Alg-28

$f : S \to S$ is injective

then f need not be surjective

unless S is a finite set.

Ex. $f : \mathbb{N} \to \mathbb{N}$

1- $f(n) = n+1$ is injective

but not surjective.

$\text{ran } f = \{2, 3, \dots\} \subsetneq \mathbb{N}$

2 $g(n) = 2n$

R is an integral domain

$K = \text{Frac}(R)$ fraction field or quotient field of R

$= \left\{ \frac{a}{b} : a \in R,\ b \in R^* = R - \{0\} \right\}$

$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ — sum

$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bc}$ — sum

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ — product

$K = \mathrm{Frac}(R)$ is a field.

$i : R \longrightarrow K$ defined by

$i(a) = \frac{a}{1}$ is an injective ring homo.

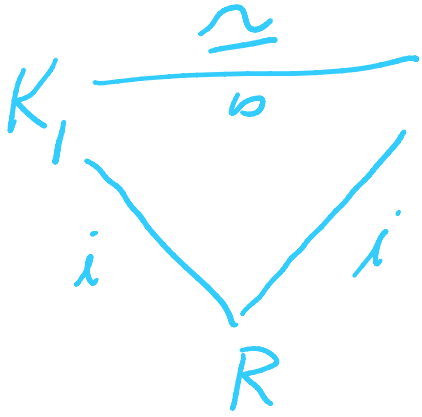
$\Rightarrow i(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i(a) + i(b)$

$\rightarrow i(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = i(a)\, i(b)$

$i(1) = \frac{1}{1} = 1.$ $\quad a \in \ker i$

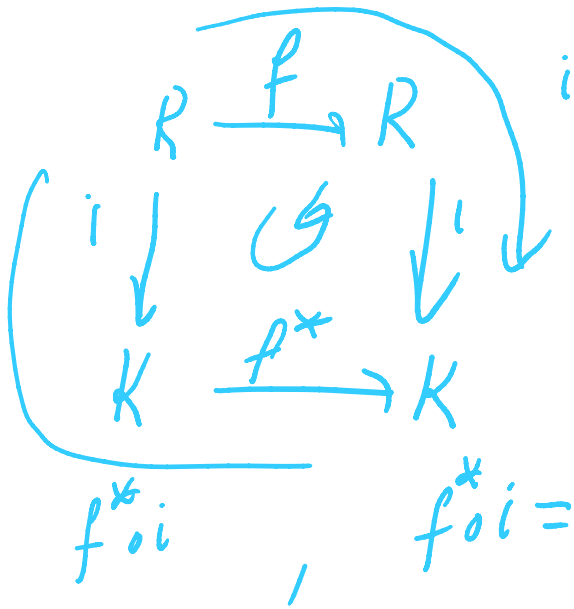
$\Rightarrow \frac{a}{1} = i(a) = \frac{a}{1} \Rightarrow a = 0$

R is embedded in K.



fraction field is unique.

FACT. $f: R \to R$ is auto of integral domain. K is its quotient field
Then $\exists!\ f^*: K \to K$ auto s.t.
$f^*(a) = f(a)\ \forall a \in R$. f^* is called
extension of f.



Polynomial functions and polynomials

$K = \mathbb{R}, \mathbb{C}(\text{or } \mathbb{Q})$, $f: \mathbb{R} \to R$

$f(t) = a_0 + a_1 t + \cdots + a_n t^n$, $a_0 \cdots a_n \in R$

$t \in R$, is called
a poly function over R.

" " H. Enderton

a poly ...

$a_n \neq 0$, is called the leading coeff of f and $n = \deg f$.

$n = 0$, $f(t)$ is a constant function $= a_0$

$n = 1$, $f(t) = a_0 + a_1 t$ — linear

$n = 2$ $f(t) = a_0 + a_1 t + a_2 t^2$ — quadratic poly

and so on.

Polynomial over a commutative ring R with identity 1.

$R[t]$, $f(t) = a_0 + a_1 t + \cdots + a_n t^n$

where $t \notin R$, t is called "indeterminate". $f(t)$ is called a poly with coeffs $a_0, \ldots, a_n \in R$.

$a_n \neq 0$, $n = \deg f(t)$

↑ the leading coeff.

