Lecture Notes in Mathematics 1600

Władysław Narkiewicz

Polynomial Mappings

Springer

Władysław Narkiewicz

Polynomial Mappings

Springer

Author

Władysław Narkiewicz
Institute of Mathematics
Wrocław University
Plac Grunwaldzki 2/4
PL-50-384-Wroclaw, Poland
E-mail: narkiew@math.uni.wroc.pl

Mathematics Subject Classification (1991): 11C08, 11R09, 11T06, 12E05, 13B25, 13F20, 14E05

ISBN 3-540-59435-3 Springer-Verlag Berlin Heidelberg New York

CIP-Data applied for

Typesetting: Camera-ready output by the author
SPIN: 10130271 46/3142-543210 - Printed on acid-free paper

Preface

1. Our aim is to give a survey of results dealing with certain algebraic and arithmetic questions concerning polynomial mappings in one or several variables. The first part will be devoted to algebraic properties of the ring $Int(R)$ of polynomials which map a given ring R into itself. In the case $R = \mathbf{Z}$ the first result goes back to G.Pólya who in 1915 determined the structure of $Int(\mathbf{Z})$ and later considered the case when R is the ring of integers in an algebraic number field. The rings $Int(R)$ have many remarkable algebraic properties and are a source of examples and counter-examples in commutative algebra. E.g. the ring $Int(\mathbf{Z})$ is not Noetherian and not a Bezout ring but it is a Prüfer domain and a Skolem ring. We shall present classical results in this topic due to G.Pólya, A.Ostrowski and T.Skolem as well as modern development.

2. In the second part we shall deal with *fully invariant sets* for polynomial mappings Φ in one or several variables, i.e. sets X satisfying $\Phi(X) = X$. In the case of complex polynomials this notion is closely related to Julia sets and the modern theory of fractals, however we shall concentrate on much more modest questions and consider polynomial maps in fields which are rather far from being algebraically closed. Our starting point will be the observation that if f is a polynomial with rational coefficients and X is a subset of the rationals satisfying $f(X) = X$, then either X is finite or f is linear. It turns out that the same assertion holds for certain other fields in place of the rationals and also for a certain class of polynomial mappings in several variables. We shall survey the development of these question and finally we shall deal with cyclic points of a polynomial mapping, i.e. with fixpoints of its iterates. Here we shall give the classical result of I.N.Baker concerning cyclic points of complex polynomials and then consider that question in rings of integers in an algebraic number field.

There are several open problems concerning questions touched upon in these lectures and we present twenty one of them.

3. This text is based on a course given by the author at the Karl-Franzens University in Graz in 1991. I am very grateful to professor Franz Halter-Koch for organizing my stay in Graz as well for several very fruitful discussions. My thanks go also to colleagues and friends who had a look at the manuscript and in particular to the anonymous referee who pointed out some inaccuracies.

The work on these lecture notes has been supported by the KBN grant 2 1037 91 01. The typesetting has been done by the author using $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX.

Notations

We shall denote the rational number field by $\mathbf{Q}$, the field of reals by $\mathbf{R}$, the complex number field by $\mathbf{C}$ and the field of p-adic numbers by $\mathbf{Q}_p$. The ring of rational integers will be denoted by $\mathbf{Z}$, the set of nonnegative rational integers by $\mathbf{N}$, the ring of integers of $\mathbf{Q}_p$ by $\mathbf{Z}_p$, the finite field of q elements by $\mathbf{F}_q$ and the ring of integers in an algebraic number field K by $\mathbf{Z}_K$.

By $a \mid b$ we shall denote the divisibility in various rings and in case of the ring of rational integers we shall write $q \parallel a$ in the case when q is the maximal power of a prime which divides a. The same notation will be used for divisibility of ideals in Dedekind domains. The symbol $\square$ will mark the end of a proof.

