Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Pier Vittorio Ceccherini

Some new results on certain finite structures

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **56** (1974), n.6, p. 840–855.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1974_8_56_6_840_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

Articolo digitalizzato nel quadro del programma bdim (Biblioteca Digitale Italiana di Matematica) SIMAI & UMI

http://www.bdim.eu/

Algebra. — *Some new results on certain finite structures* (*). Nota di PIER VITTORIO CECCHERINI (**), presentata (***) dal Socio B. SEGRE.

RIASSUNTO. — Ogni anello qui considerato viene assunto finito, commutativo ed unitario. Sotto opportune ipotesi ulteriori per l'anello, viene calcolato il numero delle funzioni polinomiali e quello delle funzioni polinomiali biunivoche; nel caso generale, vengono fornite alcune stime per i numeri anzidetti. Ciò conduce, fra l'altro, a teoremi di esistenza per «reti» $K_{1,N,k}$ (nel senso geometrico introdotto da B. Segre [10]) e per gruppi transitivi $G_{1,N,k}$, nonché a teoremi di esistenza per gli 1-disegni e per le configurazioni associati a quelli. Vengono infine determinati i binomi «minimi» del tipo $X^k - X^h$ che svaniscono sull'anello. Ulteriori precisazioni sul contenuto del lavoro trovansi nell'Introduzione.

1. INTRODUCTION

Every ring A under consideration will be finite, commutative with unit. We study:

the set Map (A^n, A) (A^n = n-th cartesian power of the set A),
the set Pol (A^n, A) of all $f \in$ Map (A^n, A) induced by an $F(\mathbf{X}) \in A[X_1, \cdots, X_n]$,
the set Trs $(A^n, A) =$ Map (A^n, A) — Pol (A^n, A),
the set Per (A) of all permutations on A,
the set PPer $(A) =$ Pol $(A, A) \cap$ Per (A),
the set TPer $(A) =$ Per (A) — PPer (A).

Let us write

$$\mu_{(n)}(A) = |\operatorname{Map}(A^n, A)| \quad , \quad \pi_{(n)}(A) = |\operatorname{Pol}(A^n, A)| \quad , \quad \tau_{(n)}(A) = |\operatorname{Trs}(A^n, A)| ,$$

$$\rho_P(A) = |\operatorname{PPer}(A)| \quad , \quad \rho_T(A) = |\operatorname{TPer}(A)| .$$

It is well known [5] that if A is a finite field, then $\pi_{(n)}(A) = \mu_{(n)}(A)$ and that $\pi_{(1)}(A) = \mu_{(1)}(A)$ iff A is a finite field [2], [7], [8]; moreover, if $A = Z_m$, the values $\pi_{(1)}(A)$, $\rho_P(A)$ are well known too [4], [3].

We prove that $\pi_{(n)}(A) = \mu_{(n)}(A)$ iff A is a finite field and that the functions $\pi_{(n)}$ and ρ_P are multiplicative. This leads to calculating the values of $\pi_{(n)}(A)$, of $\tau_{(n)}(A)$ and of $\rho_P(A)$ for certain rings A; in the general case, some estimations of those numbers are given.

We also prove that Pol (A, A) and Trs (A, A) act as 1-transitive sets of maps $A \to A$ with indices $\pi_{(1)}(A)/|A|$ and $\tau_{(1)}(A)/|A|$ resp.; moreover PPer (A) acts as a 1-transitive group of permutations on A with index $\rho_P(A)/|A|$; TPer (A) acts as a 1-transitive set of permutations on A with index $\rho_T(A)/|A|$. In this way we obtain several existence theorems for transitive groups $G_{1,k,N}$ and for nets $K_{1,k,N}$ (in the geometrical meaning introduced by B. Segre), thus partially answering a problem raised by B. Segre; other existence theorems for certain tactical configurations can be deduced.

Finally "minimal" binomials of the type $X^k - X^h$ which vanish over the ring A are determined.

(*) Work included in the activities of Section 4 of the G.N.S.A.G.A. of the C.N.R.

(**) Partially supported by a grant of the Royal Society (London) in connection with the Accademia Nazionale dei Lincei (Rome).

(***) Nella seduta del 29 giugno 1974.

2. INTRODUCTORY RESULTS

2.1. Let A be any finite commutative ring with unit 1, D the subset of A including 0 and all the zero divisors of A (if there are any); let $U = A - D$ and $\mathrm{Rad}\, A = \sqrt{0}$ be the set of nilpotent elements of A. Then:

(*a*) U is the group of units of A (i.e. D is the set of the non-invertible elements of A).

(*b*) A is a field iff $D = \{0\}$.

(*c*) The following relations hold:

$$D \cdot A = D \quad , \quad U \cdot U^{-1} = U \quad , \quad -D = D \quad , \quad -U = U .$$

(*d*) Each ideal I ($\neq$ A) of A is contained in D.

(*e*) An ideal I of A is prime iff it is maximal.

(*f*) A is a noetherian and artinian ring.

(*g*) The following conditions are equivalent:

(g_1) A is a primary ring (with prime ideal D),

(g_2) A is a local ring (with maximal ideal D),

(g_3) D is an ideal of A,

(g_4) $D = \mathrm{Rad}\, A$,

(g_5) Every idempotent of A is either 0 or 1.

(*h*) If A satisfies one of the conditions (*g*), then $|A|$ and $|D|$ are both powers of the characteristic p of the residual field A/D.

(*i*) $|A|$ is of the form p^h iff char A is of the form p^k (p prime).

(*j*) A is the direct sum of local (i.e. primary) rings and this decomposition is unique, with the number of summands equal to the number of prime ideals of A, each of these being an isolated prime ideal of (0). Moreover if

$$(j_1) \qquad A = A_1 \oplus A_2 \oplus \cdots \oplus A_s \qquad (A_i \text{ local ring})$$

is such a decomposition, then

$$(j_2) \qquad \mathrm{Rad}\, A = D(A_1) \oplus D(A_2) \oplus \cdots \oplus D(A_s)$$

where $D(A_i)$ is the maximal ideal of A_i, and

$$(j_3) \qquad U(A) = U(A_1) \otimes U(A_2) \otimes \cdots \otimes U(A_s) .$$

Here U(A)—the group of units of A—is cyclic iff each $U(A_i)$ is cyclic and

$$|U(A_1)| \quad , \quad |U(A_2)|, \cdots, |U(A_s)|$$

are coprime in pairs.

$$(j_4) \qquad \varphi(A) = \prod_{i=1}^{s} \varphi(A_i)$$

(multiplicativity of the *Euler generalized function* defined by $\varphi(A) = |U(A)|$).

(*k*) With respect to (j_1), $\mathrm{Rad}\, A = \{0\}$ iff $A_1, A_2, \cdots, A_s$ are fields. In particular

$$(k_1) \qquad A/\mathrm{Rad}\, A = \bigoplus_{i=1}^{s} A_i/D(A_i)$$

is a direct sum of fields.

(*l*) If A is a subring of a finite ring B, then $D(A) = D(B) \cap A$, $U(A) = U(B) \cap A$, $\mathrm{Rad}\, A = A \cap \mathrm{Rad}\, B$, and U(A) is subgroup of U(B).

(*m*) For each $N = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}$ and for each s such that $k \leq s \leq h_1 + h_2 + \cdots + h_k$, there exists a ring A with N elements and having s local summands according to (j_1).

(*n*) If A is local, then char $A \leq$ char $(A/D) \cdot |D|$.

(*o*) If A is local, then char $A = p^2$ iff $|D| = p$ (p prime).

Proof. Each statement is quite trivial, and the proofs are left to the reader. We note only that (j) may be deduced from elementary properties of artinian rings (cf. [11], p. 205) of from elementary properties of noetherian rings (cf. [11], p. 213).

Let $A[X]$ and $A[X_1, X_2, \cdots, X_n]$ be the rings of polynomials over A in the indeterminates X and $X_1, X_2, \cdots, X_n$ resp.

