On the density of irreducible polynomials

by Wolmer V. Vasconcelos *

This short note concerns the frequency, in some sense to be precised, with which the irreducible polynomials appear in some polynomial rings. We deal specifically with the case when the coefficients are taken in a finite field.

To simplify the arguments we deal with prime fields, i. e. Z_p. Tentatively we define a set function on the class of subsets of the polynomial ring $R=Z_p[x]$. Let $S\subset Z_p[x]$. The polynomials in S of degree at most n are in a finite number, which we denote by $D_n(S)$. If $D_n(S)/D_n(R)$ has a limit as n increases, we denote it by $D(S)$ and the class of all such S by $\mathcal{S}$. The following obvious properties of D hold:

1. $D(R)=1$ (bounded)
2. If $S\subset S'$ then $D(S)\leqq D(S')$ (monotone)
3. If $S\cap S'=\emptyset$, then $D(S\cup S')=D(S)+D(S')$ (finitely additive).

We say that D is a density function on $\mathcal{S}$. The main result is:

THEOREM. *Let* I *be the subset of irreducible polynomials in* $Z_p[x]$, *then* $D(I)=0$.

PROOF. For definiteness let K be an algebraic closure of Z_p. Due to property 3. it is enough to prove for the subset $S\subset I$, consisting of monic polynomials. If $P(n)$ is the number of those polynomials of degree n, $n\cdot P(n)$ is the number of elements in K of degree n over Z_p. This follows from the fact that the roots of those polynomials are simple (Z_p is perfect) and distinct polynomials do not have a common root. On the other hand, if we adjoin to Z_p any element of degree n, the extension is the splitting field of $x^{p^n}-x$, and so each element of degree n over Z_p is root of this polynomial. Since it has not more than p^n roots we get $n\cdot P(n)\leqq p^n$.

This implies $D_n(S)=\sum_1^n P(k)\leqq\sum_1^n p^k/k$ so that $D_n(S)/D_n(R)\leqq\sum_1^n \frac{p^k/k}{p^{n+1}}$.

A straightforward use of the integral test will complete the proof. Just notice

$$\sum_2^n \frac{p^k}{k}\leqq\int_2^{n+1}\frac{p^x}{x}\,dx=\frac{1}{\log p}\frac{p^x}{x}\Big]_2^{n+1}+\frac{1}{\log p}\int_2^{n+1}\frac{p^x}{x^2}\,dx$$

and

$$\int_2^{n+1}\frac{p^x}{x^2}\,dx\leqq\frac{p^{n+1}}{(n+1)^2}\cdot(n-1).$$

It is clear that the same argument holds for $F[x]$ where F is any finite field. If instead, we take $Z[x]$ where Z is the ring of integers, we can cope with the infinity of elements in Z in the following way: the height of a polynomial is understood as the sum of the absolute values of its coefficients and for $S\subset Z[x]$, $D_n(S)$ is defined to be the number (finite) of polynomials in S of degree and height at most n. However a similar result for the irreducible polynomials does not seem to be at hand.

* Do Instituto de Física e Matemática da Universidade do Recife com uma bolsa de estudo da Capes na Universidade de Chicago.