CONTENTS

PART A

Rings of integral-valued polynomials

I. Polynomial functions

1. Let R be an arbitrary commutative ring with unit. Every element f of $R[X]$, the ring of all polynomials in one variable with coefficients in R, defines a map $T_f : R \longrightarrow R$. The set of all maps T_f obtained in this way forms a ring, the *ring of polynomial functions on* R, which we shall denote by $P(R)$. Let I_R denote the set of all polynomials $f \in R[X]$ satisfying $f(r) = 0$ for all $r \in R$, and let $F(R)$ denote the set of all maps $R \longrightarrow R$. The following lemma collects a few easy facts concerning $P(R)$ and I_R:

LEMMA 1.1. (i) *The set I_R is an ideal in $R[X]$ and we have*

$$P(R) \simeq R[X]/I_R,$$

(ii) *If R is a domain then the equality $I_R = \{0\}$ holds if and only if R is infinite,*

(iii) *If $R = \mathbf{F}_q$ then I_R is generated by the polynomial $X^q - X$ and*

$$P(R) \simeq R[X]/(X^q - X)R[X].$$

PROOF: The assertion (i) is evident. If R is infinite then clearly only the zero polynomial vanishes identically on R. If R is a finite domain then it is a field, say $R = \mathbf{F}_q$, and the polynomial $X^q - X$ vanishes identically. This proves (ii).

The last assertion follows from the remark that if a polynomial vanishes at all elements of the field $\mathbf{F}_q$ then it must be divisible by

$$\prod_{a \in \mathbf{F}_q} (X - a) = X^q - X. \ \square$$

2. The ring $P(R)$ can be described in terms of certain ideals of R:

THEOREM 1.2. (J.WIESENBAUER [82]) *If R is a commutative ring with unit element and for $j = 0, 1, \ldots$ we define I_j to be the set of all $a \in R$ such that there exist $c_0, c_1, \ldots, c_{j-1}$ in R with*

$$ax^j + \sum_{i=0}^{j-1} c_i x^i = 0 \quad \text{for all } x \in R$$

then the I_j's form an ascending chain of ideals in R and if for $j = 0, 1, \ldots$ we fix a set A_j of representatives of R/I_j containing 0, then every $f \in P(R)$ can be uniquely written in the form

$$f(x) = \sum_{j=0}^{N} a_j x^j$$

with a suitable N, $a_j \in A_j$ and $a_N \neq 0$ in case $f \neq 0$.

PROOF: Clearly the I_j's form an ascending chain of ideals. Assume that our assertion fails for some non-zero $f \in P(R)$. Consider all possible polynomial representations:

$$\mathcal{R}: \qquad f(x) = \sum_{j=0}^{m} d_j x^j \quad (x \in R,\ d_j \in R,\ d_m \neq 0)$$

and denote by $i(\mathcal{R})$ the maximal index j with $d_j \notin A_j$. Choose now a representation $\mathcal{R}_0$ with $i = i(\mathcal{R}_0)$ minimal and write

$$f(x) = \sum_{j=0}^{i} d_j x^j + \sum_{j=1+i}^{m} a_j x^j, \tag{1.1}$$

with $d_i \notin A_i$ and $a_j \in A_j$ for $j = 1+i, 2+i, \ldots, m$. If $a_i \in A_i$ satisfies $a_i - d_i \in I_i$ then with suitable $b_0, b_1, \ldots, b_{i-1} \in R$ we have

$$(a_i - d_i)x^i + \sum_{j=0}^{i-1} b_j x^j = 0 \qquad \text{for all } x \in R,$$

hence in (1.1) we may replace the term $d_i x^i$ by

$$a_i x^i + \sum_{j=0}^{i-1} b_j x^j,$$

contradicting the choice of $\mathcal{R}_0$. □

3. If p is a rational prime then every function $\mathbf{Z}/p\mathbf{Z} \longrightarrow \mathbf{Z}/p\mathbf{Z}$ can be represented by a polynomial. The next theorem describes commutative rings with unit having this property.

THEOREM 1.3. (L.RÉDEI, T.SZELE [47], part I) *Let R be a commutative ring with a unit element. Every function $f : R \longrightarrow R$ can be represented by a* *polynomial from $R[X]$, i.e. $F(R) = P(R)$ holds if and only if R is a finite field.*

PROOF: The sufficiency of the stated condition follows immediately from the interpolation formula of Lagrange, so we concentrate on its necessity.

If R is infinite and its cardinality equals α, then the cardinality of $R[X]$ also equals α but the cardinality of all maps $R \longrightarrow R$ equals $\alpha^\alpha > \alpha$, hence not every such map can be represented by a polynomial.

