MATH H113: Honors Introduction to Abstract Algebra

2016-04-22

- Polynomials over fields
- Constructing a field extension in which a given polynomial of degree > 0 has a root

For Wednesday: Read §13.1 and 9.3

Recall *Ex. 7.4.14*: Let $f(x) \in R[x]$ (R is a commutative ring with $1 \neq 0$) be a monic polynomial of degree ≥ 1, and let bar denote passage from $R[x]$ to $R[x]/(f(x))$. Then:

a. Every element of $R[x]/(f(x))$ is represented by an element $\overline{p(x)}$, where $p(x) \in R[x]$ has degree $< n$ (or is 0)>
b. If $\overline{p(x)} = \overline{q(x)}$ with both p and q of degree $< n$ (or zero), then $p(x) = q(x)$.

Theorem: Let F be a field. Then $F[x]$ is a Euclidean domain, with norm $N(f(x)) = \begin{cases} \deg f & f \neq 0 \\ 0 & f = 0 \end{cases}$
Proof: We need to show: given $a(x), b(x) \in F[x]$ with $b(x) \neq 0$, there exist $q(x), r(x) \in F[x]$ such that $a(x) = q(x)b(x) + r(x)$ and $\deg r(x) < \deg b(x)$ or $r(x) = 0$).
Case 1: $\deg b(x) = 0$. Then $b(x) = c \in F$, and we have $a = qb + r$ with $q(x) = \frac{1}{c}a(x)$ and $r(x) = 0$.
Case 2: $\deg b(x) >$). Let c be the leading coefficient of $b(x)$ and let $n = \deg b(x)$. Let $f(x) = \frac{1}{c}b(x)$. This is monic of degree n, so by Ex. 7.4.14, $\overline{a(x)} \in R[x]/(f(x))$ is represented by $overliner(x)$ with $r = 0$ or $\deg r < n$. THen $f(x) \mid (a(x) - r(x))$, so $b(x) \mid (a(x) - r(x))$, say $b(x)q(x) = a(x) - r(x)$, $\therefore a(x) = q(x)b(x) + r(x)$ with $r = 0$ or $\deg r < n$.
Note: We also have uniqueness (as for $\mathbb{Z}$): If $a(x) = q_1(x)b\underline{(x) + r}\underline{_1(x)} = \underline{q_2(x)}b(x) + r_2(x)$ where r_1 and r_2 are 0 or have degree $< n$, Then $\overline{a(x)} = \overline{r_1(x)} = \overline{r_2(x)}$, so by (b) $r_1(x) = r_2(x)$. $\therefore q_1(x)b(x) = q_2(x)b(x)$, so $q_1 = q_2$. (*Note*: $(f(x)) = (b(x))$, so $R[x]/(f(x)) = R[x]/(b(x))$.)
Next Goal: Given a field F and a nonconstant polynomial $f(x)$, construct a field K containing F containing F as a subfield, such that $f(x)$ has a root in K.
Definition: Let F be a field. A *vector space* over F is an abelian group V, written additively, and a map $F \times V \to V$ written $(c, v) \mapsto cv$ (scalar multiplication), such that $(\forall x, y \in F; v, w \in V)$:

1. $(x + y)v = xv + yv$

2. $(xy)v = x(yv)$
3. $x(v + w) = xv + xw$
4. $1v = v$

(2) and (4) give us that $F^\times$ acts on V (plus $0v = 0 \; \forall v$).

You should know: linear (in)depependence, basis, linear transformation.
An *isomorphism* of vector spaces is a bijective linear transformation.

Examples:

1. $\mathbb{C}$ is a vector space over $\mathbb{R}$ (with basis $(1, i)$).
2. $\mathbb{R}$ is a vector space over $\mathbb{Q}$
3. Any field is a vector space over itself.
4. For any field F, $F[x]$ is a vector space over F.

In particular, let F be a field and let $n \in \mathbb{Z}_{>0}$.
Then $\{a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 : a_0, \ldots, a_{n-1} \in F\} = \{p(x) \in F[x] : p(x) = 0 \vee \deg p(x) < n\}$ is a vector subspace of $F[x]$, with basis $\{1, x, x^2, \ldots, x^{n-1}\}$. Therefore it has dimension n.
By Ex. 7. 4.14, if $f(x) \in F[x]$ is monic of degree $n > 0$, then the map from $\{p(x) \in F[x] : p(x) = 0 \vee \deg p(x) < n\}$ to $F[x]/(f(x))$ given by $p(x) \mapsto \overline{p(x)}$ is an isomorphism of vector spaces (onto by (a), and injective by (b)). (So it has dimension n as a vector space over F).

Ex. 9.2.3: Let F be a field and let $f(x) \in F[x]$. Prove that $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.
Proof:
Case 1: $f(x) = 0$. Then $(f(x)) = (0)$, so $F[x]/(f(x)) \cong F[x]$ is not a field ($x \neq 0$ and x is not invertible). Also $f(x)$ is not irreducible.
Case 2: $f(x) \neq 0$. Then
$f(x)$ is irreducible $\iff$ $f(x)$ is prime (Prop. 12 p.286)
$\iff$ $(f(x))$ is a nonzero prime ideal (Def. of prime element)
$\iff$ $(f(x))$ is a maximal ideal (Prop. 7 p. 280 and max ideals are prime and (0) is not maximal in $F[x]$)l $\iff$ $F[x]/(f(x))$ is a field (Prop. 12 p. 284)

Theorem: Let F be a field and let $p(x)$ be an irreducible polynomial in $F[x]$. Then $\exists$ a field K containing an isomorphic copy of F as a subfield, in which $p(x)$ has a root. Identifying F with this subfield shows that there exists a field K, containing F as a subfield in which $p(x)$ has a root.
Proof: Let $K = F[x]/(p(x))$. This is a field. Define $\phi : F \to K$ by $F \to F[x] \to F[x]/(p(x)) = K$. Then ϕ is a ring homomorphism, and $\phi(1) = 1$, so $\ker \phi = (1)$, $\therefore \ker \phi = (0)$, so ϕ is injective, and it gives an isomoprhism from F to $\phi(F)$, which is a subfield of K.
*Next:: Show that $p(x)$ has a root in K. Let $\theta = \overline{x}$. Then $\theta \in K$, and $p(\theta) = 0$, because if $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a$ with $a_0, a_1, \ldots, a_n \in F$, then

$0 = \overline{p(x)} = \overline{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0} = \overline{a_n}\,\overline{x}^n + \overline{a_{n-1}}\,\overline{x}^{n-1} + \ldots + \overline{a_0}$ ("bar" is a ring homomorphism) $= a_n\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_0 = p(\theta)$ $(\overline{x} = \theta)$. If we identify F with a subfield of K (via ϕ), then $p(x) \in K[x]$, and $\overline{a_i} = a_i \forall i$.

Next Time: Example $F = \mathbb{R}$, $p(x) = x^2 + 1$ gives you $\mathbb{C}$.