Elem. Math. 57 (2002) 76 – 79
0013-6018/02/020076-4 $ 1.50+0.20/0

Elemente der Mathematik

Zero sets of polynomials: one versus two variables

Mihai Caragiu

Mihai Caragiu was born in Ploiesti, Romania. He got his M.Sc. in 1988 from the University of Bucharest, and his Ph.D. in 1996 from Penn State University. He is interested in finite fields and their applications, linear recurrent sequences and their invariants, model theoretic algebra, and mathematics education. After his Ph.D. he held various positions with Washington State University, Stanford University's Educational Program for Gifted Youth and Ohio Northern University in Ada, Ohio, where he is currently an Assistant Professor of Mathematics.

1 Introduction

It is well-known that if K is any field and $f(X) \in K[X]$ is an irreducible polynomial, then either the degree of f is one, case in which there is precisely one zero of $f(X)$ in K, or the degree of f is greater than one, case in which there is no zero of $f(X)$ in K. Therefore, since K has at least two elements ($0, 1 \in K$), *it is impossible for an irreducible polynomial in one variable to always take the value zero.*

In what follows we will investigate the zero sets for polynomials in two variables, showing that in this case things could be radically different. To this effect, we will construct, over any finite field $\mathbf{F}_q$, an irreducible polynomial $f(X, Y) \in \mathbf{F}_q[X, Y]$ which *is zero at any point*, i.e., the equality $f(x, y) = 0$ holds true *for any* $x, y \in \mathbf{F}_q$. The construction is elementary and can be easily adapted so that we can build irreducible polynomials in two variables over an infinite field K taking the value zero on a given finite subset of $K \times K$.

Ist f ein irreduzibles Polynom in einer Variablen über einem Körper k, so hat f bekanntlich entweder den Grad eins und besitzt damit genau eine Nullstelle in k oder f besitzt keine Nullstelle in k. Im folgenden Beitrag wird gezeigt, dass sich die Situation im Fall von Polynomen zweier Variabler über einem endlichen Körper $\mathbf{F}_q$ deutlich vom Fall einer Veränderlichen unterscheiden kann. Der Autor weist nämlich auf elementare Weise nach, dass es absolut irreduzible Polynome $f \in \mathbf{F}_q[X, Y]$ gibt, für die $f(x, y) = 0$ für alle $x, y \in \mathbf{F}_q$ gilt. Da die explizit konstruierten Polynome hohen Grad haben können, hat dies insbesondere die interessante geometrische Konsequenz, dass es konkrete Beispiele von über $\mathbf{F}_q$ definierten (projektiv) algebraischen Kurven hohen Geschlechts mit vielen, d.h. mit $q + 1$, $\mathbf{F}_q$-rationalen Punkten gibt.

The following two well-known facts will be used in our construction:

Fact 1. $x^q - x = 0$ for any x in the finite field $\mathbf{F}_q$.

Fact 2. (*Eisenstein's theorem*) If

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in R[X]$$

is a primitive polynomial with coefficients in a unique factorization domain R and if an irreducible element $p \in R$ divides $a_0, a_1, \ldots, a_{n-1}$, p does not divide a_n and p^2 does not divide a_0, then $f(X)$ is irreducible in $R[X]$.

For details and proofs, one may consult, for example, [1] Lemma 2.3 for the first fact and [2, p. 74] for Eisenstein's theorem.

2 The construction

We now proceed to our construction. Let $\mathbf{F}_q$ be a finite field and $\phi(X) \in \mathbf{F}_q[X]$ be a quadratic irreducible. We can choose, for example,

$$\phi(X) = X^2 - \mu$$

if q is odd, with $\mu \in \mathbf{F}_q$ a quadratic nonresidue, and

$$\phi(X) = X^2 + X + \mu$$

if q is even, with $\mu \in \mathbf{F}_q$ having non-zero absolute trace (see [1], Corollary 3.79).

Clearly $\phi(X)$ is relatively prime to

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

Since $\mathbf{F}_q[X]$ is an Euclidean domain, from

$$(\phi(X), X^q - X) = 1$$

it follows (see [1], Theorem 1.55) that there exist polynomials $a(X), b(X) \in \mathbf{F}_q[X]$ with the property

$$a(X)\phi(X) + b(X)(X^q - X) = 1. \tag{1}$$

We are now in the position to state the following:

Theorem. *With the above notations, the polynomial*

$$f(X, Y) := Y^q - (1 - b(X)(X^q - X))\, Y + \phi(X)(X^q - X) \tag{2}$$

with coefficients in $\mathbf{F}_q$ *is irreducible and satisfies* $f(x, y) = 0$ *for any* $x, y \in \mathbf{F}_q$.