Let thus $R = \{a_1 = 0, a_2, \ldots, a_n\}$ be a finite unitary commutative ring of n elements. If it is not a field, then it has a zero-divisor c, since every finite domain is necessarily a field. Put

$$g(X) = \prod_{i=1}^{n}(X - a_i),$$

and observe that for all $a \in R$ one has $g(a) = 0$. This shows that if a map $R \longrightarrow R$ can be represented by a polynomial F, then F can be chosen to have its degree $\leq n - 1$, since F and F mod g represent the same function on R. The number of all maps $R \longrightarrow R$ and the number of all polynomials of degree $\leq n - 1$ both equal n^n and hence it is sufficient to find a non-zero polynomial of degree $\leq n - 1$ vanishing on R. The polynomial

$$f(X) = c\prod_{i=2}^{n}(X - a_i)$$

can serve as an example since it evidently vanishes at non-zero arguments and moreover we have $f(0) = (-1)^{n-1}ca_2a_3 \cdots a_n$, but as c is a zero-divisor there is an element $a_i \neq 0$ with $ca_i = 0$ and thus $f(0) = 0$. □

(This argument can be modified to cover also rings which do not have a unit element. Cf. L.RÉDEI, T.SZELE [47], part I, p.301).

4. Consider the following example:

Let $R = \mathbf{Z}/4\mathbf{Z}$ be the ring of residue classes mod 4 and put

$$f(x) = \begin{cases} 0 & \text{if } x = 0, 1 \\ 1 & \text{if } x = 2, 3. \end{cases}$$

The function f cannot be represented by a polynomial over R, since otherwise we would have

$$1 \equiv f(3) \equiv f(1) \equiv 0 \pmod 2.$$

However the polynomial

$$g(X) = \left(\frac{X(X-1)}{2}\right)^2$$

attains integral values at integers and it induces on R the function f.

This situation is a special case of the following construction:

Let R and $S_1 \subset S_2$ be commutative rings and let $F : S_1 \longrightarrow R$ be a surjective homomorphism. If a polynomial $f \in S_2[X]$ satisfies

(i) $f(S_1) \subset S_1$,

and

(ii) *If* $s, t \in S_1$ *and* $F(s) = F(t)$ *then* $F(f(s)) = F(f(t))$,

then f *induces a map* $\hat{f} : R \longrightarrow R$ *defined by*

$$\hat{f}(r) = F(f(s)),$$

where s *is any element of* S_1 *with* $F(s) = r$.

Following L.RÉDEI, T.SZELE [47] we shall say that S_2 is a *representation ring* for R, provided there exists $S_1 \subset S_2$ such that every map $g : R \longrightarrow R$ equals $\hat{f}$ for a suitable $f \in S_2[X]$ satisfying (i) and (ii). We shall also say that the pair $< S_1, S_2 >$ is a *representation pair* for R.

THEOREM 1.4. (T.SKOLEM [40]) *If* $q = p^k$ *is a prime power then* $< \mathbf{Z}, \mathbf{Q} >$ *is a representation pair for* $\mathbf{Z}/q\mathbf{Z}$.

PROOF: In case $k = 1$ the assertion follows from Theorem 1.3. Assume thus $k \geq 2$. The main step of the proof is embodied in the following lemma:

LEMMA 1.5. *If* $q = p^k$ *with prime* p *then there exists a polynomial* $\Phi(X) \in \mathbf{Q}[X]$ *which is integral-valued at the integers and satisfies*

$$\Phi(x) \equiv \begin{cases} 1 \pmod{q} & \text{if } q \text{ divides } x, \\ 0 \pmod{q} & \text{otherwise.} \end{cases}$$

PROOF: Let $r_1, r_2, \ldots, r_t$ be a complete reduced system of residues mod q and put

$$\Psi(X) = \prod_{i=1}^{t}(X - r_i)\left(\binom{X}{p} - r_i\right)\left(\binom{X}{p^2} - r_i\right)\cdots\left(\binom{X}{p^{k-1}} - r_i\right),$$

$$\Phi(X) = \Psi(X)^2.$$

If $x \in \mathbf{Z}$ is divisible by q, then all numbers

$$\binom{x}{p}, \ldots, \binom{x}{p^{k-1}}$$

are divisible by p. Now observe that if r runs over all residues mod q not divisible by p and a is divisible by p, then $a - r$ runs over all residues mod q not divisible by p and this gives

$$\Psi(x) \equiv (r_1 \cdots r_t)^k \equiv \pm 1 \pmod{q},$$

and

$$\Phi(x) \equiv 1 \pmod{q}.$$

If however q does not divide $x \in \mathbf{Z}$, then we may write $x = p^m y$ with $0 \leq m < k$ and y not divisible by p. Since, as is easily checked, $\binom{x}{p^m}$ is not divisible by p, we have with a suitable i

