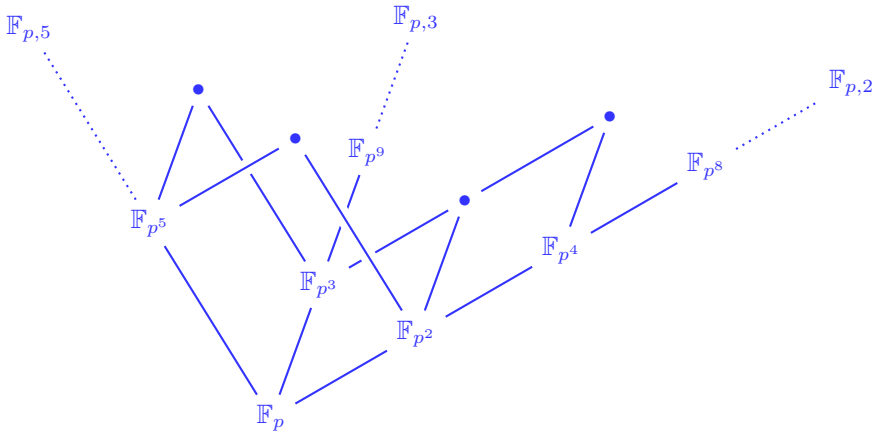
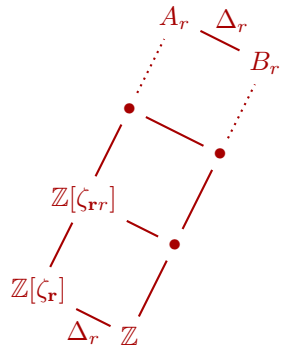
Standard models for finite fields: the definition

Bart de Smit and Hendrik W. Lenstra jr.
Mathematisch Instituut, Universiteit Leiden



Cyclotomic rings. Let r be a prime number and write $\mathbf{r} = r \cdot \gcd(r, 2)$. We write $\mathbb{Z}_r$ for the ring of r-adic integers, $\mathbb{Z}_r^*$ for its group of units, and Δ_r for the torsion subgroup of $\mathbb{Z}_r^*$; the group Δ_r is cyclic of order $\varphi(\mathbf{r})$, where φ denotes the Euler φ-function.

The ring A_r is defined to be the polynomial ring $\mathbb{Z}[X_0, X_1, X_2, \ldots]$ modulo the ideal generated by $\{\sum_{j=0}^{r-1} X_0^{j\mathbf{r}/r},\ X_{k+1}^r - X_k : k \geq 0\}$. For $k \in \mathbb{Z}_{\geq 0}$, we write $\zeta_{\mathbf{r}r^k}$ for the residue class of X_k in A_r, which is a unit of multiplicative order $\mathbf{r}r^k$. For each $u \in \mathbb{Z}_r^*$ there is a unique ring automorphism of A_r that maps each $\zeta_{\mathbf{r}r^k}$ to $\zeta_{\mathbf{r}r^k}^{\bar{u}}$, where $\bar{u} = (u \bmod \mathbf{r}r^k)$; we denote this ring automorphism by σ_u.



The ring B_r is defined by $B_r = \{a \in A_r : \sigma_u(a) = a \text{ for all } u \in \Delta_r\}$. For $k \in \mathbb{Z}_{>0}$, $i \in \{0, 1, \ldots, r-1\}$ the element $\eta_{r,k,i} \in B_r$ is defined by $\eta_{r,k,i} = \sum_{u \in \Delta_r} \sigma_u(\zeta_{\mathbf{r}r^k}^{1+i\mathbf{r}r^{k-1}})$.

Prime ideals. Let p, r be prime numbers with $p \neq r$, and let l be the number of factors r in the integer $(p^{\varphi(\mathbf{r})} - 1)/(\mathbf{r}^2/r)$. Denote by $S_{p,r}$ the set of prime ideals $\mathfrak{p}$ of B_r that satisfy $p \in \mathfrak{p}$. This set is finite of cardinality r^l, and for each $\mathfrak{p} \in S_{p,r}$ there exists a unique system $(a_{\mathfrak{p},j})_{0 \leq j < lr}$ of integers $a_{\mathfrak{p},j} \in \{0, 1, \ldots, p-1\}$ such that $\mathfrak{p}$ is generated by p together with $\{\eta_{r,k+1,i} - a_{\mathfrak{p},i+kr} : 0 \leq k < l,\ 0 \leq i < r\}$. We define a total ordering

on $S_{p,r}$ by putting $\mathfrak{p} < \mathfrak{q}$ if there exists $h \in \{0, 1, \ldots, lr-1\}$ such that $a_{\mathfrak{p},j} = a_{\mathfrak{q},j}$ for all $j < h$ and $a_{\mathfrak{p},h} < a_{\mathfrak{q},h}$. The smallest element of $S_{p,r}$ in this ordering is denoted by $\mathfrak{p}_{p,r}$.

