Yellow Group

March 19, 2021

0.1 DF 13.1.3

Show that $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and let θ be a root. Compute the powers of θ in $\mathbb{F}_2(\theta)$.

As neither 0 or 1 is a root of $x^3 + x + 1$, it must be irreducible over F_2 since it can only be reducible if it has a linear factor. We note that $1, \theta, \theta^2$ are not reducible in any way so we leave them as is. We can then get that

$$\theta^3 = -\theta - 1 = \theta + 1$$

$$\theta^4 = \theta * (\theta^3) = \theta^2 + \theta$$
$$\theta^5 = \theta^2 * (\theta^3) = \theta^2 + \theta + 1$$
$$\theta^6 = \theta * (\theta^5) = \theta^3 + \theta^2 + \theta = \theta^2 + \theta + \theta + 1 = \theta^2 + 1$$
$$\theta^7 = \theta * (\theta^6) = \theta^3 + \theta = \theta + \theta + 1 = 1$$

0.2

Determine the minimal polynomial over Q for the element $1 + i$.

Since our factors must be entirely in $\mathbb{Q}$, we must have that the complex conjugate of $1+i$ is also a root, ie that $1-i$ is a root. This polynomial looks like $(x-(1+i))(x-(1-i)) = x^2 - 2x + 2$. Since neither of those roots are in $\mathbb{Q}$, this must be the minimal polynomial.

0.3

Let F be a finite field of characteristic p. Prove that $|\mathbb{F}| = p^n$ for some positive integer n.

Since the characteristic of F is p, we have that its prime subfield $F_p \cong \mathbb{Z}/p\mathbb{Z}$. It is clear then that F is a vector space over F_p, and the dimension of F is $[F : F_p] = n$ so

$$\dim F = \dim F_p$$

are isomorphic as vector spaces. This implies that $|F| = |(F_p)^n| = |F_p|^n = |\mathbb{Z}/p\mathbb{Z}|^n = p^n$.

0.4

DF 13.2 4
Determine the degree over $\mathbb{Q}$ of $2 + \sqrt{3}$ and of $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

The minimal polynomial for $2 + \sqrt{3}$ is clearly just $(x - 2)^2 - 3$, so it has degree 2 over $\mathbb{Q}$.
For the second value, let us first set $x = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ and note that $x = 1 + (1 + \sqrt[3]{2})\sqrt[3]{2}$, so is contained within $\mathbb{Q}(\sqrt[3]{2})$, which implies that $\mathbb{Q}(x) \subseteq \mathbb{Q}(\sqrt[3]{2})$. To show the opposite direction, note that $\sqrt[3]{2}+\sqrt[3]{4} \in \mathbb{Q}(x)$, implying that $(\sqrt[3]{2}+\sqrt[3]{4})^2 = \sqrt[3]{4}+4+2\sqrt[3]{2} \in \mathbb{Q}(x)$. Subtracting the first from the square of the first, then we get $\sqrt[3]{2}+4$, which implies that $\sqrt[3]{2} \in \mathbb{Q}(x)$, which implies that $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(x)$, which implies that $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(x)$, showing that x has degree 3 over $\mathbb{Q}$.

0.5 Advanced problem A

DF 13.1 8

Prove that $f_a(x) = x^5 - ax - 1 \in \mathbb{Z}[x]$ is irreducible unless $a = 0, 2$, or -1. The first two correspond to linear factors, the third corresponds to the factorization $(x^2 - x + 1)(x^3 + x^2 - 1)$.

$a = 0 \implies x^5 - 1$
$a = 2 \implies x^5 - 2x - 1$

Suppose that $f_a(x)$ is reducible. Then it factors as a product of a degree 1 and degree 4 polynomial, or it factors as a product of a degree 3 and degree 2 polynomial. In the first case, suppose

$f_a(x) = g(x) \cdot h(x)$, where

$$g(x) = g_3x^3 + g_2x^2 + g_1x + g_0$$

$$h(x) = h_2x^2 + h_1x + h_0$$

$\Rightarrow f_a(x) = g_3x$ need to multiply this out and equate coefficients

0.6 Advanced problem B

Put $F = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and $F' = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We are askled to show that $F = F'$. Let $x \in F$ be given. Then x can be written as

$$x = a + b(\sqrt{2} + \sqrt{3})$$

$$= a + b\sqrt{2} + b\sqrt{3}$$

which clearly lies in F'. We conclude that $F \subset F'$. Now, it is clear that $\sqrt{2} + \sqrt{3} \in F'$, then so is the square

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \in F'$$

$$\Rightarrow -5 + 5 + \frac{1}{2}(2\sqrt{6}) = \sqrt{6} \in F'$$

With some creativity, we can then express $\sqrt{2}$ in terms of elements of F':

$$\sqrt{2} = \sqrt{6}(\sqrt{2} + \sqrt{3}) - 2(\sqrt{2} + \sqrt{3})$$

which implies that $\sqrt{2} \in F'$. Then since $\sqrt{2} \in F'$, we have that

$$(\sqrt{3} + \sqrt{2}) - \sqrt{2} = \sqrt{3} \in F'$$

so

$$\sqrt{2}, \sqrt{3} \in F'$$

which clearly shows that $F' \subset F$.

0.7 Advanced problem C

DF 13.2 12

Suppose the degree of an extension K/F is a prime p. Show that any subfield E of K containing F is either K or F.

By the corrolary of the tower theorem, we have that

$$[E : F] | [K : F] \implies [E : F] | p \implies ([E : F] = p) \vee ([E : F] = 1)$$

0.8 Advanced problem D

DF 13.2 14
Prove that if [F(a):F] is odd, then F(a) = F(a^2)
To see this, first note that $a^2 \in F(a)$ automatically, so $F(a^2) \subseteq F(a)$. To show the opposite direction, let us assume that a is not an element of F(a^2)