If S, S' are any sets, let $\mathrm{Map}(S, S')$ denote the set of all functions $S \to S'$. We shall be interested in the cases when $S' = A$ and $S = A^n = A \times A \times \cdots \times A \, (n \geq 1)$ or S is any overring of A. It is clear that $\mathrm{Map}(A, A)$ and, more generally, $\mathrm{Map}(A^n, A)$ become rings in the natural way and that each polynomial $F(\mathbf{X}) \in A[X_1, X_2, \cdots, X_n]$ induces a function $f \in \mathrm{Map}(A^n, A)$ defined by $f(\boldsymbol{c}) = F(\boldsymbol{c}) \; (\boldsymbol{c} \in A^n)$. In this way we get a ring morphism

$$\alpha: \; A[X_1, X_2, \cdots, X_n] \to \mathrm{Map}(A^n, A) \qquad (\alpha(F(\mathbf{X})) = f)$$

the kernel of which will be denoted by

$$I(A^n) = \{F(\mathbf{X}) \in A[X_1, X_2, \cdots, X_n] \mid \boldsymbol{c} \in A^n \Rightarrow F(\boldsymbol{c}) = 0\} ;$$

in the following we write

$$\mathrm{Pol}(A^n, A) \qquad \text{for} \quad \mathrm{Im}\, \alpha,$$

and say that $f \in \mathrm{Map}(A^n, A)$ is a *polynomial* or a "*trascendental*" *function* according as

$$f \in \mathrm{Pol}(A^n, A) \qquad \text{or} \quad f \in \mathrm{Trs}(A^n, A) = \mathrm{Map}(A^n, A) - \mathrm{Pol}(A^n, A) .$$

By the first homomorphism theorem (applied to α) we get:

2.2. The ring $A[X_1, X_2, \cdots, X_n]$ is divided into equivalence classes by

$$F(\mathbf{X}) \sim G(\mathbf{X}) \qquad \text{iff} \;\; f = g .$$

Further $\mathrm{Pol}(A^n, A)$ is a subring of $\mathrm{Map}(A^n, A)$ and

$$\mathrm{Pol}(A^n, A) \simeq A[X_1, X_2, \cdots, X_n]/I(A^n) .$$

In particular $|\mathrm{Pol}(A^n, A)|$ is a divisor of $|\mathrm{Map}(A^n, A)|$, so that $|\mathrm{Pol}(A^n, A)|$ is also a divisor of $|\mathrm{Trs}(A^n, A)|$.

We shall also be interested in the sets:

$$\mathrm{Per}(A) = \{f \in \mathrm{Map}(A, A) \mid f \text{ is a bijection}\} ,$$

$$\mathrm{PPer}(A) = \mathrm{Pol}(A, A) \cap \mathrm{Per}(A) \quad , \quad \mathrm{TPer}(A) = \mathrm{Trs}(A, A) \cap \mathrm{Per}(A).$$

2.3. $\mathrm{PPer}(A)$ is a subgroup of $\mathrm{Per}(A)$, with respect to composition of functions. In particular $|\mathrm{PPer}(A)|$ is a divisor of $|\mathrm{Per}(A)| = |A|!$, so that $|\mathrm{PPer}(A)|$ is also a divisor of $|\mathrm{TPer}(A)|$.

Proof. It is enough to show that if $f, g \in \mathrm{PPer}(A)$ then $f \circ g \in \mathrm{PPer}(A)$. If $F(X), G(X) \in A[X]$ induce f, g then $F(G(X))$ induces $f \circ g$.

Let us note that:

2.4. The ring $\mathrm{Pol}(A^n, A)$ is never a field. However $\mathrm{Pol}(A^n, A)$ is a direct sum of fields if, and only if, A is a direct sum of fields.

Proof. $\mathrm{Pol}(A^n, A)$ is never a field because 2.2 holds and $I(A^n)$ is never a maximal ideal: for instance

$$I(A^n) \subset \{F(\mathbf{X}) \in A[X_1, X_2, \cdots, X_n] \mid F(\mathbf{o}) = 0\} \subset A[X_1, X_2, \cdots, X_n].$$

For the second part, it is enough, using 2.1 (*k*), to show that

$$\mathrm{Rad}\,A = \{0\} \qquad \text{iff} \quad \mathrm{Rad}(\mathrm{Pol}(A^n, A)) = \{0\}.$$

Because $A \hookrightarrow \mathrm{Pol}(A^n, A) = B$, say, by 2.1 (*l*) it is enough to proof that $\mathrm{Rad}\,A = \{0\} \Rightarrow \mathrm{Rad}\,B = \{0\}$. Now, if $f \in \mathrm{Rad}\,B$ then $f^k = 0$ for some integer $k \geq 1$; i.e. $f(\boldsymbol{c})^k = 0$ for every $\boldsymbol{c} \in A^n$, so that $f(\boldsymbol{c}) \in \mathrm{Rad}\,A$ for each $\boldsymbol{c} \in A^n$. Because $\mathrm{Rad}\,A = \{0\}$, it follows that $f(\boldsymbol{c}) = 0$ for each $\boldsymbol{c} \in A^n$, i.e. $f = 0$. Thus $\mathrm{Rad}\,B = \{0\}$.

We note also that, because $A \hookrightarrow \mathrm{Pol}(A^n, A)$ and in virtue of 2.1 (*l*), the following.

2.5. If $U(\mathrm{Pol}(A^n, A))$ is cyclic, then $U(A)$ is cyclic. (The converse is not true: take $n = 1$, $A = GF(q)$, $q \neq 2$).

2.6. If $A = \bigoplus_{i=1}^{s} A_i$ is any decomposition of A as a direct sum of rings, then:

(*a*) $A[X_1, X_2, \cdots, X_n] \simeq \bigoplus_{i=1}^{s} A_i[X_1, X_2, \cdots, X_n]$

(*b*) $\mathrm{Pol}(A^n, A) \simeq \bigoplus_{i=1}^{s} \mathrm{Pol}(A_i^n, A_i)$,

(*c*) $\mathrm{PPer}(A) \simeq \bigotimes_{i=1}^{s} \mathrm{PPer}(A_i)$.

Proof. (*a*) Trivial. (*b*) By 2.2 it follows that

$$\mathrm{Pol}(A^n, A) \simeq A[X_1, X_2, \cdots, X_n]/I(A^n) \simeq$$

$$\left(\bigoplus_{i=1}^{s} A_i[X_1, X_2, \cdots, X_n]\right) \Big/ \bigoplus_{i=1}^{s} I(A_i^n) \simeq$$

$$\simeq \bigoplus_{i=1}^{s} A_i[X_1, X_2, \cdots, X_n]/I(A_i^n) \simeq \bigoplus_{i=1}^{s} \mathrm{Pol}(A_i^n, A_i).$$

(*c*) By (*b*) $\mathrm{Pol}(A, A) \simeq \bigoplus_{i=1}^{s} \mathrm{Pol}(A_i, A_i)$; define the isomorphism

$$\beta : \bigoplus_{i=1}^{s} \mathrm{Pol}(A_i, A_i) \to \mathrm{Pol}(A, A) \qquad \text{by} \quad \beta\left(\sum_{i=1}^{s} f_i\right) = \sum_{i=1}^{s} f_i\, pr_i,$$

where $f_i \in \mathrm{Pol}(A_i, A_i)$ and pr_i is the projection of A onto A_i.

Then $\Sigma f_i\, pr_i$ is a permutation on A iff each f_i is a permutation on A_i. So β induces a group isomorphism (with respect to composition of functions)

$$\beta' : \bigotimes_{i=1}^{s} \mathrm{PPer}(A_i) \to \mathrm{PPer}(A)$$

and (*c*) follows.

We can reformulate 2.6 as in the following 2.7 (of which a direct proof is possible without using 2.2).

