MA503: Homework 9

Exercise 9.1. [5pts] Let F_1, F_2 be subfields of a field E. Prove that $F = F_1 \cap F_2$ is a subfield of E.

Solution:

- F is closed under $+$ and $\cdot$ because for any $a, b \in F$ we have

$$\begin{aligned} a, b \in F &\Rightarrow a, b \in F_1 \text{ and } a, b \in F_2 \\ &\Rightarrow a + b \in F_1 \text{ and } a + b \in F_2 \\ &\Rightarrow a + b \in F_1 \cap F_2 = F, \end{aligned}$$

  similarly,

$$\begin{aligned} a, b \in F &\Rightarrow a, b \in F_1 \text{ and } a, b \in F_2 \\ &\Rightarrow a \cdot b \in F_1 \text{ and } a \cdot b \in F_2 \\ &\Rightarrow a \cdot b \in F_1 \cap F_2 = F. \end{aligned}$$

- $0 \in F_1$ and $0 \in F_2 \quad \Rightarrow \quad 0 \in F_1 \cap F_2 = F$.
- $1 \in F_1$ and $1 \in F_2 \quad \Rightarrow \quad 1 \in F_1 \cap F_2 = F$.
- F with any x contains $-x$:

$$\begin{aligned} x \in F = F_1 \cap F_2 &\Rightarrow x \in F_1 \text{ and } x \in F_2 \\ &\Rightarrow -x \in F_1 \text{ and } -x \in F_2 \\ &\Rightarrow -x \in F_1 \cap F_2 = F. \end{aligned}$$

- F with any non-trivial x contains x^{-1}:

$$\begin{aligned} x \in F = F_1 \cap F_2 &\Rightarrow x \in F_1 \text{ and } x \in F_2 \\ &\Rightarrow x^{-1} \in F_1 \text{ and } x^{-1} \in F_2 \\ &\Rightarrow x^{-1} \in F_1 \cap F_2 = F. \end{aligned}$$

- $+$ and $\cdot$ are associative and commutative because E is a field.
- Distributivity holds as well because E is a field.

□

Exercise 9.2. [16pts] Let $f(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$.

(a) Show that $f(x)$ is irreducible. Hence, $E = F[x]/f(x)$ is a field.
(b) Is $x^3 - x^2 - 1$ trivial in E, or not? Why?
(c) $x^3 + 2x = 2x^2$ in E, or not? Why?
(d) Find the multiplicative inverse of $x + 1$ in E.
(e) $\chi(E) =$
(f) $|E| =$
(g) Find the order of $x + 2$ in E.
(h) Is x a primitive root in E?

Solution: (a) A quadratic polynomial $f(x)$ is irreducible because it has no zeros in $\mathbb{Z}_3$:

$$f(0) = 2 \qquad\qquad f(1) = 1 \qquad\qquad f(2) = 2.$$

(b) $x^3 - x^2 - 1$ is trivial modulo $I = \langle f(x) \rangle$ because

$$x^3 - x^2 - 1 = (x + 1)f(x)$$

and, so, $x^3 - x^2 - 1 \in I$.

(c) Yes, $x^3 + 2x = 2x^2$ in E, because $(x^3 + 2x) - (2x^2) = x^3 + x^2 + 2x = xf(x) \in I$.

(d) We can use the Euclidean algorithm for $f(x) = x^2 + x + 2$ and $g(x) = x + 1$:

$$f(x) = xg(x) + \mathbf{2} \qquad \Rightarrow \quad \gcd(f, g) = \gcd(2, x + 1) = 2$$

And, hence

$$2 = f(x) - xg(x)$$

Multiplying by 2 we get

$$1 = 2f(x) - 2xg(x).$$

Therefore, $1 = 2f(x) - 2xg(x) = -2xg(x)$ in E. Hence,

$$(x + 1)^{-1} = -2x = x \text{ in } E.$$

(e) $\chi(E) = 3$ because $1 + 1 + 1 = 0$ in E.

(f) $|E| = p^n$, where $p = 3$ and $n = 2 = \deg(f)$.

(g) $|E^*| = 8$. Hence, the order of every $\alpha \in E^*$ is a divisor of 8. Hence, $|x + 2| = 2, 4$, or 8. Direct computations produce the following:

$$\begin{aligned} (x+2)^2 &= x^2 + 4x + 4 \equiv_{f(x)} 2 \not\equiv_{f(x)} 1 \\ (x+2)^4 &\equiv_{f(x)} 2^2 = 4 \equiv_{f(x)} 1. \end{aligned}$$

Thus, $|x + 2| = 4$.

(h) As in (g)

$$\begin{aligned} x^2 &\equiv_{f(x)} 2x + 1 \not\equiv_{f(x)} 1 \\ x^4 &\equiv_{f(x)} (2x+1)^2 = 4x^2 + 4x + 1 \equiv_{f(x)} 2. \end{aligned}$$

Therefore, $|x| = 8$ and x is a primitive root.

$\square$