MATH 4576 Rings and Fields | QUIZ 7
Prof. I. Drozd | Spring 2011

(1) Find an irreducible polynomial $p(x)$ of degree 2 over Z_5.

The polynomial $x^2 - 2$ has no roots in Z_5 (verify!) and is of degree 2, so it is irreducible.

(2) Construct a field K with 25 elements.

Let $K = Z_5(\theta)$, where θ is a root of $p(x) = x^2 - 2$. Then $[K : Z_5] = \deg p(x) = 2$, therefore $\#(K) = 5^2 = 25$.

(3) Find a primitive element β of the field K, that is an element $\beta \in K$ such that $K = \{ 0, 1, \beta, \beta^2, \dots, \beta^{23} \}$.

Try $\beta = \theta + 2$. Find $\mathrm{ord}(\beta)$:

$\beta^2 = \theta^2 + 4\theta + 4 = -\theta + 1$ (since $\theta^2 = 2$),

$\beta^3 = -\theta$,

$\beta^5 = \theta^5 + 2^5 = 4\theta + 2 = -\theta + 2$ (since $\mathrm{char}\, K = 5$),

$\beta^8 = 2 - 2\theta \neq 1$,

$\beta^{10} = \theta + 1$,

$\beta^{12} = -1$.

Since $\beta^8 \neq 1$, $\beta^{12} \neq 1$, the only possibility is that $\mathrm{ord}(\beta) = 24$. Then all elements $\{ 1, \beta, \beta^2, \dots, \beta^{23} \}$ are different, therefore $K = \{ 0, 1, \beta, \beta^2, \dots, \beta^{23} \}$.

(Note that $\theta + 1$ does not match, since $(\theta + 1)^3 = 2$ and $(\theta + 1)^{12} = 2^4 = 1$).

(4) Find an irreducible polynomial of degree 2 over K.

Let $f(x) = x^2 - \beta$. We verify that it has no roots in K. Indeed, every nonzero element $\gamma \in K$ equals β^k for some $0 \leq k < 24$. Then $\gamma^2 = \beta^{2k}$. If $\beta^{2k} = \beta$, then $\beta^{2k-1} = 1$, hence $24 \mid 2k - 1$, which is impossible, since $2k - 1$ is odd and 24 are even. Therefore $f(x)$ has no roots in K, so it is irreducible.

Note that the answers are NOT unique!