Proof. First of all, the fact $f(x, y) = 0$ for any $x, y \in \mathbf{F}_q$ is an immediate consequence of the Fact 1. On the other hand, $f(X, Y)$ can be viewed as a monic polynomial in Y with coefficients in $R := \mathbf{F}_q[X]$. All the non-leading coefficients of $f(X, Y)$ are divisible by the irreducible element $\phi(X) \in R$. Indeed, from (1) and (2) we get

$$f(X, Y) = Y^q - a(X)\phi(X)Y + \phi(X)(X^q - X).$$

Moreover, the free coefficient $\phi(X)(X^q - X)$ is not divisible by $\phi^2(X)$. It is now the moment to apply the second fact to conclude that $f(X, Y) \in R[Y] = \mathbf{F}_q[X, Y]$ is irreducible. □

3 A few examples and further remarks

The theorem proved in the previous section is an efficient tool of building irreducible polynomials in two variables with coefficients in a finite field which have a maximal possible zero set. By applying the method described above we find the following irreducibles that take the value zero at any point with coordinates in the specified finite field:

$$\text{Over } \mathbf{F}_2: \quad f(X,Y) = Y^2 + Y(X^2 + X + 1) + X^4 + X$$

$$\text{Over } \mathbf{F}_3: \quad f(X,Y) = Y^3 + Y(2X^4 + X^2 + 2) + X^5 + 2X$$

$$\text{Over } \mathbf{F}_5: \quad f(X,Y) = Y^5 + Y(X^6 + 4X^2 + 4) + X^7 + 4X^3 + 3X^5 + 2X$$

$$\text{Over } \mathbf{F}_7: \quad f(X,Y) = Y^7 + Y(X^8 + 6X^2 + 6) + X^9 + 4X^7 + 6X^3 + 3X$$

Remark 1. One may notice that (2) is an irreducible element of $\overline{\mathbf{F}}_q[X,Y]$ where $\overline{\mathbf{F}}_q$ represents an algebraic closure of $\mathbf{F}_q$. Indeed, let $\lambda \in \overline{\mathbf{F}}_q$ be a root of $\phi(X)$ in the quadratic extension of $\mathbf{F}_q$. Then, Eisenstein's theorem applies in a similar way to (2) together with the irreducible $X - \lambda \in \overline{\mathbf{F}}_q[X]$. Thus, we conclude that the polynomial we constructed is irreducible in the larger ring $(\overline{\mathbf{F}}_q[X])[Y] = \overline{\mathbf{F}}_q[X,Y]$.

Remark 2. Note that a slight modification of the above argument applies to infinite fields as well. Thus, if K is an infinite field then there are irreducible polynomials $f(X,Y) \in K[X,Y]$ such that the zero set $\{(x,y) \in K \times K : f(x,y) = 0\}$ contains a given *finite* subset $S \subset K \times K$. Indeed, let $\{x_1, \ldots, x_r\}$ and $\{y_1, \ldots, y_s\}$ be the set of distinct x- and y-coordinates of the points of S, respectively. Since K is infinite, it is possible to choose $\mu \in K \setminus \{x_1, \ldots, x_k\}$. Then, the polynomials $(X - x_1) \ldots (X - x_k)$ and $X - \mu$ (the analogues of $X^q - X$ and $\phi(X)$, respectively, in the above finite fields proof) are relatively prime. As before, we will select the two polynomials $a(X), b(X) \in K[X]$ satisfying

$$a(X)(X - \mu) + b(X)(X - x_1) \ldots (X - x_k) = 1. \tag{3}$$

Clearly, we may assume that $a(X)$ is not divisible by $X - \mu$ (it will be enough to note that if we replace $a(X)$ by $a(X) + (X - x_1) \ldots (X - x_k)h(X)$ and $b(X)$ by $b(x) - (X - \mu)h(X)$ where $h(X) \in K[X]$, the equality in (3) will be preserved). Then the polynomial $a(X)(X - \mu) = 1 - b(X)(X - x_1) \ldots (X - x_k)$ will take the value 1 on S. This, together with the fact that the polynomial in Y

$$(Y - y_1) \ldots (Y - y_s) = Y^s + c_{s-1}Y^{s-1} + \cdots + c_1 Y + c_0$$

takes the value zero on S, implies that the polynomial

$$\begin{aligned} f(X,Y) = {} & Y^s + c_{s-1}a(X)(X - \mu)Y^{s-1} + \cdots + c_1 a(X)(X - \mu)Y \\ & + c_0 a(X)(X - \mu) + (X - x_1) \ldots (X - x_k)(X - \mu) \end{aligned}$$

also takes the value zero on S. The fact that $f(X,Y) \in K[X,Y]$ is irreducible follows as a consequence of Eisenstein's theorem applied to $f(X,Y)$ viewed as a polynomial

in Y with coefficients in the unique factorization domain $R = K[X]$, together with the irreducible $p := X - \mu \in R$. Thus, $f(X, Y)$ will be an irreducible polynomial whose zero set contains the given finite set S. As in Remark 1 above, if we apply Eisenstein's theorem to $f(X, Y)$ viewed as an element of $(\overline{K}[X])[Y]$ we conclude that $f(X, Y)$ is in fact absolutely irreducible.

References

[1] R. Lidl and H. Niederreiter: *Finite fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[2] B.L. Van der Waerden: *Modern Algebra*, Volume 1, Frederick Ungar Publishing Co. New York 1953.

Mihai Caragiu
Ohio Northern University
Department of Mathematics
Ada, OH 45810, USA
e-mail: m-caragiu1@onu.edu