1.5 Lecture 5: Finite fields

1.5.1 Some definitions

Let $\mathbb{A}$ be a ring.

- The **group of units in** $\mathbb{A}$, or the **group of invertible elements of** $\mathbb{A}$ is

$$\mathbb{A}^\times = \{a \in \mathbb{A} \mid \text{there exists } a^{-1} \in \mathbb{A} \text{ such that } a^{-1}a = aa^{-1} = 1\}.$$

- The **characteristic of** $\mathbb{A}$ is $p \in \mathbb{Z}_{>0}$ such that $\ker(\varphi) = p\mathbb{Z}$, where $\varphi\colon \mathbb{Z} \to R$ is the ring homomorphism given by $\varphi(1) = 1$.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{A} \\ 1 & \mapsto & 1 \end{array} \quad \text{has } \ker(\varphi) = p\mathbb{Z}.$$

Let $\mathbb{F}$ be a field.

- The **Frobenius map** is the field morphism $F\colon \mathbb{F} \to \mathbb{F}$ given by

$$\begin{array}{rl} \text{if } \mathrm{char}(\mathbb{F}) = 0 \text{ and } \alpha \in \mathbb{F} & \quad \text{then } F(\alpha) = \alpha, \\ \text{if } p \in \mathbb{Z}_{>0} \text{ and } \mathrm{char}(\mathbb{F}) = p \text{ and } \alpha \in \mathbb{F} & \quad \text{then } F(\alpha) = \alpha^p. \end{array}$$

- A **perfect field** is a field $\mathbb{F}$ such that the Frobenius map $F\colon \mathbb{F} \to \mathbb{F}$ is an automorpihsm.

Theorem 1.11. *(Classification of finite fields). The map*

$$\begin{array}{cccc} \mathbb{F}\colon & \{p^k \mid p, k \in \mathbb{Z}_{>0},\ p \textit{ is prime}\} & \leftrightarrow & \{\textit{finite fields}\} \\ & \mathrm{Card}(\mathbb{K}) & \longleftarrow & \mathbb{K} \\ & p & \longmapsto & \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \\ & p^k & \longmapsto & \mathbb{F}_{p^k} = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^k} = \alpha\} \end{array}$$

Proof. Let $\mathbb{K}$ be a finite field.
The ring homomorphism

$$\begin{array}{cccc} \varphi\colon & \mathbb{Z} & \to & \mathbb{K} \\ & 1 & \mapsto & 1 \end{array} \quad \text{is not injective.}$$

Let $p \in \mathbb{Z}_{>0}$ be minimal such that $\varphi(m) = 0$.
If $q, r \in \mathbb{Z}_{>0}$ and $p = qr$ then $\varphi(q)\varphi(r) = \varphi(qr) = \varphi(p) = 0$.
So $q = 1$ and $r = p$ or vice versa and p is prime.
So $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a subfield of $\mathbb{K}$.

So $\mathbb{K}$ is a finite dimensional $\mathbb{F}_p$-vector space.
So there exists $k \in \mathbb{Z}_{>0}$ such that $|\mathbb{K}| = p^k$.

Let $\alpha \in \mathbb{K}$ with $\alpha \neq 0$.
Since $\mathbb{K}^\times$ is an abelian group of order $p^k - 1$ then $\alpha^{p^k-1} = 1$.
So α is a root of $x^{p_k - 1} - 1$.
There are $p^k - 1$ roots of $x^{p^k-1} - 1$ (the $(p^k - 1)$th roots of unity) and

$$\mathrm{Card}(\mathbb{K}) = \mathrm{Card}(\mathbb{K}^\times) + \mathrm{Card}(\{0\}) = (p^k - 1) + 1 = p^k.$$

So

$$\mathbb{K} = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^k} = \alpha\}.$$

□