2.7. Let $A = \bigoplus_{i=1}^{s} A_i$ be any decomposition of A as a direct sum of rings. Then define a function

$$\beta : \bigoplus_{i=1}^{s} \mathrm{Map}\,(A_i^n, A_i) \to \mathrm{Map}\,(A^n, A)$$

taking $\beta\left(\sum_{i=1}^{s} f_i\right) = \sum_{i=1}^{s} f_i\, Pr_i$, where $f_i \in \mathrm{Map}\,(A_i^n, A_i)$ and $Pr_i : A^n \to A_i^n$ is defined by $Pr_i = \bigotimes_{j=1}^{n} pr_i$, i.e. for $\boldsymbol{a} = (a_1, a_2, \cdots, a_n) \in A^n$, $Pr_i\,\boldsymbol{a} = (pr_i\,a_1, pr_i\,a_2, \cdots, pr_i\,a_n)$. Then:

(i) β is a ring monomorphism,

(ii) $\beta\left(\sum_{i=1}^{s} f_i\right)$ surjective $\Longleftrightarrow f_j$ surjective $\quad (j = 1, 2, \cdots, s)$,

(iii) $\beta\left(\sum_{i=1}^{s} f_i\right)$ injective $\Longleftrightarrow f_j$ injective $\quad (j = 1, 2, \cdots, s)$.
(impossible unless $n = 1$)

Let us now introduce the following notation:
$N = |A|$, $\delta = |D|$, $u = |U| = \varphi(A)$, $\mu_{(n)} = |\mathrm{Map}\,(A^n, A)|$, $\pi_{(n)} = |\mathrm{Pol}\,(A^n, A)|$, $\tau_{(n)} = |\mathrm{Trs}\,(A^n, A)|$, $\rho = |\mathrm{Per}\,(A)|$, $\rho_P = |\mathrm{PPer}\,(A)|$, $\rho_T = |\mathrm{TPer}\,(A)|$, $\nu_{(n)} = [\mathrm{Map}\,(A^n, A)^{(+)} : \mathrm{Pol}\,(A^n, A)^{(+)}]$ (= the number of cosets of Pol (A^n, A) in Map (A^n, A) considered as additive groups).

From the preceding discussion it follows that:

$\mu_{(n)} = \tau_{(n)} + \pi_{(n)} = \pi_{(n)}\,\nu_{(n)} = N^{N^n}$, $\pi_{(n)}(\nu_{(n)} - 1) = \tau_{(n)}$, $\pi_{(n)} \mid \mu_{(n)}$, $\pi_{(n)} \mid \tau_{(n)}$, $\rho = \rho_P + \rho_T = N!$, $\rho_P \mid \rho$, $\rho_P \mid \rho_T$. For simplicity write $\tau_{(1)} = \tau$, $\pi_{(1)} = \pi$, $\nu_{(1)} = \nu$, $\mu_{(1)} = \mu$ and $\pi_{(n)}(A)$ etc. wherever confusion about the ring could arise. 2.6, (*b*), (*c*) immediately give the following important result:

2.8. The functions $\pi_{(n)}$ and ρ_P are multiplicative. More precisely, if $A = \bigoplus_{i=1}^{s} A_i$ is any decomposition of A as direct sum of rings then

$$\pi_{(n)}(A) = \prod_{i=1}^{s} \pi_{(n)}(A_i) \quad , \quad \rho_P(A) = \prod_{i=1}^{s} \rho_P(A_i) .$$

2.9. The values of $\pi_{(n)}(A)$ and of $\rho_P(A)$ can be easily calculated in the following cases:

(*a*) A is a field; (*b*) $A = \bigoplus_{i=1}^{s} GF(q_i)$;

(*c*) $A = \mathbf{Z}_N\,(N \geq 2)$, if $n = 1$; (*d*) $A = \bigoplus_{j=1}^{t} \mathbf{Z}_{N_j}$ $(N_j \geq 2)$, if $n = 1$;

(*e*) $A = \left(\bigoplus_{i=1}^{s} GF(q_i)\right) \oplus \left(\bigoplus_{j=1}^{t} \mathbf{Z}_{N_j}\right)$ $(N_j \geq 2)$, if $n = 1$.

Therefore also $\tau_{(n)}(A)$ and $\rho_T(A)$ can be calculated by

$$\tau_{(n)}(A) = \mu_{(n)}(A) - \pi_{(n)}(A) = N^{N^n} - \pi_{(n)}(A),$$
$$\rho_T(A) = \rho(A) - \rho_P(A) = N! - \rho_P(A).$$

More precisely, in the respective cases

(*a*) $\pi_{(n)}(A) = \mu_{(n)}(A) = N^{N^n} \quad , \quad \rho_P(A) = \rho = N!,$

(*b*) $\pi_{(n)}(A) = \prod_{i=1}^{s} q_i^{q_i^n} \quad , \quad \rho_P(A) = \prod_{i=1}^{s} q_i!$

(*c*)

(c_1) N prime. This is case (*a*) with $s = 1$, $q_1 = N$;

(c_2) $N = p^2$, p prime. Then

$$\pi(Z_{p^2}) = p^{3p} \quad , \quad \rho_P(Z_{p^2}) = p!\,(p-1)^p p^p$$

(c_3) $N = p^h$, p prime, $h > 2$. Let $\eta(h) = \sum_{j=3}^{h} \beta(j)$, where $\beta(j)$ is the smallest integer t such that $p^j \mid t!$. Then

$$\pi(Z_{p^h}) = p^{3p+\eta(h)} \quad , \quad \rho_P(Z_{p^h}) = p!\,p^p(p-1)^p p^{\eta(h)};$$

(c_4) N any integer, say $N = \prod_{j=1}^{t} p_j^{r_j}$, p_j distinct primes. Then

$$\pi(Z_N) = \prod_{j=1}^{t} p_j^{3p_j+\eta(r_j)} \quad , \quad \rho_P(Z_N) = \prod_{j=1}^{t} p_j!\,(p_j-1)^{p_j} p_j^{\eta(r_j)+p_j}$$

(*d*) $\pi(A) = \prod_{j=1}^{t} \pi(Z_{N_j}) \quad , \quad \rho_P(A) = \prod_{j=1}^{t} \rho_P(Z_{N_j}),$

(*e*) $\pi(A) = \prod_{i=1}^{s} \pi(GF(q_i)) \prod_{j=1}^{t} \pi(Z_{N_j}) \quad , \quad \rho_P(A) = \prod_{j=1}^{s} \rho_P(GF(q_i)) \prod_{j=1}^{t} \rho_P(Z_{N_j}),$

where – in (*d*), (*e*) – the explicit values are given by (*a*), (c_4).

Proof. The case (*a*) follows from the next 4.4; (*b*) follows from (*a*) and 2.8; (c_2) and (c_3) were proved by [3] (cf. also [4]); (c_4) follows from (c_2), (c_3), 2.8; (*d*) follows from (c_4), 2.8; (*e*) follows from (*b*), (c_4), 2.8.

3. FINITE RINGS AND TRANSITIVE SETS OF FUNCTIONS

If S is any set with N elements, the following standard notation will be used:

$H_{t,N,k}$ for any subset of Map (S, S), which is *t*-transitive with index *k*;

$K_{t,N,k}$ for any subset of Per (S), which is *t*-transitive with index *k*;

$G_{t,N,k}$ for any subgroup of Per (S) (with respect to composition of functions), which is *t*-transitive with index *k*.

3.1. If A is a ring with N elements, then:

(*a*) $\mathrm{Pol}(\mathrm{A}, \mathrm{A}) = \mathrm{H}_{1,\mathrm{N},\pi/\mathrm{N}}$; (*b*) $\mathrm{Trs}(\mathrm{A}, \mathrm{A}) = \mathrm{H}_{1,\mathrm{N},\tau/\mathrm{N}}$;

(*c*) $\mathrm{PPer}(\mathrm{A}) = \mathrm{G}_{1,\mathrm{N},\rho_{\mathrm{P}}/\mathrm{N}}$; (*d*) $\mathrm{TPer}(\mathrm{A}) = \mathrm{K}_{1,\mathrm{N},\rho_{\mathrm{T}}/\mathrm{N}}$.

Proof. (*a*) For any $a, b, c \in \mathrm{A}$, let $\mathrm{P}_b^a = \{f \in \mathrm{Pol}(\mathrm{A}, \mathrm{A}) \mid f(a) = b\}$. Putting $\psi : f \to f + c - b$ defines a bijection (the inverse map is obvious) $\psi : \mathrm{P}_b^a \to \mathrm{P}_c^a$ which gives $|\mathrm{P}_b^a| = |\mathrm{P}_c^a|$. Thus $|\mathrm{P}_b^a| = \pi/\mathrm{N}$, because each of the N elements of A is the image of a under some element of Pol (A , A).

