Workshop 4

Algebra 2

2026 Semester 1

Warm-up with finite fields

1. $char(K) = 7$, $[\mathrm{K} : \mathbf{F}_p] = 12$
2. $[K : \mathbf{F}_p] = [K : F][F : \mathbf{F}_p]$ where $[F : \mathbf{F}_p] = m$
3. The field K has a unique subfield of size 7^m and is given by
$$F = \{x \in K \mid x^{7^m} - x = 0\}.$$
4. We subtract elements in smaller subfields (degree dividing 12) using inclusion-exclusion. $7^{12} - 7^6 - 7^4 + 7^2$

Finite fields and bit strings

1. If $x = b_0b_1b_2b_3$ and $y = c_0c_1c_2c_3$, then $x + y = (b_0 + c_0, b_1 + c_1, b_2 + c_2, b_3 + c_3) \mod 2$
2. $a \cdot (b_0 + b_1a + b_2a^2 + b_3a^3) = b_3 + (b_0 + b_3)a + b_1a^2 + b_2a^3$
3. (a) If we call the bit-string 1110 by "14", then this is not the image of 14 under the usual homomorphism $\mathbf{Z} \to \mathbf{F}$ where $n \mapsto n \cdot 1$, because $14 \cdot 1 = 0$ in F.
   (b) Take $x = 1 + a + a^2 = 0111 =$ "7" and $y = 1 = 0001 =$ "1". In F, $x + y = a + a^2 = 0110 =$ "6". But as integers $7 + 1 = 8$.

   Let $x = a =$ "2" and $y = a^3 =$ "8". In F, $xy = 1 + a =$ "3", but in integers $2 \cdot 8 = 16$.

The Frobenius

1. We have $(x+y)^p = x^p + y^p$ since other coefficients in the binomial expansion have p as a factor, and $(xy)^p = x^p y^p$.

   The non-zero elements of $\mathbf{F}_p$ form the multiplicative group $\mathbf{F}_p^\times$, which has order $p-1$. By Lagrange's theorem, the order of any element divides the order of the group, so for all $x \in \mathbf{F}_p^\times$ we have

   $$x^{p-1} = 1.$$

   Multiplying both sides by x, it follows that $x^p = x$ for all non-zero $x \in \mathbf{F}_p$. The equality also holds trivially for $x = 0$. Therefore, for all $x \in \mathbf{F}_p$, we have

   $$x^p = x.$$

   Hence, the Frobenius map $x \mapsto x^p$ is the identity map on $\mathbf{F}_p$.

2. In the previous problem, we showed that if $\alpha \in \mathbf{F}_p$, then $\alpha^p = \alpha$. Conversely, suppose that α satisfies $\alpha^p = \alpha$. We show that $\alpha \in \mathbf{F}_p$.

   Consider the polynomial $f(x) = x^p - x \in \mathbf{F}_p[x]$. Since $\deg(f) = p$, it has at most p roots. Every element $a \in \mathbf{F}_p$ satisfies $a^p = a$, so all elements of $\mathbf{F}_p$ are roots of $f(x)$. Thus, $f(x)$ has exactly p distinct roots, namely the elements of $\mathbf{F}_p$.

3. Given a field K such that $|K| = p^r$. We have $Frob^r(\alpha) = \alpha^{p^r} = \alpha$, since $K^\times = K \backslash \{0\}$ is the multiplicative group and order of any element divides the order of the group.

   Suppose there exists $d < r$ such that $Frob^d(\alpha) = \alpha$ for all $\alpha \in K$. That is, $\alpha^{p^d} = \alpha$ for all $\alpha \in K$, which implies the equation $x^{p^d} - x = 0$ has p^r solutions. This is a contradiction since $x^{p^d} - x = 0$ has at most p^d roots and $p^d < p^r$.

4. Suppose $m_\alpha(x) \in \mathbf{F}_p[x]$ is the minimal polynomial of α. Then

   $$m_\alpha(Frob(\alpha)) = m_\alpha(\alpha^p) = (m_\alpha(\alpha))^p = 0,$$

   since the coefficients of $m_\alpha(x)$ are in $\mathbf{F}_p$. Since $Frob(\alpha)$ is a root of $m_\alpha(x)$ and $m_\alpha(x)$ is irreducible in $\mathbf{F}_p[x]$, it is also the minimal polynomial of $Frob(\alpha)$.

Let

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where $\alpha_1 = \alpha$, $\alpha_2 = \alpha^p, \ldots, \alpha_n = \alpha^{p^n}$. Let $m_\alpha(x)$ be the minimal polynomial of α, we need to show that $m_\alpha(x) = f(x)$. By definition α is a root of $f(x)$. Enough to show that $f(x) \in \mathbf{F}_p[x]$ and is irreducible.

If $Frob(f(x)) = f(x)$, then $f(x) \in \mathbf{F}_p[x]$. We have

$$f(x)^p = (x - \alpha_1^p)(x - \alpha_2^p) \cdots (x - \alpha_n^p) = f(x),$$

since the Frobenius map cyclically permutes the roots. Therefore, $f(x) \in \mathbf{F}_p[x]$.

By definition of the minimal polynomial, $m_\alpha(x)$ divides $f(x)$. Since $\alpha_1, \alpha_2, \ldots, \alpha_n$ are roots of the minimal polynomial $m_\alpha(x)$, we have $f(x)$ divides $m_\alpha(x)$. Thus, $m_\alpha(x) = f(x)$.