$$\binom{x}{p^m} \equiv r_i \pmod{q},$$

hence $\Phi(x) \equiv \Psi^2(x) \equiv 0 \pmod{q}$. □

To conclude the proof of the theorem observe that if the map $f : \mathbf{Z}/q\mathbf{Z} \longrightarrow \mathbf{Z}/q\mathbf{Z}$ is arbitrary and a_i is a representative of the residue class $f(i)$ mod q, then the polynomial

$$F(X) = \sum_{i=0}^{q-1} a_i \Phi(X - i)$$

represents f. □

(L.RÉDEI,T.SZELE [47] showed also that the ring of all rational numbers whose denominators are powers of a prime p can serve as a representation ring for $\mathbf{Z}/q\mathbf{Z}$ where q is a power of p. They proved moreover that every ring whose additive group is a cyclic p-group has $\mathbf{Q}$ for its representation ring).

It should be noted that the analogue of Theorem 1.4 fails for composite integers which are not prime-powers. Indeed, assume that one can find a polynomial $f \in S(\mathbf{Z})$ such that

$$f(x) \equiv \begin{cases} 1 \pmod{6} & \text{if 6 divides } x, \\ 0 \pmod{6} & \text{otherwise.} \end{cases}$$

If we write

$$f(X) = \frac{g(X)}{q}$$

with $g \in \mathbf{Z}[X]$ and $q \in \mathbf{Z}$ then

$$g(x) \equiv \begin{cases} q \pmod{6q} & \text{if 6 divides } x, \\ 0 \pmod{6q} & \text{otherwise.} \end{cases}$$

Observe that $6 \mid q$ because if $p = 2$ or $p = 3$ then

$$0 \equiv g(p) \equiv g(6) \equiv q \pmod{p}$$

and $p \mid q$ follows. Write now $q = 2^\alpha M$ with $\alpha \geq 1$ and odd $M \in \mathbf{Z}$ divisible by 3 and choose $x \in \mathbf{Z}$ satisfying

$$x \equiv 0 \pmod{2^{1+\alpha}}, \quad x \equiv 1 \pmod{M}.$$

Then $f(x) \equiv 0 \pmod{6}$ and $f(0) \equiv 1 \pmod{6}$, however $x \equiv 0 \pmod{2^{1+\alpha}}$ implies $g(x) \equiv g(0) \pmod{2^{1+\alpha}}$, hence with a suitable $A \in \mathbf{Z}$ we may write $g(x) - g(0) = A2^{1+\alpha}$ and finally the number

$$f(x) - f(0) = \frac{2A}{M}$$

turns out to be even, contradicting $f(x) - f(0) \equiv 5 \pmod{6}$.

5. We shall see later (see the Corollary to Theorem 1.7) that for composite m, which are not prime powers, the ring $\mathbf{Z}/m\mathbf{Z}$ does not have any representation pair. The problem of determination of all commutative rings which have a representation ring seems to be open (**PROBLEM I**). We shall present now a necessary condition given by L.RÉDEI, T.SZELE [47], but first we have to recall certain elementary properties of difference operators:

If R is an arbitrary commutative ring and $f : \mathbf{Z} \longrightarrow R$ an arbitrary map, then we put

$$\Delta^1 f(x) = f(x+1) - f(x),$$

and

$$\Delta^{n+1} f(x) = \Delta^n f(x+1) - \Delta^n f(x) \quad \text{for } n = 0, 1, \ldots .$$

LEMMA 1.6. (i) *For any $f : \mathbf{Z} \longrightarrow R$, for $n = 1, 2, \ldots$ and for all $x \in \mathbf{Z}$ one has*

$$\Delta^n f(x) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(x+i),$$

(ii) *If $f \in R[X]$, $r \in R$ and we put for $x \in \mathbf{Z}$*

$$g_r(x) = f(xr),$$

then for a suitable positive integer N we have

$$\Delta^N g_r(x) = 0$$

for all $x \in \mathbf{Z}$.

PROOF: The assertion (i) is obtained by a simple recurrence argument and to prove (ii) it suffices to observe that $g_r(x)$ is a polynomial in x. □

COROLLARY. *Let R be a ring having a representation ring and let $< S_1, S_2 >$ be a representation pair for R. For every map $F : R \longrightarrow R$ and every non-zero $r \in R$ there exists a positive integer N such that the N-th iterate δ_r^N of the operator δ_r, defined by*

$$\delta_r F(x) = F(x+r) - F(x)$$

vanishes identically.