(*b*) Proceed in a similar way as for (*a*), or instead by observing that, putting

$$\mathrm{T}_b^a = \{f \in \mathrm{Trs}(\mathrm{A}, \mathrm{A}) \mid f(a) = b\},$$

we have

$$|\mathrm{T}_b^a| = |\{f \in \mathrm{Map}(\mathrm{A}, \mathrm{A}) \mid f(a) = b\} - \mathrm{P}_b^a| = \mathrm{N}^{\mathrm{N}-1} - \pi/\mathrm{N} = (\mathrm{N}^{\mathrm{N}} - \pi)/\mathrm{N} = \tau/\mathrm{N}.$$

(*c*) PPer (A) is a subgroup of Per (A), by 2.3 (with respect to composition of functions). Let a, b, c be any elements of A and let $\mathfrak{S}_b^a = \{f \in \mathrm{PPer}(\mathrm{A}) \mid f(a) = b\}$. The bijection $\psi : \mathrm{P}_b^a \to \mathrm{P}_c^a$ considered in (*a*) induces a bijection $\psi' : \mathfrak{S}_b^a \to \mathfrak{S}_c^a$; each of the N elements of A is the image of a under some element of PPer (A), so that $|\mathfrak{S}_b^a| = \rho_{\mathrm{P}}/\mathrm{N}$.

(*d*) Let a, b be any elements of A, and put $\mathfrak{T}_b^a = \{f \in \mathrm{TPer}(\mathrm{A}) \mid f(a) = b\}$. Then $|\mathfrak{T}_b^a| = |\{f \in \mathrm{Per}(\mathrm{A}) \mid f(a) = b\} - \mathfrak{S}_b^a| = (\mathrm{N} - 1)! - \rho_{\mathrm{P}}/\mathrm{N} = (\mathrm{N}! - \rho_{\mathrm{P}})/\mathrm{N} = \rho_{\mathrm{T}}/\mathrm{N}$.

From 3.1 and from 2.9 (with $n = 1$), it follows that:

3.2. (*a*) For any integer $\mathrm{N} = q_1 q_2 \cdots q_s$ (whatever the decomposition of N into primary integers, whether standard or not) there exist:

$$(a_1) \quad \mathrm{H}_{1,\mathrm{N},q_1^{q_1-1} q_2^{q_2-1} \cdots q_s^{q_s-1}} = \mathrm{Pol}\left(\bigoplus_{i=1}^{s} \mathrm{GF}(q_i), \bigoplus_{i=1}^{s} \mathrm{GF}(q_i)\right);$$

$$(a_2) \quad \mathrm{H}_{1,\mathrm{N},\mathrm{N}^{\mathrm{N}-1} - q_1^{q_1-1} \cdots q_s^{q_s-1}} = \mathrm{Trs}\left(\bigoplus_{i=1}^{s} \mathrm{GF}(q_i), \bigoplus_{i=1}^{s} \mathrm{GF}(q_i)\right);$$

$$(a_3) \quad \mathrm{G}_{1,\mathrm{N},(q_1-1)!(q_2-1)!\cdots(q_s-1)!} = \mathrm{PPer}\left(\bigoplus_{i=1}^{s} \mathrm{GF}(q_i)\right);$$

$$(a_4) \quad \mathrm{K}_{1,\mathrm{N},(\mathrm{N}-1)!-(q_1-1)!(q_2-1)!\cdots(q_s-1)!} = \mathrm{TPer}\left(\bigoplus_{i=1}^{s} \mathrm{GF}(q_i)\right);$$

(*b*) For any prime p, there exist:

$$(b_1) \quad \mathrm{H}_{1,p^2,p^{3p-2}} = \mathrm{Pol}(\mathbf{Z}_{p^2}, \mathbf{Z}_{p^2});$$

$$(b_2) \quad \mathrm{H}_{1,p^2,(p^2)^{p^2-1}-p^{3p-2}} = \mathrm{Trs}(\mathbf{Z}_{p^2}, \mathbf{Z}_{p^2});$$

$$(b_3) \quad \mathrm{G}_{1,p^2,p!(p-1)^p p^{p-2}} = \mathrm{PPer}(\mathbf{Z}_{p^2});$$

$$(b_4) \quad \mathrm{K}_{1,p^2,(p^2-1)!-p!(p-1)^p p^{p-2}} = \mathrm{TPer}(\mathbf{Z}_{p^2});$$

(*c*) For any prime p and for any integer $n > 2$, there exist:

(c_1) $H_{1,p^n,p^{3p+\eta(n)-n}} = \mathrm{Pol}(\mathbf{Z}_{p^n}, \mathbf{Z}_{p^n})$;

(c_2) $H_{1,p^n,(p^n)^{p^n-1}-p^{3p+\eta(n)-n}} = \mathrm{Trs}(\mathbf{Z}_{p^n}, \mathbf{Z}_{p^n})$;

(c_3) $G_{1,p^n,p!(p-1)^p p^{p+\eta(n)-n}} = \mathrm{PPer}(\mathbf{Z}_{p^n})$;

(c_4) $K_{1,p^n,(p^n-1)!-p!(p-1)^p p^{p+\eta(n)-n}} = \mathrm{TPer}(\mathbf{Z}_{p^n})$;

(*d*) For any $\mathrm{N} = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$, p_j distinct primes, there exist:

(d_1) $H_{1,\mathrm{N},\prod_{i=1}^{s} p_i^{3p_i+\eta(r_i)-r_i}} = \mathrm{Pol}(\mathbf{Z}_\mathrm{N}, \mathbf{Z}_\mathrm{N})$;

(d_2) $H_{1,\mathrm{N},\mathrm{N}^{\mathrm{N}-1}-\prod_{i=1}^{s} p_i^{3p_i+\eta(r_i)-r_i}} = \mathrm{Trs}(\mathbf{Z}_\mathrm{N}, \mathbf{Z}_\mathrm{N})$;

(d_3) $G_{1,\mathrm{N},\prod_{i=1}^{s} p_i!(p_i-1)^{p_i} p_i^{p_i+\eta(r_i)-r_i}} = \mathrm{PPer}(\mathbf{Z}_\mathrm{N})$;

(d_4) $K_{1,\mathrm{N},(\mathrm{N}-1)!-\prod_{i=1}^{s} p_i!(p_i-1)^{p_i} p_i^{p_i+\eta(r_i)-r_i}} = \mathrm{TPer}(\mathbf{Z}_\mathrm{N})$.

N. B. (*d*) holds also if the p_j's are not distinct: replace $\mathbf{Z}_\mathrm{N}$ by $\bigoplus_{i=1}^{s} \mathbf{Z}_{p_i}^{r_i}$.

3.3. (i) If any $K_{t,\mathrm{N},k}$ exists, then a $K_{1,\mathrm{N}-t+1,k}$ exists;

(ii) Moreover: $K_{t,\mathrm{N},k} = K_{1,\mathrm{N},k(\mathrm{N}-1)(\mathrm{N}-2)\cdots(\mathrm{N}-t+1)}$;

(iii) As (i), (ii) but replacing K by G.

Proof. Cf. B. Segre [10], p. 79.

3.4. The following groups $G_{1,\mathrm{N},k}$ exist:

(*a*) $G_{1,\mathrm{N},1}$ for all integers $\mathrm{N} \geq 1$;

(*b*) $G_{1,\mathrm{N},(\mathrm{N}-1)!}$ and (*c*) $G_{1,\mathrm{N},(\mathrm{N}-1)!/2}$ for all integers $\mathrm{N} \geq 3$;

(*d*) $G_{1,q,q-1}$ and (*e*) $G_{1,q+1,q(q-1)}$ for all primary integers q;

(*f*) $G_{1,11,720}$; (*g*) $G_{1,12,7920}$.

Proof. (*a*) Take $G_{1,\mathrm{N},1}$ as the group of right multiplications of a group of order N. (*b*) Apply 3.3 (i), (ii) to the symmetric group $G_{\mathrm{N}-1,\mathrm{N},1}$. (*c*) Apply 3.3 (i), (ii) to the alternating group $G_{\mathrm{N}-2,\mathrm{N},1}$. (*d*) Apply 3.3 (i), (ii) to a $G_{2,q,1}$ (which exists, cf. B. Segre [10], p. 151 and p. 79). (*e*) Apply 3.3 (i), (ii) to a $G_{3,q+1,1}$ (which exists, cf. B. Segre [10], p. 151). (*f*) Apply 3.3 (i), (ii) to the Mathieu group $G_{4,11,1}$. (*g*) Apply 3.3 (i), (ii) to the Mathieu group $G_{5,12,1}$.

