Algebra II: Tutorial 10

April 20, 2022

Problem 1 (Finite fields are normal)**.** Let $f(x)$ be a monic irreducible polynomial over $\mathbb{F}_p$, and let α be a root of f in some splitting field of f over $\mathbb{F}_p$. Show that $L = \mathbb{F}_p(\alpha)$ is a splitting field for f over $\mathbb{F}_p$.

Solution. By the structure theory of finite fields, we know that every finite field L is the splitting field of some polynomial over $\mathbb{F}_p$; in particular L is normal. Since f is irreducible over $\mathbb{F}_p$ and has a root in L, f splits completely in L. A straightforward argument shows that L is then a splitting field. ■

Problem 2. Show that there are exactly two cubic irreducible polynomials in $\mathbb{F}_2[x]$, namely $f = x^3 + x + 1$ and $g = x^3 + x^2 + 1$. Write down the multiplication tables of the field extensions of $\mathbb{F}_2$ by adding a root of f and g, say $\mathbb{F}_8$ and $\mathbb{F}'_8$. Show that they are isomorphic.

Solution. This is a tedious but straightforward exercise. We omit the solution. ■

Problem 3 (Recognising prime subfields of finite fields)**.** Let L be a field containing $\mathbb{F}_p$. For $\alpha \in L$, show that $\alpha \in \mathbb{F}_p$ if and only if $\alpha^p - \alpha = 0$.

Solution. This is a special case of a theorem in the notes. If $\alpha \in \mathbb{F}_p$, then either $\alpha = 0$ or $\alpha \in \mathbb{F}_p^*$. In the former case, our claim holds trivially. In the latter case, $\mathbb{F}_p^*$ is an abelian group of order 8, so $\alpha^8 = 1$, which proves our claim. Conversely, any element $\alpha \in L$ satisfying $\alpha^p - \alpha = 0$ is a root of the polynomial $f_1(x) = x^p - x$. This polynomial has at most p roots, and all the elements in $\mathbb{F}_p$ are roots, hence any root must be an element of $\mathbb{F}_p$. ■

Problem 4. Let $f(x) = x^9 - x + 1$ in $\mathbb{F}_3$.

1. Show that f has no roots in $\mathbb{F}_3$ and in $\mathbb{F}_9$.
2. Show that $\mathbb{F}_{27} \cong \frac{\mathbb{F}_3[x]}{(x^3-x-1)}$, and show that every root of $x^3 - x - 1$ is a root of f.
3. Determine all the roots of f over $\mathbb{F}_{27}$, and deduce a factorisation of f over $\mathbb{F}_3$.

Solution. 1. A direct computation shows that f has no roots in $\mathbb{F}_3$. Let $\alpha \in \mathbb{F}_9$, in particular $\alpha^9 = \alpha$, and so $f(\alpha) = 1$, so f has no roots in $\mathbb{F}_9$.
2. It is easy to see that $x^3 - x - 1$ has no roots in $\mathbb{F}_3$ and so is irreducible over $\mathbb{F}_3$. The quotient $\frac{\mathbb{F}_3[x]}{(x^3-x-1)}$ is a finite field extension of $\mathbb{F}_3$ of degree $\deg(f) = 3$, so is isomorphic to $\mathbb{F}_{27}$. Let $\alpha \in \mathbb{F}_{27}$ be a root of $x^3 - x - 1$. Then, $\alpha^9 - \alpha + 1 = (\alpha + 1)^3 - \alpha + 1$. By the binomial identity for fields with characteristic p, $(\alpha + 1)^3 = \alpha^3 + 1 = \alpha + 2$, so $\alpha^9 - \alpha + 1 = \alpha + 2 - \alpha + 1 = 0$.
3. By part 2. we know that $x^3 - x - 1$ divides f, and a direct computation shows that $f(x) = (x^3 - x - 1)(x^6 + x^4 + x^3 + x^2 - x - 1)$. Note that any element of $\mathbb{F}_{27}$ can be expressed uniquely as $\beta = a\alpha^2 + b\alpha + c$ for $a, b, c \in \mathbb{F}_3$. Note that

$$\begin{aligned}\beta^9 - \beta + 1 &= a\alpha^{18} + b\alpha^9 + c - (a\alpha^2 + b\alpha + c) + 1 \\ &= a(\alpha + 1)^6 + b(\alpha + 1)^3 - a\alpha^2 - b\alpha + 1 \\ &= a\alpha + 2(b + 1).\end{aligned}$$

Suppose now that β is a root of $f(x)$, i.e. $\beta^9 - \beta + 1 = a\alpha + 2(b+1) = 0$. This implies that $a = 0$ and $b = -1$, with $c \in \mathbb{F}_3$ free. Then, a direct check shows that $\alpha, \alpha + 1$ and $\alpha + 2$ are indeed the only roots of f (this fact could already be established combining Problem 1 with the fact that there are at most three roots of f in $\mathbb{F}_{27}$). Notice this already implies that $x^6+x^4+x^3+x^2-x-1$ is irreducible over $\mathbb{F}_3$, and $f(x) = (x^3-x-1)(x^6+x^4+x^3+x^2-x-1)$ is a factorisation into irreducibles over $\mathbb{F}_3$. Suppose not, say $g(x) = x^6+x^4+x^3+x^2-x-1$ is reducible over $\mathbb{F}_3$. Then, $g(x)$ has an irreducible factor of degree 1, 2 or 3. By Problem 1, $g(x)$ splits into linear factors in a field extension of degree 1, 2 or 3 respectively. Yet we have shown that g has no roots in $\mathbb{F}_3$, $\mathbb{F}_9$. Furthermore, f has three roots in $\mathbb{F}_{27}$, none of which are roots of g: this is a contradiction. ■