 1.$$
$$D_n(a,x)=\sum_{i=0}^{[n/2]}\frac{n}{n-i}\binom{n-i}{i}\,a^{n-2i}x^i\quad n\geqslant 1.$$

If we put $a=1$ in $S_n(a,x)$ then we have that

$$S_n(1,x)=\sum_{i=0}^{[n/2]}\binom{n-i}{i}x^i=S_n(x)$$

where $S_n(x)$ is the Shinwon polynomial of order n (see [2] and [3]). If we put $a=x$ and $b=-c$ in $D_n(a,b)$ then we obtain the another polynomial

$$D_n(x, -c) = \sum_{k=0}^{[n/2]} \frac{n}{n-k}\binom{n-k}{k}(-c)^k x^{n-2k} = g_n(x, c)$$

where $g_n(x, c)$ is the Dickson polynomial ([4]).

DEFINITION. For any non-zero integer a and positive integer n, $S_n(a, x)$ is called the *general Shinwon polynomial of order n*. $D_n(a, x)$ is called the *Dickson polynomial of the second kind of order n*.

By the preceding theorems and lemmas we obtain many interesting identities.

$$S_n(a, x) = aS_{n-1}(a, x) + xS_{n-2}(a, x) \quad n \geqslant 2$$

$$D_n(a, x) = aS_{n-1}(a, x) + 2xS_{n-2}(a, x) \quad n \geqslant 2$$

$$S_n(a, x) = S_r(a, x)S_{n-r}(a, x) + xS_{r-1}(a, x)S_{n-r-1}(a, x) \quad n > r \geqslant 1$$

$$D_n(a, x) = S_{r-1}(a, x)D_{n-r+1}(a, x) + xS_{r-2}(a, x)D_{n-r}(a, x) \quad n > r \geqslant 2$$

$$S_{n(r+1)-1}(a, x) \equiv 0 \pmod{S_r(a, x)}$$

$$D_{n(2r+1)}(a, x) \equiv 0 \pmod{D_n(a, x)}$$

$$S_{p-1}(a, x) \equiv (a^2+4x)^{(p-1)/2} \pmod{p} \quad p: \text{odd prime}$$

$$D_p(a, x) \equiv a \pmod{p}$$

$$S_p(a, x) \equiv a[S_{p-1}(a, x) + a^{p-1}](p+1)/2$$

$$\equiv [xS_{p-2}(a, x) - a^p](p-1) \pmod{p} \quad p: \text{odd prime}$$

$$S_{2n-1}(a, x) = S_{n-1}(a, x)D_n(a, x)$$

$$S_p(a, x) = S_{(p-1)/2}(a, x)D_{(p+1)/2}(a, x) \quad p: \text{odd prime}$$

For every odd prime p, the polynomial $S_p(x)$ splits over the finite field F_p and has distinct $(p-1)/2$ roots in F_p (see [2]).

THEOREM 3. *Let a be a non-zero fixed element in F_p where p is an odd prime. Then the polynomial $S_p(a, x)$ splits over F_p and has distinct $(p-1)/2$ roots in F_p.*

Proof. By the Lemma 5 and 6, we have in F_p

$$S_p(a, x) = a[(a^2+4x)^{(p-1)/2} + a^{p-1}](p+1)/2.$$

But for all $x \in F_p$ we have that $(a^2+4x)^{(p-1)/2} = 1$ or -1 or 0 and $a^{p-1} = 1$. If x runs over F_p so also does $y = a^2+4x$. There are exactly $(p-1)/2$ distinct elements in F_p, namely $y_1 = a^2+4x_1$, $y_2 = a^2+4x_2, \ldots, y_{(p-1)/2} = a^2+4x_{(p-1)/2}$, such that $y_i^{(p-1)/2} = -1$ for $i = 1, 2, \ldots (p-1)/2$. This means that $x_1, \ldots, x_{(p-1)/2}$ are roots of $S_p(a, x)$. Since the degree of $S_p(a, x)$ is $(p-1)/2$, the theorem is evident.

COROLLARY. *For every odd prime p and positive integer n, the polynomial $S_{n(p+1)-1}(a, x)$ over F_p has at least $(p-1)/2$ solutions in F_p.*

Proof. Since the polynomial $S_p(a, x)$ has distinct $(p-1)/2$ roots in F_p and

$$S_{n(p+1)-1}(a, x) \equiv 0 \pmod{S_p(a, x)}$$

the corollary is valid.

LEMMA 9. *For every odd prime p, the polynomial x^2-ax-b is irreducible over F_p if and only if $S_p(a, b)=0$.*

Proof. By the Lemma 6, we have in F_p that $S_p(a, b)=a[(a^2+4b)^{(p-1)/2}+1](p+1)/2$. A root of x^2-ax-b is $\alpha=(a+\sqrt{a^2+4b})/2$. If x^2-ax-b is irreducible over F_p, then a^2+4b is a non-quadratic residue *mod* p and $(a^2+4b)^{(p-1)/2}=-1$ in F_p. This means that $S_p(a, b)=0$. Conversely, assume that $S_p(a, b)=0$. Then we have $(a^2+4b)^{(p-1)/2}=-1$ and α belongs to the splitting field of x^2-ax-b. So x^2-ax-b is irreducible over F_p.