From 3.1, 3.3, 2.8 it is possible to assert the existence of several other $H_{1,\mathrm{N},k}$, $K_{1,\mathrm{N},k}$, $G_{1,\mathrm{N},k}$, e.g. by considering rings of the type

$$\mathrm{A} = \bigoplus_{i=1}^{s} \mathrm{GF}(q_i) \oplus \bigoplus_{j=1}^{t} \mathrm{Z}_{\mathrm{N}_j}.$$

Other existence theorems arise from the following:

3.5. Let be S, S' any sets with $|S| = N$ and $|S'| = N'$ elements, $H' \subseteq \mathrm{Map}(S', S')$, $H \subseteq \mathrm{Map}(S, S)$, $K \subseteq \mathrm{Per}(S)$, $K' \subseteq \mathrm{Per}(S')$, $H'' = H \times H'$, $K'' = K \times K'$. Then:

(*a*) $H'' \subseteq \mathrm{Map}(S \times S', S \times S')$; (*b*) $K'' \subseteq \mathrm{Per}(S \times S')$;

(*c*) K, K' are groups iff K'' is a group;

(*d*) $H = H_{1,N,h}$, $H' = H'_{1,N',h'} \Rightarrow H'' = H''_{1,NN',hh'}$;

(*e*) $K = K_{1,N,k}$, $K' = K'_{1,N',k'} \Rightarrow K'' = K''_{1,NN',kk'}$;

(*f*) K'' group, $K'' = K''_{1,NN',k''} \Rightarrow K = G_{1,N,k}$ and $K' = G'_{1,N',k'}$ for suitable k, k' such that $kk' = k''$.

Proof. (*a*) $(f, f') \in H \times H'$ maps $(a, a') \in S \times S'$ to $(f(a), f'(a')) \in S \times S'$. (*b*) If $f \in H$, $f' \in H'$ are both bijective then $(f, f') \in H''$ is also. (*c*), (*d*), (*e*) are trivial. (*f*) By (*c*), K and K′ are groups; both are trivially transitive, so that (cf. e.g. B. Segre [9], 16.1.7) they must have some transitivity characters: $K = G_{t,N,k^0}$, $K' = G'_{t',N',k'^0}$. It follows (cf. 3.3, (iii)) that $K = G_{1,N,k}$ and $K' = G'_{1,N,k'}$, with $k = k^0 (N - 1) \cdots (N - t + 1)$ and $k' = k'^0 (N' - 1)(N' - 2) \cdots (N' - t' + 1)$. By (*e*) it follows that $kk' = k''$.

By 2.8, 3.2, 3.4, 3.5 several numerical examples of $H_{1,N,k}$, $K_{1,N,k}$, $G_{1,N,k}$ can be deduced. In particular we obtain several existence theorems for $K_{1,N,k}$, thus partially answering a problem raised by B. Segre [10], pp. 88–89. It is well known (cf. e.g. B. Segre [10], p. 283) that each $K_{1,N,k}$ gives rise to a design $1 - (N^2, Nk, N, k)$ i.e. to a *configuration*

$$(N^2_N, Nk_k);$$

this is defined as a set C of N^2 elements provided with a set S of Nk subsets of C such that each subset in S contains N elements of C, and each element of C belongs to k subsets in S. It follows that each existence theorem for a $K_{1,N,k}$ may be converted to an existence theorem for a configuration with the above parameters.

4. Estimations for the number of polynomial functions over finite rings

According to 2.2, it is clear that the polynomial functions of $\mathrm{Pol}(A^n, A)$ can all be obtained from $\pi_{(n)}(A)$ polynomials of $A[X_1, X_2, \cdots, X_n]$ (one in each equivalence class mod α); the following 4.1 asserts that it is enough to consider the $\mu_{(n)}$ polynomials of the "reduced type", i.e. the set

$$G_{(n)} = \{G(\mathbf{X}) \in A[X_1, X_2, \cdots, X_n] \mid G(\mathbf{X}) = 0$$

$$\text{or } G(\mathbf{X}) \text{ is of degree } \leq N - 1 \text{ in } X_j \text{ for } \forall j\}.$$

4.1. For each $F(\mathbf{X}) \in A[X_1, X_2, \cdots, X_n]$ there exists a $G(\mathbf{X}) \in G_{(n)}$ such that $F(\mathbf{X}) \sim G(\mathbf{X}) \bmod \alpha$.

Proof. Let $A = \{a_1, a_2, \cdots, a_N\}$. For every h, with $1 \leq h \leq n$, $(X_h - a_1)(X_h - a_2) \cdots \cdots (X_h - a_N) \sim 0$, and so, expanding,

$$X_h^N - E_h(X_h) \sim 0, \qquad \text{say},$$

where $E_h(X_h) \in G_{(n)}$. It follows that

$$X_h^N \sim E_h(X_h) \qquad \text{and then} \quad X_h^{N+j} \sim X^j E_h(X_h) \qquad (j = 1, 2, \cdots).$$

Applying these equivalences to each factor of every monomial of $F(\mathbf{X})$, one reduces $F(\mathbf{X})$ to an equivalent $G(\mathbf{X}) \in G_{(n)}$.

As noted $|G_{(n)}| = N^{N^n} = \mu_{(n)} = |\mathrm{Map}(A^n, A)|$.

4.2. The following conditions are equivalent:

(a_n) $\mathrm{Pol}(A^n, A) = \mathrm{Map}(A^n, A)$, i.e. $\pi_{(n)} = \mu_{(n)}$;

(b_n) Distinct polynomials of $G_{(n)}$ are inequivalent mod α.

(c_n) The only polynomial of $G_{(n)}$ which vanishes on each element of A^n is 0, i.e. $G_{(n)} \cap I(A^n) = \{0\}$.

Proof. Consider the following commutative diagram

$$\begin{tikzcd} G_{(n)} \arrow[r, two heads, "\gamma"] \arrow[dr, "\alpha"'] & \mathrm{Pol}(A^n, A) \arrow[r, hook, "\beta"] \arrow[d, leftrightarrow, "\delta"] & \mathrm{Map}(A^n, A) \\ & A[X_1, X_2, \cdots, X_n]/I(A^n) & \end{tikzcd}$$

where δ is the isomorphism mentioned in 2.2, α, γ are epimorphisms by 4.1, and β is the inclusion map.

α is mono (i.e. (b_n) holds) $\Longleftrightarrow \ker \alpha = G_{(n)} \cap I(A^n) = \{0\}$ (i.e. (c_n) holds). Moreover α is mono (i.e. (b_n) holds) $\Longleftrightarrow \gamma$ is mono $\Longleftrightarrow \gamma \circ \beta$ is mono $\Longleftrightarrow \beta$ is surjective (i.e. (a_n) holds) provided that $|G_{(n)}| = |\mathrm{Map}(A^n, A)|$ as noted above.

4.3. If some of the conditions (a_i), (b_i), (c_i) are satisfied for a given fixed integer $i \geq 1$, then each of the (a_n), (b_n), (c_n) is satisfied for every integer $n \geq 1$.

Proof. Without loss of generality, we can assume $i < n$. Let us consider the following commutative diagram.

$$\begin{tikzcd} G_{(i)} \arrow[r, hook, "\varepsilon"] \arrow[d, "\alpha_i"] & G_{(n)} \arrow[d, "\alpha_n"] \\ A[X_1, X_2, \cdots, X_i]/I(A^i) \arrow[r, hook, "\eta"] & A[X_1, X_2, \cdots, X_n]/I(A^n) \end{tikzcd}$$

where the α_i, α_n are the epimorphisms like α in 4.2, ε is the inclusion map, and η is the natural monomorphism, well defined and mono because $A[X_1, X_2, \cdots, X_i] \subset A[X_1, X_2, \cdots, X_n]$ and

$$I(A^i) = I(A^n) \cap A[X_1, X_2, \cdots, X_n].$$

α_i is mono (i.e. (b_i) holds) $\Longleftrightarrow \alpha_n$ is mono (i.e. (b_n) holds), and this proves the theorem by 4.2 (where n can take any integer value ≥ 1).

