Workshop 5

Algebra 2

2026 Semester 1

Warm-up with finite fields

Let K be a finite field of size $q = 7^{12}$.

1. What is the characteristic of K? What is the degree of the extension $\mathbf{F}_p \subset K$?
2. Suppose K contains a subfield F of size 7^m. Prove that m must divide 12.
   Hint: Consider the extension $F \subset K$.
3. Conversely, suppose m divides 12. Does K have a subfield of size 7^m? How many? How do we find them?
4. How many elements of K have degree 12 over $\mathbf{F}_p$?
   This is a bit tricky. Warm-up by looking at fields of smaller size like $7^2, 7^3, 7^4$, and 7^6.

Finite fields and bit strings

Let $F = \mathbf{F}_2[a]/(a^4 + a + 1)$. Note that $1, a, a^2, a^3$ is a basis of F as an $\mathbf{F}_2$ vector space. So we can represent every element of F uniquely as $b_0 + b_1 a + b_2 a^2 + b_3 a^3$, where $b_0, \ldots, b_3 \in \mathbf{F}_2$.

1. We abbreviate $b_0 + b_1 a + b_2 a^2 + b_3 a^3$ by the bit-string $b_0 b_1 b_2 b_3$. Then the elements of F are represented by the 16 strings $0000, 0001, 0010, \ldots, 1111$. Explain the addition law of F in terms of bit-strings.
2. Describe multiplication by a in terms of bit-strings.
3. Sometimes, instead of writing the 4 bit-strings, people write the integer they represent in binary notation, for exmaple, writing "14" for the bit-string "1110". Then the elements of F become the more familiar symbols $0, \cdots, 15$ (for example, $a^3 + a^2 + a$ will be "14").
   (a) Show that this representation conflicts with our convention that the integer symbol n represents the image of n under the unique homomorphism from $\mathbf{Z}$.
   (b) Show that this representation respects neither the addition nor the multiplication law.

The Frobenius

1. Let R be any ring of characteristic p. Prove that the map $R \to R$ that raises every element to the p-th power is a ring homomorphism. This homomorphism is called the Frobenius homomorphism. On $\mathbf{F}_p$, what does the Frobenius do?
2. Let K be a finite field of size p^r. Prove that $\alpha \in K$ lies in $\mathbf{F}_p \subset K$ if and only if $\mathrm{Frob}(\alpha) = \alpha$.
3. With K as above, prove that Frob applied r times is the identity on K and r is the smallest with this property.
4. With K as above, prove that α and $\mathrm{Frob}(\alpha)$ have the same minimal polynomial over $\mathbf{F}_p$.
   In fact, let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be the orbit of the Frobenius applied to α (the set of elements that we get if we repeatedly apply Frob to α; this set will have at most r elements, but possibly fewer; in fact, its size will be a factor of r). Show that the minimal polynomial of α over $\mathbf{F}_p$ is
   $$(x - \alpha_1) \cdots (x - \alpha_n).$$