PROOF: Let $\varphi : S_1 \longrightarrow R$ be a surjective homomorphism, realizing the representation of R by the pair $< S_1, S_2 >$ and let $r = \varphi(s)$ for some $s \in S_1$. It suffices now to apply part (ii) of the lemma to the polynomial inducing F. □

THEOREM 1.7. (L.RÉDEI, T.SZELE [47], part II, Satz 5) *Let R be a commutative ring with unit element e and assume that R has a representation ring. Then there exists a prime power q such that $qe = 0$.*

PROOF: Let $< S_1, S_2 >$ be a representation pair for R.

First assume that R contains an element s of infinite additive order, i.e. all elements $s, 2s, 3s, \ldots$ are distinct and non-zero, and let $f : R \longrightarrow R$ satisfy $f(s) = s$ and $f(ks) = 0$ for $k \in \mathbf{Z}$. It suffices now to apply the Corollary to Lemma 1.6, since it is obvious that none of the iterated differences of the sequence $s, 0, 0, \ldots$. can vanish.

We may thus assume that all elements of R have a finite additive order. Assume also that there is a non-zero element $s \in R$ whose order m is not a prime power. Let p be a prime divisor of m and define k by $q = p^k \parallel m$. Consider any map $f : R \longrightarrow R$ satisfying $f(is) = e$ for $i \equiv p^k \pmod{m}$ and $f(is) = 0$ for all other $i \in \mathbf{Z}$. By the Corollary to Lemma 1.6 the N-th differences $\delta_r^n f$ vanish for all sufficiently large N and hence we may find such an N which is a power of p, say $N = p^u$. We may assume that u exceeds k and moreover the congruence

$$p^{u-k} \equiv 1 \pmod{\frac{m}{p^k}}$$

holds. (Simply choose sufficiently large u satisfying $u \equiv k \pmod{\varphi(m/p^k)}$)). The last congruence implies

$$(1.2) \qquad p^u \equiv p^k \pmod{m}$$

and if we put $\hat{f}(x) = f(rx)$ then with the use of Lemma 1.6 (i) we get

$$\hat{f}(p^u) - \binom{p^k}{1} \hat{f}(p^u - 1) + \cdots + (-1)^{p^k} \hat{f}(0) = 0$$

and the congruence

$$\hat{f}(p^u) \equiv \hat{f}(0) \pmod{pR}$$

follows. (Note that our assumption about m implies that pR is not the zero ideal). Finally note that since the function $\hat{f}$ is periodic of period m, the congruence (1.2) leads to

$$0 = \hat{f}(0) \equiv \hat{f}(p^u) \equiv \hat{f}(p^k) \pmod{pR},$$

a contradiction.

It follows that the additive order of every non-zero element of R must be a prime-power, and this applies in particular to the unit element. □

Corollary. *The ring $\mathbf{Z}/m\mathbf{Z}$ has a representation ring if and only if m is a prime power.*

Proof: The necessity follows from the last theorem and the sufficiency is contained in Theorem 1.4. □

6. We conclude this section with two results dealing with $P(R)$ in the case $R = \mathbf{Z}/q\mathbf{Z}$ and start with a theorem of L. Carlitz [64]:

Theorem 1.8. *Let $q = p^n$ be a prime power, let $f : \mathbf{Z}/q\mathbf{Z} \longrightarrow \mathbf{Z}/q\mathbf{Z}$ be a given map, let $A_q = \{0, 1, 2, \ldots, q-1\}$ and denote by $\hat{f} : A_q \longrightarrow A_q$ the map induced by f. Then $\hat{f}$ is a restriction to A_q of a polynomial $F \in \mathbf{Z}[X]$ if and only if $\Delta^r \hat{f}(0)$ is divisible by $(q, r!)$ for $r = 0, 1, \ldots, q-1$.*

Proof: *Necessity.* In view of Lemma 1.6 (i) it suffices to establish the following lemma:

Lemma 1.9. *If $F \in \mathbf{Z}[X]$ then the numbers*

$$\sum_{i=0}^{r}(-1)^{r-i}\binom{r}{i}F(i)$$

are for all $r \geq 0$ divisible by $r!$.