4.4. If A is a finite field with N elements, the conditions (a_n), (b_n), (c_n) hold for every $n \geq 1$. In particular

$$(a_n) \quad \mathrm{Pol}(A^n, A) = \mathrm{Map}(A^n, A), \quad \text{i.e.} \quad \pi_{(n)} = \mu_{(n)} = N^{N^n},$$

and $$(a_1) \quad \mathrm{Pol}(A, A) = \mathrm{Map}(A, A), \quad \text{i.e.} \quad \pi = \mu = N^N,$$

which implies

$$\mathrm{PPer}(A) = \mathrm{Per}(A), \quad \text{i.e.} \quad \rho_P = \rho = N!.$$

Proof. By 4.3 it is enough to show that (c_1) holds. If $G(X) \in G_{(1)}$ is non-zero (i.e. of degree $\leq N - 1$), then $G(X)$ cannot vanish over A, for otherwise it would have a number of roots, N, greater than its degree.

N. B. Another proof that (a_n) holds for finite fields can be found in [5].

4.5. If A is not a field, than none of the conditions (a_n), (b_n), (c_n) $(n \geq 1)$ is satisfied. Moreover $\mathrm{PPer}(A) \subset \mathrm{Per}(A)$.

Proof. By 4.3 it is enough to prove that (a_1) does not hold, i.e. that $\mathrm{Pol}(A, A) \subset \mathrm{Map}(A, A)$. Actually, the ring A contains zero divisors (cf. 2.1, (b)), and let be $d \in C$, $d \neq 0$. Let $f \in \mathrm{Map}(A, A)$ be such that $f(0) = 0$ and $f(d) \in U$; we assert that $f \notin \mathrm{Pol}(A, A)$. Otherwise let $F(X) \in A[X]$ be a polynomial inducing f; $F(0) = 0$ implies that $F(X)$ is of the type $F(X) = XF_1(X)$, with $F_1(X) \in A[X]$, and then $f(d) = F(d) = d \cdot F_1(d) \in D \cdot A = D$ (cf. 2.1, (c)), which contradicts the hypothesis $f(d) \in U$. Our assumption "$f(0) = 0$, $f(d) \in U$" may be taken also for $f \in \mathrm{Per}(A)$, so that $\mathrm{PPer}(A) \subset \mathrm{Per}(A)$.

N. B. Another proof that (a_1) does not hold for finite rings with zero divisors can be found in [2].

Summarizing 4.4 and 4.5 we get that:

4.6. The conditions (a_n), (b_n), (c_n) are satisfied (for every $n \geq 1$) if, and only if, the ring A is a finite field. Moreover $\mathrm{PPer}(A) = \mathrm{Per}(A)$ iff A is a field, i.e. $\rho_P = \rho = N!$ iff A is a field.

Our purpose now is to give some lower bounds for $\tau_{(n)}$, in the general case, i.e. some upper bounds for $\pi_{(n)}$. We begin with the case $n = 1$; the case $n \geq 1$ will be discussed in 4.12, 4.13.

4.7. $\tau \geq \lambda^{(1)} = N^N - \delta^{\delta-1} N^{u+1}$, i.e. $\pi \leq \delta^{\delta-1} N^{u+1}$. Moreover
$\rho_T \geq \sigma^{(1)} = N! - (\delta - 1)!\, u!\, N$, i.e. $\rho_P \leq (\delta - 1)!\, u!\, N$.

Proof. Consider the subset $F(0)$ of $\mathrm{Map}(A, A)$ defined by

$$F(0) = \{f \in \mathrm{Map}(A, A) \mid f(0) = 0 \text{ and } f(D) \nsubseteq D\}.$$

In the proof of 4.5, it was shown that $F(0) \subseteq \mathrm{Trs}(A, A)$. Clearly $F(0) = \{f \in \mathrm{Map}(A, A) \mid f(0) = 0\} - \{f \in \mathrm{Map}(A, A) \mid f(0) = 0$ and $f(D - \{0\}) \subseteq D\}$, so that $|F(0)| = |\mathrm{Map}(A - \{0\}, A)| - |\mathrm{Map}(D - \{0\}, D)|$ $|\mathrm{Map}(U, A)| = N^{N-1} - \delta^{\delta-1} N^u$. Consider now the subset $F(1)$ of $\mathrm{Map}(A, A)$ defined by

$$F(1) = \{f + c\}_{f \in F(0),\, c \in A - \{0\}}.$$

First of all we have $F(1) \subseteq \mathrm{Trs}(A, A)$, because if $f + c \in \mathrm{Pol}(A, A)$ for some $f \in F(0)$ and $c \in A - \{0\}$, then $f \in \mathrm{Pol}(A, A)$ as $c \in \mathrm{Pol}(A, A)$, which contradicts $f \in F(0) \subseteq \mathrm{Trs}(A, A)$. Further $F(0) \cap F(1) = \varnothing$, because each $f + c \in F(1)$ is different from each $g \in F(0)$ at least in their action on zero. Finally, it is easy to check that $|F(1)| = |F(0) \times (A - \{0\})| = |F(0)| \cdot$ $\cdot |A - \{0\}| = |F(0)|(N - 1)$, i.e. that if $(f, c), (f', c') \in F(0) \times (A - \{0\})$, then $(f, c) \neq (f', c')$ implies $f + c \neq f' + c'$. In conclusion we have $F(0) \cup F(1) \subseteq \mathrm{Trs}(A, A)$ and $|F(0) \cup F(1)| = |F(0)| + |F(1)| =$ $= |F(0)| + |F(0)|(N - 1) = |F(0)| N = N^N - \delta^{\delta-1} N^{u+1} = \lambda^{(1)}$, so that $\tau \geq \lambda^{(1)}$.

For the second part, put $P(0) = \{f \in \mathrm{Per}(A) \mid f(0) = 0 \text{ and } f(D - \{0\} \nsubseteq D\}$, $P(1) = \{f + c\}_{f \in P(0),\, c \in A\{0\}}$. Then $P(0) \subseteq \mathrm{TPer}(A)$ (cf. proof of 4.5), $P(1) \subseteq \mathrm{TPer}(A)$, $P(0) \cap P(1) = \varnothing$, and $|P(1)| = |P(0)|(N - 1)$ as above. Moreover $|P(0)| = |\mathrm{Per}(A - \{0\})| - |\mathrm{Per}(D - \{0\})| \cdot |\mathrm{Per}(U)| =$ $= (N - 1)! - (\delta - 1)!\, u!$, so that $|P(0) \cup P(1)| = |P(0)| N =$ $= N! - (\delta - 1)!\, u!\, N = \sigma^{(1)}$, and $\rho_T \geq \sigma^{(1)}$.

Remark. Equality may occur in 4.7, because, for example, if A is a field, then $\delta = 1$, $u = N - 1$, $\lambda^{(1)} = 0$, and $\sigma^{(1)} = 0$; moreover $\tau = 0$ and $\rho_T = 0$, according to 4.4.

Let h denote a positive integer, and consider the following

CONDITION (C_h). There exist elements $d \in D$, $u_1, u_2, \cdots, u_h \in U$ such that $d + u_1, d + u_2, \cdots, d + u_h \in D$.

From (C_h) it follows that $d \neq 0$ and $d + u_i \neq d + u_j$ for $i \neq j$. We wish to find the maximum $h \geq 1$ for which (C_h) holds.

Remark. (C_h) does not hold for any field A, nor, for example for $A = Z_4$ or $A = Z_8$; however Z_6 satisfies (C_2) (with $d = \bar{3}$, $u_1 = \bar{1}$, $u_2 = \bar{5}$); Z_{10} satisfies (C_4) (with $d = \bar{5}$, $u_1 = \bar{1}$, $u_2 = \bar{3}$, $u_3 = \bar{7}$, $u_4 = \bar{9}$). More generally:

4.8. If $n = p^t$ (p prime), $\mathbf{Z}_n$ does not satisfy (C_h). If $n = 2^t(2k + 1)$ $(t \geq 1)$, $\mathbf{Z}_n$ satisfies (C_h) with $h = \varphi(n)$ (φ Euler function) and d any fixed divisor $(\neq \pm 1)$ of $2k + 1$.

Proof. In $\mathbf{Z}_n$, with $n = p^t$ (p prime), we have that $\bar{d} \in D$ iff $d \equiv 0 \bmod p$, and that $\bar{u} \in U$ iff $u \not\equiv 0 \bmod p$, so that $\bar{d} \in D$, $\bar{u} \in U$ implies $\bar{d} + \bar{u} \in U$. In $\mathbf{Z}_n$, with $n = 2^t (2k+1)$ $(t \geq 1)$, we have that $\bar{u} \in U$ implies $u \not\equiv 0 \bmod 2$, so that for each fixed $\bar{d} \in D$ such that $d \mid (2k+1)$ and for each of the $\varphi(n)$ elements $\bar{u} \in U$, we have that $\bar{d} + \bar{u} \in D$.

