MATH 407

5/11/18

$F[x]/\langle f \rangle$, f polynomial

$[a]^{-1}$ exists for $a \in F[x]$ iff $\gcd(a, f) = 1$
iff $[a]$ not a zero divisor

$\Phi : F \to F[x]$
$\Phi(a) =$ const poly $a_1 + 0x^1 + \dots$
Φ preserves '+', '×'
$\Phi_f : F \to F[x]/\langle f \rangle$

If F_1, F_2 fields then $\Phi : F_1 \to F_2$ is isomorphism
iff $\Phi(a+b) = \Phi(a) + \Phi(b)$
$\Phi(a \times b) = \Phi(a) \times \Phi(b)$, $\forall a, b$

$F[x]/\langle f \rangle$ is field iff f is irreducible.

$F_1 \subseteq F_2$, $(F_1, +, \times)$ is a field then F_1 is a subfield of F_2. F_2 is an extension field of F_1.

* Ex. $\mathbb{R}[x]/\langle x^2+1 \rangle$, basis $\{[1], [x]\}$
$[x^2+1] = [0] = 0$
$\Rightarrow [x]^2 + [1] = [x]^2 + 1$
so, $[x]^2 = -1$, $[x] = i$
$\Rightarrow \mathbb{R}[x]/\langle x^2+1 \rangle = \{a \cdot 1 + bi : a, b \in \mathbb{R}\}$
$= \{a + bi : a, b \in \mathbb{R}\}$
$= \mathbb{C}$

Let $f(x) \in F[x]$. Factor out all roots $(x-r_1)\dots(x-r_k)g(x)$
$g(c) \neq 0$ any $c \in F$.
g has irreducible factor p.

$F[x]/\langle p \rangle$ is extension field of F.
$p(\alpha) = 0$ if $\alpha = [x]$
$p(x) = a_0 + a_1 x^1 + \dots + a_k x^k$
$$\begin{aligned} p([x]) &= a_0 + a_1[x]^1 + \dots + a_k [x]^k \\ &= a_0 + a_1[x^1] + \dots + a_k[x^k] \\ &= [a_0 + a_1 x^1 + \dots + a_k x^k] \\ &= [p] = [0] = 0 \end{aligned}$$

$F \subseteq F[x]/\langle p \rangle$.
$g(\alpha) = 0$, since $p(\alpha) = 0$.
$f(\alpha) = 0$.

$F = F_0 \subseteq F_1 = F[x]/\langle p \rangle$
f has at least one more root $f \in F_1[x]$

By induction, $F_0 \subseteq F_1 \subseteq \dots \subseteq F_\ell$.
Process must eventually stop as degrees decrease monotonically, and f is factored completely.
(Kronecker)
Thm. If $f \in F[x]$, there is an extension field E of F s.t. $f(x) \in F[x]$ is $\prod_{i=1}^{n}(x - r_i)$, $n = \deg(f)$

Thm (Gauss) $\mathbb{C}[x]$ is s.t. every (non-const) polynomial has a root.

Thus, every f in $\mathbb{C}(x)$ is $a_n(x-r_1)\dots(x-r_n)$ where $a_n \in \mathbb{C}$, $\{r_1, \dots, r_n\} \subseteq \mathbb{C}$

⊛ Sec. 4.4: Polynomials in $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$

$f(x) \in \mathbb{Q}[x]$

$f = a_0 + a_1 x^1 + \dots + a_n x^n$

$= \frac{r_0}{s_0} + \frac{r_1}{s_1} x^1 + \dots + \frac{r_n}{s_n} x^n$, $\gcd(r_i, s_i) = 1$

$s = \operatorname{lcm}(s_0, \dots, s_n)$

$sf = r_0\left(\frac{s}{s_0}\right) + \dots + r_i\left(\frac{s}{s_i}\right)x^i + \dots + r_n\left(\frac{s}{s_n}\right)x^n$

$= b_0 + b_1 x^1 + \dots + b_i x^i + \dots + b_n x^n \in \mathbb{Z}[x]$

Thm Let $f(x) = b_0 + \dots + b_n x^n \in \mathbb{Z}[x]$

If $\alpha = \frac{r}{s}$ is a root, $\gcd(r, s) = 1$,

then $s \mid b_n$ and $r \mid b_0$

Pf. $f(\alpha) = b_0 + b_1 \frac{r^1}{s^1} + b_2 \frac{r^2}{s^2} + \dots + b_n \frac{r^n}{s^n}$

$f\left(\frac{r}{s}\right) = \frac{1}{s^n}\left(b_0 s^n + \overbrace{b_1 r s^{n-1} + \dots + b_{n-1} r^{n-1} s + b_n s^n}^{r}\right)$

$\Rightarrow s \mid b_n, \; r \mid b_0$

Ex. $f(x) = x^3 - 3x^2 + 2x - 6$

$b_3 = 1$

$b_0 = -6$

s has to be a divisor of $b_3 = \pm 1$

$r = \pm 1, \pm 2, \pm 3, \pm 6$ (divisors of $b_0 = -6$)

$f(3) = 0$ is a root

$\Rightarrow (x^2+2)(x-3)$

Cor. If $f \in \mathbb{Z}[x]$ is monic, then only integer roots in $\mathbb{Q}$