LEMMA 10. *Let $f(x)=x^2-ax-b$ be irreducible over F_p. Then the order of $f(x)$ is equal to the order of the matrix $A=\begin{bmatrix}0 & b\\ 1 & a\end{bmatrix}$ in the general linear group $GL(2, F_p)$ and divides p^2-1.*

Proof. We will denote the order of $f(x)$ by $|f|$. Suppose that $|f|=r$ and t is an element in the splitting field of f which satisfies $x^2-ax-b=0$. Then $t^2=at+b$ and straightforward calculation shows that $t^r=[aS_{r-1}(a, b)]t+bS_{r-2}(a, b)$. Since $t^r=1$, this means that $S_{r-1}(a, b)=0$ and $bS_{r-2}(a, b)=1$, so by the Lemma 1 we have that $A^r=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$. If f is irreducible over F_p, then $S_p(a, b)=0$. So we have that $t^{p+1}=bS_{p-1}(a, b)=-b$. This means that $t^{p^2-1}=1$ and $|f| \mid (p^2-1)$.

In [2] I had proved that if $f(x)=x^2-x-a$ is irreducible over F_p, p is a prime, and $S(f)$ (*Shinwon number or subperiod of* f) $=p+1$, then $g=x^{p+1}-x-a$ is irreducible over F_p.

S. D. Cohen [1] has showed the more general result: if $f(x)=\sum_{i=0}^{m} a_i x^i$ is an irreducible polynomial over F_q with subperiod M, then the degree of every irreducible factor of $f^*(x) = \sum_{i=0}^{m} a_i x^{(q^i-1)/q-1}$ is M.

By these, we have the following fact. If $f=x^2-ax-b$ is irreducible over F_p and $S(f)=p+1$, then $g=x^{p+1}-ax-b$ is also irreducible over F_p.

LEMMA 11. *Let a be a non-zero fixed element of F_p. If the irreducible polynomial $f(x)=x^2-ax-b$ over F_p has $S(f)=r$, then $S_{r-1}(a,b)=0$ and $|f|=r\cdot Ord(bS_{r-2}(a,b))$ where $Ord(bS_{r-2}(a,b))$ is the order of $bS_{r-2}(a,b)$ in the multiplicative group F_p.*

Proof. Since $S(f)=r$, there exists some $d\in F_p$ such that $f(x)$ divides x^r-d. Let t be an element which satisfies the polynomial $f=x^2-ax-b$, then $t^2=at+b$ and $t^r=d$. So, $t^r=[aS_{r-1}(a,b)]t+bS_{r-2}(a,b)=d$ means that $S_{r-1}(a,b)=0$ and $bS_{r-2}(a,b)=d$. Since $t^r=d$, we have that $|f|=r\cdot$ Ord(d).

LEMMA 12. *Let p be an odd prime such that $p=2n-1$ for some n. If the polynomial $f=x^2-ax-b$ is irreducible over F_p and has $S(f)=p+1$, then $D_n(a,b)=0$.*

Proof. By the Lemma 7 we have that

$$S_p(a,b)=S_{2n-1}(a,b)=S_{n-1}(a,b)D_n(a,b).$$

Suppose that the polynomial $f=x^2-ax-b$ is irreducible over F_p. Then $S_p(a,b)=S_{n-1}(a,b)D_n(a,b)=0$. If $S_{n-1}(a,b)=0$ then $S(f)=n$. But this contradicts to $S(f)=p+1=2n$. Hence $D_n(a,b)=0$.

THEOREM 4. *Let a be a non-zero fixed element of F_p and p an odd prime such that $p=2n-1$ for some n. Then there exists an element b in F_p such that the polynomial $f(x)=x^2-ax-b$ over F_p has $S(f)=p+1$.*

Proof. Since the polynomial $S_p(a,x)$ splits over F_p and $S_p(a,x)=S_{n-1}(a,x)D_n(a,x)$, the polynomial $D_n(a,x)$ splits over F_p. By the Lemma 8 $D_n(a,x)$ has not any $S_r(a,x)$ as a factor. If $D_n(a,x)$ does not contain any polynomial $D_r(a,x)$ for $r\geqslant 2$ as a factor, then for every root b of $D_n(x,a)$ in F_p we have that $S(f)=p+1$ where $f=x^2-ax-b$. If $D_n(a,x)$ contains the factors $D_{r_1}(a,x),\dots, D_{r_i}(a,x)$, then $D_n(a,x)$ is of the form $D_n(a,x)=h(a,x)D_{r_1}(a,x)\cdots D_{r_i}(a,x)$ where $\deg h(a,x)\geqslant 1$. Since $h(a,x)$ splits over F_p, $h(a,x)$ has a root b in F_p and for the polynomial $f=x^2-ax-b$ we have that $S(f)=p+1$.

References

1. S.D. Cohen, *Reducibility of sub-linear polynomials over a finite field*, Bull. Korean Math. Soc. **22**(1985) 53-56.
2. S.W. Kang, *Remarks on finite fields*, Bull. Korean Math. Soc. **20**(1983), 81-85.
3. S.W. Kang, *Remarks on finite fields II*, Bull. Korean Math. Soc. **22**(1985) 37-41.
4. R. Lidl and H. Niederreiter, *Finte fields*, Cambridge University Press, 1984.

Hanyang University
Seoul 133, Korea