4.9. $|U| < |D|$, then A satisfies (C_1).

Proof. For each $u \in U$, the map $\sigma_u : D \to A$ defined by $\sigma_u : d \to u + d$ is injective; therefore $|U| < |D|$ implies $\sigma_u(D) \nsubseteq U$, i.e. there exists $d \in D$ such that $u + d \in D$.

4.10. If A satisfies (C_h), then $\tau \geq \lambda^{(2)} = \lambda^{(1)} + h N^u \delta^{\delta-2} = N^N - \delta^{\delta-2} N(\delta N - h)$, i.e. $\pi \leq \delta^{\delta-2} N^u(\delta N - h)$.

Proof. Let F (0) and F (1) be the subsets of Trs (A , A) as in 4.7, and let $d \in D$, $u_1, u_2, \cdots, u_h \in U$ satisfy (C_h). For each u_j put

$$F^0(d, u_j) = \{f \in F(0) \mid f(d) = u_j ;\ d' \in D - \{0, d\} \Rightarrow f(d') \in D - d'\}$$

and define

$$F(d, u_j) = \{f + x \mid f \in F^0(d, u_j)\} \quad \text{where} \quad x = \mathrm{Id}_A .$$

Because $F(0) \subseteq \mathrm{Trs}(A, A)$ we have $f + x \in \mathrm{Trs}(A, A)$ for all $f \in F(0)$, so that $F(d, u_j) \subseteq \mathrm{Trs}(A, A)$. Clearly

$$F(d, u_j) = \{f \in \mathrm{Map}(A, A) \mid f(0) = 0,\ f(d) = d + u_j ;$$
$$d' \in D - \{0, d\} \Rightarrow f(d') \in D\} .$$

Therefore $|F(d, u_j)| = |D^{D-\{0,d\}}|\ |A^U| = \delta^{\delta-2} N^u$. Now

$$F(d, u_j) \cap F(0) = \varnothing \quad \text{and} \quad F(d, u_j) \cap F(1) = \varnothing$$

because

$$f \in F(d, u_j) \Rightarrow f(D) \subseteq D \quad , \quad f \in F(0) \Rightarrow f(D) \nsubseteq D$$

and

$$f \in F(d, u_j) \Rightarrow f(0) = 0 \quad , \quad f \in F(1) \Rightarrow f(0) \neq 0 .$$

Finally

$$i \neq j \Rightarrow F(d, u_i) \cap F(d, u_j) = \varnothing, \quad \text{because} \quad i \neq j \Rightarrow u_i \neq u_j$$

and $\quad f \in F(d, u_i) \Rightarrow f(d) = u_i + d \quad , \quad f \in F(d, u_j) \Rightarrow f(d) = u_j + d .$

Therefore, for the set $F(d) = \bigcup_{j=1}^{h} F(d, u_j)$, we obtain $|F(d)| = h\,|F(d, u_j)| = h\delta^{\delta-2} N^u$, $F(d) \subseteq \mathrm{Trs}(A, A)$, $F(d) \cap (F(0) \cup F(1)) = \varnothing$, so that $\tau \geq |F(0) \cup F(1)| + |F(d)| = \lambda^{(1)} + h\delta^{\delta-2} N^u$, as required.

4.11. Suppose that $D \neq \{0\}$ and that there exist $h \geq 1$ elements of U pairwise incongruent mod D. Then

$$\tau \geq \lambda^{(3)} = [h/(h+1)]\, N^N, \qquad \text{i.e.} \quad \pi \leq (h+1)^{-1}\, N^N.$$

Proof. Let $u_1, u_2, \cdots, u_h \in U$ be elements such that $u_i \not\equiv u_j \bmod D$ (i.e. $u_i - u_j \in U$) for $i \neq j$. Since $D \neq \{0\}$, we can fix an element $d \in D$, $d \neq 0$. If F(0) is the set introduced in the proof of 4.7, pick an element

$$f^d_{u_i} \in F(0) \qquad \text{such that} \quad f^d_{u_i}(0) = 0, \; f^d_{u_i}(d) = u_i \qquad (1 \leq i \leq h).$$

If $i \neq j$, then $u_i - u_j \in U$, so that

$$f^d_{u_i} - f^d_{u_j} \in F(0) \qquad \text{which implies} \quad f^d_{u_i} \not\equiv f^d_{u_j} \bmod \mathrm{Pol}(A, A).$$

Thus there are at least $h+1$ classes in the factorial additive group Map (A, A)/Pol (A, A).

Let us now discuss the case $n \geq 1$.

4.12. $\tau_{(n)} \geq (N^{nN} - \delta^{(\delta-1)n}\, N^{n(u+1)})/N^{n-1}$. Further if (C_h) holds for A, then

$$\tau_{(n)} \geq (N^{nN} - \delta^{n(\delta-2)}\,(\delta N - h)^n)/N^{n-1},$$

and, if A satisfies the condition mentioned in 4.11, then

$$\tau_{(n)} \geq N^{nN}\,(1 - 1/(h+1)^n)/N^{n-1}.$$

(Note that, for $n = 1$, 4.12 yields 4.7, 4.10 and 4.11).

Proof. Let $\{f_1, f_2, \cdots, f_n\} \subseteq \mathrm{Map}(A, A)$ be such that (i) $f_j(0) = 0$ for $1 \leq j \leq n$, (ii) $f_j \in \mathrm{Trs}(A, A)$ for at least one j. Define the subset M of $\mathrm{Map}(A,A) \times \cdots \times \mathrm{Map}(A,A)$ (n times) by $M = \{(f_1, f_2, \cdots, f_n) \mid \{f_1, f_2, \cdots, f_n\}$ satisfies (i), (ii)$\}$ and consider the map $\varphi : M \to \mathrm{Map}(A^n, A)$ defined by $\varphi : (f_1, f_2, \cdots, f_n) \to f = \sum_{i=1}^{n} f_i\, pr_i$. It is easy to check that φ acts as an injection from M to $\mathrm{Trs}(A^n, A)$. For the set $M' = \varphi(M) + (A - \{0\})$ we have that $M' \subseteq \mathrm{Trs}(A^n, A)$, $|M'| = |M|\,(N-1)$, and $M' \cap \varphi(M) = \varnothing$, so that $\varphi(M) \cup M' \subseteq \mathrm{Trs}(A^n, A)$ and

$$\tau_{(n)} \geq |\varphi(M) \cup M'| = |M| + |M'| = |M| \cdot N.$$

For computing $|M|$ consider the negation of (ii), i.e. the following condition (iii) f_j Pol (A, A) for all j. Clearly $M = \{(f_1, f_2, \cdots, f_n) \mid \{f_1, f_2, \cdots, f_n\}$ satisfies (i)$\} - \{(f_1, f_2, \cdots, f_n) \mid \{f_1, f_1, \cdots, f_n\}$ satisfies (i), (iii)$\} = M_1 - M_2$, say, so that $|M| = |M_1| - |M_2|$, and using (*a*) of 3.1 for calculating $|M_2|$, we obtain

$$|M| = N^{(N-1)n} - (\pi/N)^n = N^{n(N-1)} - ((N^N - \tau)/N)^n$$

so that

$$\tau_{(n)} \geq |M|\, N = [N^{nN} - (N^N - \tau)^n]/N^{n-1};$$

replacing τ by the expression occurring in either 4.7, or 4.10, or 4.12 (according to the hypothesis of the theorem) leads to the required formulae.

4.13. $\pi_{(n)} \geq \pi^n/N^{n-1}$.

Proof. Let P be the set defined as M_2 in 4.12. The map $\psi : P \rightarrow \text{Map}(A^n, A)$ defined by $\psi : (f_1, f_2, \cdots, f_n) \rightarrow f = \Sigma f_i \, pr_i$ acts as an injection from P to $\text{Pol}(A^n, A)$. Further the set $P' = \psi(P) + (A - \{0\})$ satisfies the following conditions

$$\psi(P) \cup P' \subseteq \text{Pol}(A^n, A) \quad , \quad P' \cap \psi(P) = \varnothing \, , \qquad |P'| = |P|(N - 1)$$

so that $\pi_{(n)} \geq |\psi(P)| + |P'| = |P| \cdot N = (\pi/N)^n N$, where we have used (*a*) of 3.1 for calculating $|P|$.