Proof: Observe first that if we define for $j = 0, 1, \ldots$ the polynomials F_j by

$$F_j(X) = X(X-1)\cdots(X-j+1),$$

then every polynomial of $\mathbf{Z}[X]$ can be uniquely written as a linear combination of the F_j's with rational integral coeffficients. A simple inductive argument shows that for $r = 1, 2, \ldots$ one has

$$\Delta^r F_j(X) = j(j-1)\cdots(j-r+1)F_{j-r}(X),$$

and since the product of r consecutive integers is divisible by $r!$ the assertion follows for the polynomials F_j and by linearity the lemma results. □

Sufficiency. We need a simple lemma:

Lemma 1.10. *If h is any function defined on the set A_q then for for all $a \in A_q$ one has*

$$h(a) = \sum_{j=0}^{q}\Delta^j h(0)\binom{a}{j}.$$

Proof: Using Lemma 1.6 (i) and the equality

$$\binom{a}{j}\binom{j}{i} = \binom{a}{i}\binom{a-i}{j-i}$$

we get

$$\begin{aligned}\sum_{j=0}^{q}\Delta^j h(0)\binom{a}{j} &= \sum_{i=0}^{q}h(i)\sum_{j=i}^{q}(-1)^{j-i}\binom{j}{i}\binom{a}{j}\\ &= \sum_{i=0}^{q}\binom{a}{i}h(i)\sum_{t=0}^{q-i}(-1)^t\binom{a-i}{t}.\end{aligned}$$

Since for $t > a-i$ we have $\binom{a-i}{t} = 0$, the last expression equals

$$\sum_{i=0}^{q}\binom{a}{i}h(i)\sum_{t=0}^{a-i}(-1)^t\binom{a-i}{t} = \sum_{i=0}^{q}\binom{a}{i}h(i)(1-1)^{a-i} = h(a). \quad \square$$

Observe now that the denominator of the fraction $\Delta^j \hat{f}(0)/j!$ in its reduced form is for $j \leq q$ not divisible by p and so we may find $0 \leq \xi_j < q$ satisfying

$$\Delta^j \hat{f}(0) \equiv \xi_j j! \pmod{q}.$$

Applying the last lemma to $h = \hat{f}$ we obtain that the polynomial

$$F(X) = \sum_{j=0}^{q} \xi_j X(X-1)\cdots(X-j+1)$$

realizes $\hat{f}$. □

It has been shown by F.DUEBALL [49] that if p is a prime and $n > 1$ then every polynomial in $\mathbf{Z}/(p^n\mathbf{Z})[X]$ is uniquely determined by its values at $x = 0, 1, \ldots, tp-1$, where t is defined as follows: if $p^{c_j} \parallel p^j j!$ for $j = 0, 1, \ldots,$ then c is the smallest index satisfying $c_t \geq n$. This is closely related to the polynomial interpolation problem. A necessary and sufficient condition for its solvability in an arbitrary commutative ring has been given by R.SPIRA [68].

A characterization of functions $f : (\mathbf{Z}/p^n\mathbf{Z})^k \longrightarrow \mathbf{Z}/p^n\mathbf{Z}$ which can be represented by k-ary polynomials has been given by I.G.ROSENBERG [75].

7. The number of of elements of $P(\mathbf{Z}/q\mathbf{Z})$ for any integer q has been found by A.J.KEMPNER [21]. We give a proof due to J.WIESENBAUER [82]. (Another proofs had been given by G.KELLER, F.R.OLSON [68] and G.MULLEN, H.STEVENS [84]. Cf. also J.V.BRAWLEY, G.L.MULLEN [92], who considered the more general case of polynomial functions in a *Galois ring* $\mathbf{Z}[X]/I$ with $I = p\mathbf{Z}[X] + f\mathbf{Z}[X]$, where p is a prime and $f \in \mathbf{Z}[X]$ is a polynomial irreducible mod p. For the theory of Galois rings see [MD]. The number of elements in $P(R)$ in the case when R is a finite commutative local principal ideal ring has been determined by A.A.NEČAEV [80]).

THEOREM 1.11. *Let $n \geq 1$ be an integer and denote by $M(n)$ the cardinality of $P(\mathbf{Z}/n\mathbf{Z})$. Then*

$$M(n) = \prod_{i=0}^{N} \frac{n}{(n, N!)} \quad ,$$

where $N = N_n$ denotes the largest integer such that n does not divide $N!$. Moreover $M(n)$ is a multiplicative function, i.e. $(n_1, n_2) = 1$ implies $M(n_1 n_2) = M(n_1)M(n_2)$.