We define $\mathbb{F}_{p,r}$ to be the ring $B_r/\mathfrak{p}_{p,r}$, and for $k \in \mathbb{Z}_{>0}$ we define $\alpha_{p,r,k} \in \mathbb{F}_{p,r}$ to be the residue class of $\eta_{r,k+l,0}$ modulo $\mathfrak{p}_{p,r}$.

Equal characteristic. Let p be a prime number and put $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let the element $f = f(X, Y)$ of the polynomial ring $\mathbb{F}_p[X, Y]$ be defined by $f = X^p - 1 - Y \cdot \sum_{i=1}^{p-1} X^i$. We define $\mathbb{F}_{p,p}$ to be the polynomial ring $\mathbb{F}_p[X_1, X_2, X_3, \ldots]$ modulo the ideal generated by $\{f(X_1, 1),\ f(X_{k+1}, X_k) : k > 0\}$. For $k \in \mathbb{Z}_{>0}$ we denote the image of X_k in $\mathbb{F}_{p,p}$ by $\alpha_{p,p,k}$.

An algebraic closure. Let p be a prime number. Then for any prime number r it is true that the ring $\mathbb{F}_{p,r}$ is a field containing $\mathbb{F}_p$; that for each $k \in \mathbb{Z}_{>0}$, the element $\alpha_{p,r,k}$ of $\mathbb{F}_{p,r}$ is algebraic of degree r^k over $\mathbb{F}_p$; and that one has $\mathbb{F}_{p,r} = \mathbb{F}_p(\alpha_{p,r,1}, \alpha_{p,r,2}, \ldots)$.

We write $\bar{\mathbb{F}}_p$ for the tensor product, over $\mathbb{F}_p$, of the rings $\mathbb{F}_{p,r}$, with r ranging over the set of all prime numbers. For any prime number r and $k \in \mathbb{Z}_{>0}$, the image of $\alpha_{p,r,k}$ under the natural ring homomorphism $\mathbb{F}_{p,r} \to \bar{\mathbb{F}}_p$ is again denoted by $\alpha_{p,r,k}$.

The ring $\bar{\mathbb{F}}_p$ is a field containing $\mathbb{F}_p$, and it is an algebraic closure of $\mathbb{F}_p$. We have $\bar{\mathbb{F}}_p = \mathbb{F}_p(\alpha_{p,r,k} : r \text{ prime},\ k \in \mathbb{Z}_{>0})$, each $\alpha_{p,r,k}$ being algebraic of degree r^k over $\mathbb{F}_p$.

A vector space basis. Let p be a prime number. For each $s \in \mathbb{Q}/\mathbb{Z}$, the element $\epsilon_s \in \bar{\mathbb{F}}_p$ is defined as follows. There exists a unique system of integers $(c_{r,k})_{r,k}$, with r ranging over the set of prime numbers and k over $\mathbb{Z}_{>0}$, such that each $c_{r,k}$ belongs to $\{0, 1, \ldots, r-1\}$ and s equals the residue class of $\sum_{r,k} c_{r,k}/r^k$ modulo $\mathbb{Z}$, the sum being finite in the sense that $c_{r,k} = 0$ for all but finitely many pairs r, k. With that notation, ϵ_s is defined to be the finite product $\prod_{r,k} \alpha_{p,r,k}^{c_{r,k}}$.

The system $(\epsilon_s)_{s \in \mathbb{Q}/\mathbb{Z}}$ is a vector space basis of $\bar{\mathbb{F}}_p$ over $\mathbb{F}_p$. In addition, for each $s \in \mathbb{Q}/\mathbb{Z}$ the degree of ϵ_s over $\mathbb{F}_p$ equals the order of s in the additive group $\mathbb{Q}/\mathbb{Z}$.

For any $n \in \mathbb{Z}_{>0}$, the $\mathbb{F}_p$-span of $\{\epsilon_s : s \in \mathbb{Q}/\mathbb{Z},\, ns = 0\}$ is the unique subfield of $\bar{\mathbb{F}}_p$ of cardinality p^n; it is denoted by $\mathbb{F}_{p^n}$.

Standard models for finite fields. Let p be a prime number and let n be a positive integer. Denote by e_0, e_1, …, e_{n-1} the standard basis of $\mathbb{F}_p^n$ over $\mathbb{F}_p$, and write ψ for the unique $\mathbb{F}_p$-vector space isomorphism $\mathbb{F}_p^n \to \mathbb{F}_{p^n}$ sending e_i to $\epsilon_{i/n \bmod \mathbb{Z}}$, for $0 \leq i < n$. Define a multiplication map on $\mathbb{F}_p^n$ by $v \cdot w = \psi^{-1}(\psi(v) \cdot \psi(w))$, for v, $w \in \mathbb{F}_p^n$. Together with vector addition, this multiplication makes $\mathbb{F}_p^n$ into a field with unit element e_0. This field is defined to be the standard model for a finite field of cardinality p^n.