More precisely:

$$Pol_R = \{ f : \mathbb{N} \cup \{0\} \longrightarrow R \text{ s.t. } f(n) \neq 0 \text{ for finitely many } n. \}$$

$$\{ \operatorname{supp} f \text{ is finite} \}$$

$$f = (a_0, a_1, \dots a_n, 0 - - - - 0)$$

$$g = (b_0, b_1, \dots b_m, - - - - 0)$$

$$f+g \overset{\text{def}}{=} (a_0+b_0, a_1+b_1, \dots - - -$$

$$fg = (c_0, c_1, \dots, c_k, \dots, 0 - - - 0)$$

$$c_0 = a_0 b_0, \quad c_1 = a_0 b_1 + a_1 b_0$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

$$\vdots$$

$$c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_{k-1} b_1 + a_k b_0$$

$$= \sum_{i+j=k} a_i b_j$$

$$= \sum_{i+j=k} (\quad)$$

$(Pol_R, +, \cdot)$ is a commutative ring with identity.

$$0_{Pol_R} = (0, 0, \ldots 0, \ldots) \qquad 0 : \mathbb{N} \cup \{0\} \to R$$

$$1_{Pol_R} = (1, 0, \ldots 0, \ldots)$$

$$f \cdot 1 = f = f \cdot f.$$

$t : \mathbb{N} \cup \{0\} \to R.$

$t(0) = 0, \quad t(1) = 1, \quad t(n) = 0 \ \forall\ n \geq 2$

$t = (0, 1, 0, \ldots 0, \ldots) \in Pol_R.$

$t^2 = (0, 0, 1, 0, \ldots 0, \ldots)$

$t^3 = (0, 0, 0, 1, 0, \ldots 0, \ldots)$

$$t^n = (\underbrace{0,0,\ldots,0}_{n},1,0,\ldots,0)$$

$$f = (a_0, a_1, a_2, \ldots, a_n, 0, \ldots, 0)$$

$$= a_0(1,0,\ldots,0,\ldots) + a_1(0,1,0,\ldots,0) + a_2(0,0,1,\ldots,\ldots)$$

$$\vdots$$

$$+ a_n(\underbrace{0,\ldots,0}_{n},1,0,\ldots,0)$$

$$+ \cdots$$

$$f = (a_0, a_1, a_2, \ldots, a_n, 0, \ldots, 0)$$

$$= a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + 0 \cdots 0$$

$$= a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$$

$$Pol_R = R[t] \qquad t = (0,1,0,\ldots,0)$$

$$f = t.$$

Let R be a subring of a commutative

Let K be a subring of ring S. $f \in R[t]$

Define a map $f_S : S \to S$

by $f_S(x) = f(x) = a_0 + a_1 x + \cdots + a_n x^n \in S$

for $x \in S$

where $f = a_0 + a_1 t + \cdots + a_n t^n$, $a_0, \ldots, a_n \in R$

f_S is a function.

For $c \in S$, define

$ev_c : R[t] \to S$ by

$ev_c(f) = f(c) = f_S(c)$. Then ev_c is a ring homo, called the evaluation map or homo. It need not be injective: $ev_c(f) = 0 = f(c)$

$\not\Rightarrow$ f is the 3rd bday.

Ex $\alpha = \sqrt{2}$, $R = \mathbb{Z}$,

$\mathbb{Z}[t] \longrightarrow \mathbb{R}$

$ev_\alpha(f) = f(\alpha)$. $im(ev_\alpha) = \mathbb{Z}[\alpha]$

$= q_0 + q_1\alpha + \cdots + q_n\alpha^n$

$q_0 \cdots q_n \in \mathbb{Z}$

called the ring generated by α & $\mathbb{Z}$

& $\mathbb{Z}[\alpha]$ is a subring of $\mathbb{R}$

R subring of S, a commutative ring !

$x \in S$, $ev_x : R[t] \longrightarrow R$

$ev_x(f) = f(x)$

$im(ev_x)$ is a subring of S

$\| \; R[x]$, and is called the subring of S generated by R and x.

