Mathematics 3: Algebra

Workshop 3

Fields as vector spaces

The aim of this workshop is to work with some fields as vector spaces, particularly over the 3-element field $\mathbb{F}_3$.

(1) (a) Let F be a field. Prove that if a polynomial $P(x) \in F[x]$ is of degree 2 or 3 and $P(x) = 0$ has no root in F, then $P(x)$ is irreducible over F.
(b) Find all irreducible monic (i.e., leading coefficient 1) quadratic polynomials over $\mathbb{F}_3$.
(c) Give an example of a quartic polynomial $P(x)$ over $\mathbb{F}_3$ that is reducible but $P(x) = 0$ has no roots in $\mathbb{F}_3$.
(d) (Back to F) Suppose that $P(x) \in F[x]$ and that $P(\alpha) = 0$. Let $k \in \mathbb{Z}$. Write down polynomials $P_-(x)$ and $P_k(x) \in F[x]$ of the same degree as P and such that $P_-(-\alpha) = 0$ and $P_k(\alpha + k) = 0$.
(e) (Back to $\mathbb{F}_3$!) Let α be a root of $x^2 + 1 = 0$, and F_1 be the field $\mathbb{F}_3[\alpha]$. Write down a basis for F_1, considered as a vector space over $\mathbb{F}_3$. Write out the elements of F_1 explicitly.
(f) For which elements α' of F_1 do 1 and α' form a basis for F_1 over $\mathbb{F}_3$?
(g) Show that all the polynomials you found in (b) above have a root in F_1.
(h) Deduce that if you repeat the construction in (e) above with a different quadratic polynomial irreducible over $\mathbb{F}_3$ (instead of x^2+1), you get the same field F_1.

(a) A reducible polynomial of degree two must be a product of linear factors, and so have a root in F. So if it has no root in F, it must be irreducible.
A reducible polynomial of degree three must be eith a product of 3 linear factors, or a product of a linear factor and a quadratic factor. In each case it has a root in F. So if it has no root in F, it must be irreducible.
(b) There are three: x^2+1, x^2+2x+2 and x^2+x+2.
(c) $(x^2+1)^2$.
(d) Define $P_-(x) = P(-x)$. Then $P_-(-\alpha) = P(-(-\alpha)) = P(\alpha)$=0.
Define $P_k(x) = P(x-k)$. Then $P_k(\alpha+k) = P((\alpha+k)-k) = P(\alpha)$=0.
(e) $1, \alpha$ is a basis. Elements of F_1 are $0, 1, -1, 0+\alpha, 1+\alpha, -1+\alpha, 0-\alpha, 1-\alpha, -1-\alpha$.
(f) $1, \alpha'$ are a basis for F_1 for α' any element of F_1 except $0, 1$ or -1

(g) Now $x^2+2x+2 = (x+1)^2+1$, so has $\alpha-1 (= \alpha+2)$ as a root. Its other root is $-\alpha-1$.

Also $x^2+x+2 = (x+2)^2+1$, so it has $\alpha+1$ as a root. Other root is $-\alpha+1$.

Since x^2+1 has a root α in F_1, all three polynomials have a root in F_1.

(h) You will again get a 9-element field, but because the roots of all polynomials lie in F_1, the field you get will be a 9-element subfield of F_1, and so the whole of F_1.

(2) (a) *Counting the number of irreducible monic quadratic polynomials over $\mathbb{F}_p$, p a prime.*

Criticise and correct the following argument:

" For a polynomial x^2+ax+b over $\mathbb{F}_p$, there are p choices for each of a and b, and so p^2 such polynomials in total. If the polynomial is reducible, it factorises as $(x-\alpha)(x-\alpha')$ say, where α and α' are also in $\mathbb{F}_p$. Again there are p choices for each of α and α', but their order is unimportant, so the number of unordered pairs α, α' is $\binom{p}{2} = p(p-1)/2$. Hence the number of reducible polynomials is $p(p-1)/2$, and so the number of irreducible polynomials x^2+ax+b is $p^2 - p(p-1)/2 = p(p+1)/2$."

(b) Check your corrected result from (a) for $p=3$ (see 1(b) above) and $p=2$.

(a) There are indeed p^2 polynomials in total. But $\binom{p}{2} = p(p-1)/2$ counts only the unordered pairs α, α' where $\alpha \neq \alpha'$. We must also allow the possibility that $\alpha = \alpha'$, giving p more reducible polynomials $(x-\alpha)^2$. So the total number of reducible polynomials is $p(p-1)/2+p = p(p+1)/2$, and so the number of irreducible polynomials x^2+ax+b is $p^2-p(p+1)/2 = p(p-1)/2$.

[For those who did Discrete Maths: we're actually counting the number of two-element multisubsets α, α' of $\{0,1,2,\ldots,p-1\}$ here. This gives $p(p+1)/2$ directly for the number of reducible polynomials.]

(b) Indeed, for $p=3$, we have $p(p-1)/2 = 3$, as in Q 1(b). For $p = 2$ we have $p(p-1)/2 = 1$, and x^2+x+1 is indeed the unique irreducible quadratic polynomial over $\mathbb{F}_2$.