In particular, if $n = p^k$ is a prime power, then $M(n) = p^{k(N+1)-s}$ where s is the exponent of the prime p in the canonical factorization of $\prod_{j=2}^{N} j!$.

PROOF: It has been noted in the proof of Lemma 1.9 that every polynomial f of degree not exceeding r over $\mathbf{Z}$ can be written uniquely in the form

$$f(X) = \sum_{j=0}^{r} a_j F_j(X),$$

with $F_j(X) = X(X-1)\cdots(X-j+1)$. Restricting the coefficients by $0 \leq a_j < n$ we get a general form of a polynomial over $\mathbf{Z}/n\mathbf{Z}$. Observe now that f has all its values divisible by n if and only if for $i = 0, 1, \ldots, r$ one has

$$a_i \equiv \frac{n}{(n, i!)} \pmod{n}.$$

In fact, if this condition is satisfied, then we get

$$a_i f(X) = a_i i! \binom{X}{i} \equiv n \frac{i!}{(n, i!)} \binom{X}{i} \equiv 0 \pmod{n},$$

and if f vanishes identically mod n, then evidently $a_0 = f(0)$ is divisible by n and if for $k = 0, 1, \ldots, i-1$ we have $a_k \equiv n/(n, k!) \pmod{n}$, then

$$0 \equiv f(i) = \sum_{j=0}^{r} a_j f_j(i) \equiv a_i j! \pmod{n},$$

implying our assertion. It follows that for every j the ideal I_j occuring in theorem 1.2 is generated by $n/(n, j!)$ and thus the first assertion follows from that theorem. Multiplicativity of $M(n)$ is an immediate consequence of the Chinese Remainder Theorem and the last assertion is just a special case of the first. □

Exercises

1. (I.NIVEN,LEROY J.WARREN [57]) Let m be a positive integer and $R = \mathbf{Z}/m\mathbf{Z}$. Prove that I_R is a finitely generated ideal in $R[X]$ which is principal if and only if m is a prime.

2. Let R be a domain and let A be a finite subset of R. Prove that every map $A \longrightarrow R$ can be realized by a polynomial in $R[X]$ if and only if every non-zero difference of elements of A is invertible.

3. Prove the analogue of Theorem 1.3 for functions of several variables.

4. (G.MULLEN, H.STEVENS [84]) Prove the analogue of Theorem 1.11 for polynomials in several variables.

5. Let $f \in \mathbf{Z}[X]$ and let N be a positive integer. One says that f is a *permutation polynomial* mod N, if it induces a permutation of $\mathbf{Z}/N\mathbf{Z}$.

(i) Show that if p is a prime then $f \in \mathbf{Z}[X]$ is a permutation polynomial mod p^2 if and only if it is a permutation polynomial mod p and for all $x \in \mathbf{Z}$ one has

$$f'(x) \not\equiv 0 \pmod{p}.$$

(ii) Show that if p is a prime and f is a permutation polynomial mod p^2, then it also a permutation polynomial mod p^n for $n = 3, 4, \ldots$.

(iii) Prove that f is a permutation polynomial mod N if and only if it is a permutation polynomial mod q for all prime powers q dividing N.

6. (G.MULLEN, H.STEVENS [84]) Let p be a prime and $n \geq 2$. Prove that the number of polynomial functions which permute the elements of $\mathbf{Z}/p^n\mathbf{Z}$ equals

$$p!(p-1)^p p^D,$$

where

$$D = (N+1)(n - c(N)) + \delta(N) - 2p,$$

(with N being the largest integer with $c(N) < n$, where $c(N)$ is the exponent of p in the factorization of $n!$) and

$$\delta(n) = \frac{1}{2}\sum_{r=1}^{\infty} p^r \left[\frac{n}{p^r}\right]\left(\left[\frac{n}{p^r}\right]+1\right).$$

7. (L. Carlitz [63]) Prove that if a polynomial $f \in \mathbf{F}_p[X]$ induces a permutation in all fields $\mathbf{F}_{p^k}$ $(k = 1, 2, \dots)$ then with suitable $a, b \in \mathbf{F}_p$, $a \neq 0$ and $r \geq 1$ one has

$$f(X) = aX^{p^r} + b.$$