$\mathbb{Z}[\alpha] = \{ a + b\alpha : a, b \in \mathbb{Z} \}$

$\rightarrow \mathbb{Z}[i] = \{ a + bi : a, b \in \mathbb{Z} \}$ — the ... of

$\mathbb{Z}[i] = \{ a+bi : a, b \in \mathbb{Z} \}$ — the ring of Gaussian integers

$\mathbb{Z}[\sqrt{-5}] = \{ a+b\sqrt{-5} : a, b \in \mathbb{Z} \}$

$\mathbb{Z}[\alpha]$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-5}]$ are integral domains $\mathbb{Z}[\sqrt{-5}]$ is not a UFD (unique factorization domain)

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

are irreducible in $\mathbb{Z}[\sqrt{-5}]$

$ev_\alpha : \mathbb{Z}[t] \longrightarrow \mathbb{R}$

PID (Principal ideal domain) R is an integral domain & I is an ideal of R, then

If R, then $R = (a)$, simply generated principal ideal

Thm R is a PID $\Rightarrow R[t]$ is a PID

$\mathbb{R}[t]$, $\mathbb{C}[t]$, $\mathbb{Q}[t]$

$\mathbb{R}$: real; $\mathbb{C}$: complex; $\mathbb{Q}$: rational

R is a commutative ring with 1

J is an ideal of R. If $1 \in J$

$\Rightarrow J = R = (1)$

$a \in R \quad a = 1 \cdot a \in J$

$\top - D$

$a \in K \quad a = 1 \cdot a \in J$

$R \subseteq J \subseteq R \Rightarrow J = R$

$ev_\alpha : \mathbb{Z}[t] \longrightarrow R$

$ev_\alpha(f) = f(\alpha)$ is a ring homo $\ker(ev_\alpha) = I$ is an ideal of $\mathbb{Z}[t]$

$f \in \ker(ev_\alpha) \Rightarrow f(\alpha) = 0$

$I = (t^2 - 2) = \{ g(t)(t^2-2) \quad \alpha = \sqrt{2}$

$t^2 - 2 \in \ker(ev_\alpha)$

$ev_\alpha(t^2 - 2) = (\alpha^2 - 2) = f(\alpha)$

$= 2 - 2$

$= 0$

Ex p prime $\mathbb{F} = K = \mathbb{Z}/p\mathbb{Z}$ is a field $\Rightarrow K^* = \mathbb{Z}/p\mathbb{Z} - \{0\}$ is a group with $p-1$ elements

$\rightarrow$ Lagrange's

$a \in \mathbb{Z}/p\mathbb{Z} - \{0\}$

$a^{p-1} = 1 \pmod p$

So $a^p = a \pmod p$

$f(t) = t^p$, $f(t), g(t) \in \mathbb{Z}_p[t]$

$g(t) = t$

$f(t) \neq g(t)$ as $\deg f(t) = p$

$\deg g(t) = 1$

Claim $f(a) = g(a) \quad \forall a \in \mathbb{Z}_p$

$a = 0 \quad 0^p = 0 = g(a)$ $\mathbb{Z}/p\mathbb{Z}$.

$a \in \mathbb{Z}_p - \{0\}$ $a^p = a \pmod p$

$f(a) = g(a)$.

$f(t) = t^p$, $g(t) = t$ are not equal poly but functions $f, g : \mathbb{Z}_p \to \mathbb{Z}_p$

equal as functions $f, g: \mathbb{F}_p \to \mathbb{F}_p$
they are equal.

K is a field, $f(t) = f \in K[t]$

Def. $\alpha \in K$ is a root or zero of $f(t)$ iff $f(\alpha) = 0$.

$Z(f)$ = the set of roots of f in K.

The zero set $Z(f)$ may be empty. Ex $f(t) = t^2 + 1 \in \mathbb{R}[t]$

Then $Z(f) = \emptyset$

Thm Euclidean Algorithm.
$f(t), g(t) \in K[t] - \{0\}$ non-zero polynomials with coeff in K, a field. Then there are unique $q(t)$ and $r(t)$ poly in $K[t]$ s.t. $f(t) = q(t)\, g(t) + r(t)$,
where $r = 0$ or $\deg r(t) < \deg g(t)$

where $0 \le \deg r(t) < \deg g(t)$

or $r(t)$ is the zero poly

$g(t)$ is called the quotient and

$r(t)$ is called the remainder.

Note. The deg of the zero poly is not defined.

Cor $\alpha \in K$ is a root of $f(t) \in K[t]$

$\iff$ $t-\alpha$ divides $f(t)$ ie.

$f(t) = g(t)(t-\alpha)$ for some $g(t) \in K[t]$

$\Longrightarrow$ Assume $f(\alpha) = 0$.