5. Minimal binomials in I (A)

5.1. In the ideal I(A) of A[X] there exist binomials of the type $X^E - X^e$. Each such pair (E, e) will be called a "couple of exponents for A".

Proof. Let $\boldsymbol{a} = (a_i) = (a_1, a_2, \cdots, a_N)$ be any fixed ordered N-tuple containing all the N elements of A. Put $\boldsymbol{a}^k = (a_i^k)$; the set $\{\boldsymbol{a}^k\}_{k=1,2,\cdots}$ contains at most N^N elements, so that there are integers, E and e, with $1 \leq e < E \leq N^N$, such that $\boldsymbol{a}^E = \boldsymbol{a}^e$, i.e. such that $X^E - X^e \sim 0$.

Consider the set $C(A) = \{(E, e) \in \mathbf{N} \times \mathbf{N} \mid (E, e)$ is a couple of exponents for $A\}$ with the partial ordering

$$(E, e) < (E', e') \qquad \text{iff either} \quad E < E' \qquad \text{or} \quad E = E' \ \& \ e < e'.$$

We shall denote the *minimal couple of exponents for* A by $(E^*, e^*) = \min C(A)$.

5.2. Let $A = \bigoplus_{1=0}^{s} A_i$ the standard decomposition of A as in 2.1, (*j*), and let us denote: D_i the maximal ideal of the local ring A_i, $U_i = A_i - D_i$, 1_i the unit of U_i and 0_i the zero of A_i. Let

$$\lambda_i = \min\{t \in \mathbf{N} \mid a \in U_i \mapsto a^t = 1_i\} \qquad (\text{note that } \lambda_i \leq |U_i|)$$
$$\rho_i = \min\{r \in \mathbf{N} \mid d \in D_i \mapsto d^r = 0_i\} \qquad (\text{note that } \rho_i \leq |D_i|)$$
$$\rho = \max\{\rho_0, \rho_1, \cdots, \rho_s\} \quad , \quad \lambda = [\lambda_0, \lambda_1, \cdots, \lambda_s] .$$

Then $\lambda = \min\{t \in \mathbf{N} \mid a \in U \mapsto a^t = 1\}$, and $E^* = \lambda + \rho$, $e^* = \rho$.

Proof. There exists an element $d \in D$ such that $d, d^2, \cdots, d^{\rho-1}$ are non-zero (and distinct) elements, and $d^\rho = d^{\rho+1} = \cdots = 0$. It follows that $e^* \geq \rho$. For each $a \in U$, we have $a^\lambda = 1$, so that $a^{\lambda+k} = a^k$ for each $a \in U$. It follows that $e^* = \rho$ and $E^* = \lambda + \rho$.

Corollary 5.3. *Let* $A = \mathbf{Z}_m$, *with* $m = 2^{r_0} p_1^{r_1} \cdots p_s^{r_s} \in \mathbf{Z}$ and $2, p_1, p_2, \cdots, p_s$ *distinct primes (so that* $\mathbf{Z}_m = \mathbf{Z}_{2^{r_0}} \oplus \mathbf{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbf{Z}_{p_s^{r_s}}$*). Then, using the notation of* 5.2, *we have*

$\lambda_0 = \lambda_0(2^{r_0}) = 1$ if $r_0 = 0, 1$; $\lambda_0(2^{r_0}) = 2$ if $r_0 = 2$; $\lambda_0(2^{r_0}) = 2^{r_0-2}$ *if* $r_0 \geq 3$;
$\lambda_i = \varphi(p_i^{r_i}) = (p_i - 1) p_i^{r_i-1}$ *for* $1 \leq i \leq s$; $\rho_i = r_i$ *for* $0 \leq i \leq s$;
$\lambda = \lambda(m) = [\lambda_0(2^{r_0}), \varphi(p_1^{r_1}), \cdots, \varphi(p_s^{r_s})]$ *and* $\rho = \rho(m) = \max\{r_0, \cdots, r_s\}$.
In conclusion $E^* = \lambda(m) + \rho(m)$, $e^* = \rho(m)$.

Proof. Define $\lambda_0(1) = 1$; $\lambda_0(2) = 1$ because $U(\mathbf{Z}_2) = \{1\}$; $\lambda_0(4) = 2$ because $U(\mathbf{Z}_4) = \{1, 3\}$. If $r_0 \geq 3$ we have the well-known isomorphism $U(\mathbf{Z}_{2^{r_0}}) \simeq \mathbf{Z}_2^{(+)} \oplus \mathbf{Z}_{2^{r_0-2}}^{(+)}$, so that each element of $U(\mathbf{Z}_{2^{r_0}})$ has a period which is a divisor of 2^{r_0-2} and the element $(1, 1) \in U(\mathbf{Z}_{2^{r_0}})$ has precisely period 2^{r_0-2}. $\lambda_i = \varphi(p_i^{r_i})$ $(1 \leq i \leq s)$ because the groups $U(\mathbf{Z}_{p_i^{r_i}})$ are cyclic with $\varphi(p_i^{r_i})$ elements. $\rho_i = r_i$ $(0 \leq i \leq s)$ because $D(\mathbf{Z}_{p_i^{r_i}}) = (\bar{p}_i)$ and $\bar{p}_i^h = \bar{0}$ in $\mathbf{Z}_{p_i^{r_i}}$ iff $h \geq r_i$. By 5.2, the corollary now follows immediately.

It is easy to prove that

5.4. If $(E, e) \in C(A)$ and $E < N$, then $\pi \leq N^E$, i.e. $\tau \geq N^N - N^E$. More generally, $\pi_{(n)} \leq N^{E^n}$, i.e. $\tau_{(n)} \geq N^{N^n} - N^{E^n}$.

Applying 5.2 and 5.4 leads to other bounds for $\pi_{(n)}$ and for $\tau_{(n)}$, which can be compared with those obtained in 4.7–4.13.

Note that if A is a field, then $I(A) = (X^N - X)$. In [6], $I(Z_m)$ was determined. The problem of determining $I(A^n)$ in the general case will be studied in a future paper by the author.

Acknowledgments. I wish to thank very much C. Walter (research student of the University of Cambridge), who kindly helped me with my English.

BIBLIOGRAPHY

[1] R. D. CARMICHAEL (1956) – *Introduction to the theory of groups of finite order.* (Reprint of the 1st ed., 1937). New York, Dover.

[2] BROTHER J. HEISLER (1967) – *A characterization of finite fields,* « Amer. Math. Monthly », *74,* 537–538 and 1211.

[3] G. KELLER and F. R. OLSON (1968) – *Counting polynomial functions (mod p^n),* « Duke Math. J. », *35,* 835–838.

[4] A. J. KEMPNER (1921) – *Polynomials and their residue system,* « Amer. Math. Soc. Trans. », *22,* 240–288.

[5] R. LEHTI (1959) – *Evaluation matrices for polynomials in Galois fields,* « Soc. Sci. Fenn. Comment. Phys., Math. », *22* (3), 18 pp.

[6] I. NIVEN and L. J. WARREN (1957) – *A generalization of Fermat's theorem* « Proc. Amer. Math. Soc. », *8,* 306–313.

[7] W. NOBAUR (1962) – *Funktionen auf kommutative Ringen,* «Math. Ann. », *147,* 166–175.

[8] L. REDEI and T. SZELE (1947) – *Algebraisch-zahlentheoretische Betrachtungen über Ring,* I, « Acta Math. », *79,* 291–320; II, « Acta Math. », *82* (1950), 209–241.

[9] B. SEGRE (1965) – *Istituzioni di geometria superiore.* I: *Strutture algebriche.* Lezioni raccolte da P. V. Ceccherini. Roma, Ist. Mat. « G. Castelnuovo ».

[10] B. SEGRE (1965) – *Istituzioni di geometria superiore.* III: *Complessi, reti, disegni.* Lezioni raccolte da P. V. Ceccherini. Roma, Ist. Mat. « G. Castelnuovo ».

[11] O. ZARISKI and P. SAMUEL (1958) – *Commutative algebra,* I. New York etc., Van Nostrand Reinhold.