Using Euclidean alg with $g(t) = t-\alpha$, we get

$$\boxed{f(t) = g(t)(t-\alpha) + r(t)}$$

where $r(t), g(t) \in K[t]$

and $0 \le \deg r(t) < \deg(t-\alpha)$

//

and $\deg r(t) < 1$

$\deg r(t) < 1$

$\Rightarrow \deg r(t) = 0, \quad r(t) = a_0, a_0 \in K$

↑ const poly

Now $0 = f(\alpha) = g(\alpha)(\alpha - \alpha) + r(\alpha)$

$= 0 + r(\alpha)$

$0 = r(\alpha) = a_0$

$\Rightarrow (t-\alpha) g(t) = f(t)$

that is $t-\alpha$ divides $f(t)$!

Conversely, suppose $f(t) = (t-\alpha) g(t)$ for some $g(t) \in K[t]$

then $f(\alpha) = (\alpha - \alpha) g(\alpha) = 0$

i.e. α is a root of f

Thm (Rational root thm)

$f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{Z}[t]$

$f(t) = a_0 + a_1 t \cdots + a_n t^n$

$a_0, \ldots a_n \in \mathbb{Z}$, $a_n \neq 0$

If $r = \frac{c}{d} \in \mathbb{Q}$, $(c,d) = 1$,

then $c \mid a_n$ & $d \mid a_0$

Cor $f(t) \in \mathbb{Z}[t]$ is monic poly

i.e. $a_n = 1$, then $f(t)$ has no rational root.

Proof $f(t) = a_0 + a_1 t \cdots + a_{n-1} t^{n-1} + t^n$, $n \geq 1$

If $r = \frac{a}{b}$, $(a,b) = 1$ is a root of $f(t)$, then $a \mid 1$ & $b \mid a_0$

$a = 1, -1$, not possible.

Ex $f(t) = t^2 - 2$ has no rational root.

$r = \frac{a}{b}$, $(a,b) = 1$.

$a^2 - 2 = 0 \Rightarrow a^2 = 2b^2$

$$\frac{a^2}{b^2} - 2 = 0 \Rightarrow a^2 = 2b^2$$

$$2 \mid 2b^2 = a^2$$

$$2 \mid a \Rightarrow$$

$$a = 2m$$

$$2b^2 = a^2 = 4m^2$$

$$b^2 = 2m^2, \quad 2 \mid b^2$$

$$2 \mid b$$

2 is a common factor of a & b

FACT K is a field. G is a finite subgroup of $K^* = K - \{0\}$.
Then G is cyclic.

Cor $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ is a cyclic group.

$\Gamma = \Gamma$ is a finite field

Ex F is a finite field.
Then the product of nonzero elements of F must be -1.

$a_0 = 0, a_1 \ldots a_{d-1} \in F^*$, $|F| = d$

Then $a_1 a_2 \cdots a_{d-1} = -1$

$(p-1)! = -1 \bmod p$ Wilson's Thm.

$\mathbb{Z}_p$, $[1][2]\cdots[p-1] = [-1]$

$[1\,2\cdots p-1] = [-1]$

$(p-1)! = -1 \bmod p$.

↑ prime

p is prime $\Rightarrow p \mid 1 + (p-1)!$

K is a field.
$K[t]$ is a commutative ring with 1

$1 = 1 + 0t + 0t^2 \cdots$

$U(K[t]^*) = K^*$

$U(K[t]) = ?$

R is a commutative ring with 1

$U(R^*) = \{a \in R^* : \exists b \in R^* \text{ s.t. } ab = 1 = ba\}$

is a subring of R, called the ring of units.

$f(t) = a_0 + \cdots + a_n t^n$

$g(t) = b_0 + \cdots + b_m t^m$

$f(t) \cdot g(t) = 1$. then $a_0 b_0 = 1$

$f \in U(K[t]^*) = K^*$

Thm $J \subseteq K[t]$ ideal of $K[t]$

(1) if J is the zero ideal, then $J = (0)$

(2) If J is a nonzero ideal of $K[t]$, then $J = (f(t))$ where $f(t)$ is a poly in J of smallest

degree.

Thm $f_1 \ldots f_m \in K[t]$, not all are zero

$J = (f_1 \ldots f_m)$, the ideal generated by $f_1 \ldots f_m$.

$$= \{g_1 f_1 + \ldots + g_m f_m,\ g_1 \ldots g_m \in K[t]\}$$

Then $J = (g)$, g is the gcd of $f_1 \ldots f_m$.

Def. g is a greatest common divisor of $f_1 \ldots f_m$ iff

(i) $g \mid f_i$ for $i = 1 \ldots m$

(ii) if $h \mid f_i$, $\forall i$, then $h \mid g$