R - ring (commutative, as usual)

There is a homomorphism $\mathbb{Z} \xrightarrow{\varphi} R$ $\varphi(n)=n$ viewed as element of R

$1 \longmapsto 1$

$n \longmapsto n$ $n = \underbrace{1+1+\dots+1}_{\text{sum in } R}$ $n>0$

Possibilities for $\mathrm{im}(\varphi)$ - subring. $-n = -\underbrace{(1+\dots+1)}_{\text{sum in } R.}$

(a) φ is injective. Then $\varphi(\mathbb{Z}) \simeq \mathbb{Z}$, $\ker\varphi = 0$.

$\Rightarrow R$ contains $\mathbb{Z}$ as subring. Examples: $\mathbb{Z}, \mathbb{Z}[\frac{1}{n}], \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[x], \dots$

(b) φ is not injective. $\ker(\varphi) \neq 0$. Since $\mathbb{Z}$ is a PID, any ideal is principal, $\ker(\varphi) = (n)$, $n>0$. $(n) = (-n)$

Then $\mathrm{im}(\varphi) \simeq \mathbb{Z}/\ker(\varphi) \simeq \mathbb{Z}/(n)$. $n=0$ in case (a)

The image of $\mathbb{Z}$ in R is a finite ring of residues modulo n

$0, 1, \dots, n-1$, $n=0$ in R. Example: $R = \mathbb{Z}/(n)$, $\mathbb{Z}/n[x] \dots$

Any ring R contains either $\mathbb{Z}$ or $\mathbb{Z}/n$, for a unique n, as a subring

Assume R is a field, $R = F$

$\Rightarrow n=0$ or $n=p$ prime above — zero divisors if $n = km$

$n=0 \Rightarrow F \supset \mathbb{Z}$, even $F \supset \mathbb{Q}$ as subfield $\mathbb{Q} \subset F$

$n=p$ $\mathbb{F}_p = \{0, \dots, p-1\}$ field of residues mod p, $\mathbb{F}_p = \mathbb{Z}/p$ another notation

<u>Example</u> F field $F[x]$ - polynomials in F, $\mathrm{Frac}(F[x])$ - field of rational functions in x, coefficients in F.

$F(x) = \mathrm{Frac}(F[x])$ elements $\dfrac{f(x)}{g(x)}$, $f(x), g(x) \in F[x]$, $g(x) \neq 0$.

+ equivalence relation, $\dfrac{f(x)r(x)}{g(x)r(x)} = \dfrac{f(x)}{g(x)}$ $r(x) \neq 0$.

Prop If integral domain R is a subring of field F, there is a homomorphism $\mathrm{Frac}(R) \longrightarrow F$ that extends the inclusion

$$\begin{tikzcd} R \arrow[r, "\alpha"] \arrow[d, hook, "i"'] & F \\ \mathrm{Frac}(R) \arrow[ur, dashed, "\beta"'] & \end{tikzcd}$$

$\alpha = \beta i$

such β is unique

How to define β? Elements of $\mathrm{Frac}(R)$ are pairs (a,b), $b \neq 0$, $a, b \in R$ modulo equivalence relation. (a/b).

Define $\beta(ab^{-1}) = \alpha(a)\,\alpha(b)^{-1}$

Exercise: this is well-defined on cosets $(a,b) \sim (c,d)$ if $ad = bc$ in R

Exercise: 1) β is a ring homomorphism.

2) why is β unique? why is β injective?

Proposition says that any inclusion of an integral domain R into a field F extends to an inclusion of the ring of fractions $\mathrm{Frac}(R) = Q(R) \subset F$.

Example $\mathbb{Z} \subset F \iff \mathbb{Q} \subset F$ $\quad \mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$

Corollary Each field F either contains subfield $\mathbb{Q}$ or $\mathbb{F}_p$

$\mathbb{Q}$, $\mathbb{F}_p$ are called prime fields.

if $\mathbb{F}_p \subset F$, say that characteristic of F is p, $\mathrm{char}(F) = p$

if $\mathbb{Q} \subset F$, say that characteristic of F is 0, $\mathrm{char}(F) = 0$

Exercise a) if integral domain R is a subring of a field F, $R \subset F$, then the smallest subfield of F that contains R is isomorphic to $Q(R) = \mathrm{Frac}(R)$

b) Take a collection of elements $\{a_i\}_{i \in I}$ in a field F. Show that there exists the smallest subfield of F that contains all a_i (think how to define it).

F-field, $F[x]$

division with a remainder. Given polynomials $f(x), g(x) \in F[x]$, $g(x) \neq 0$ there exist unique polynomials

$$f(x) = q(x) g(x) + r(x), \quad \deg r(x) < \deg g(x).$$

$\deg f(x) = n$
$\deg g(x) = m$

To construct $q(x), r(x)$ we divide $f(x)$ by $g(x)$ with a remainder.

By induction on $\deg f(x)$.

If $\deg f(x) < \deg g(x)$ $(n < m)$ done: $f(x) = 0 \cdot g(x) + f(x)$
$r(x) = f(x)$

If $n \geq m$ $\quad f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \quad a_n \neq 0$
$\quad g(x) = b_m x^m + \ldots + b_0 \quad b_m \neq 0$

$a_n b_m^{-1} g(x) = a_n b_m^{-1} (b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0) = a_n x^m + a_n b_m^{-1} b_{m-1} x^{m-1} + \ldots$

b_m^{-1} ← can invert in F, important that F is a field. lower order terms

$f(x) - a_n b_m^{-1} g(x) \cdot x^{n-m} = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 - (a_n x^m x^{n-m} + a_n b_m^{-1} b_{m-1} x^{n-1} + \ldots)$

$a_n x^m x^{n-m} = a_n x^n$

$= (a_{n-1} - a_n b_m^{-1} b_{m-1}) x^{n-1} + \ldots$

$f(x) - (a_n b_m^{-1} x^{n-m}) g(x)$ has degree $\leq n-1$. Proceed by induction.

This proves existence of $q(x)$, $r(x)$ as above

<u>Uniqueness</u> $f(x) = q_1(x) g(x) + r_1(x)$, $f(x) = q_2(x) g(x) + r_2(x) \Rightarrow$

$$q_1(x) g(x) + r_1(x) = q_2(x) g(x) + r_2(x)$$

$$(q_1(x) - q_2(x)) g(x) = r_2(x) - r_1(x)$$

↑ unless $q_1 = q_2$, deg of LHS is $\geq \deg g(x) = m$

↖ degree $< \deg g(x) = m$

Contradiction with degrees.

Division of polynomials with a remainder

Example over $\mathbb{F}_3 = \{0,1,2\}$ mod 3 $\qquad 2+1=0, \ldots \qquad 2+2=1$

$f(x) = x^5+x^4+2x^2+x \qquad g(x) = x^2+2x-1$

$2=-1 \mod 3$

personal preference 2 or -1

$$
\begin{array}{r|l}
 & x^3 + 2x^2 + 1 \\
\hline
x^2 - x - 1 & x^5 + x^4 + 0\cdot x^3 + 2x^2 + x \\
 & -\;(x^5 - x^4 - x^3) \\
\hline
 & 2x^4 + x^3 + 2x^2 + x \\
 & -\;(2x^4 - 2x^3 - 2x^2) \\
\hline
 & 0\cdot x^4 + 0\cdot x^3 + \cancel{4}x^2 + x \\
 & -\;(x^2 - x - 1) \\
\hline
 & 2x+1
\end{array}
$$

$4 = 1 \pmod 3$

$$\underbrace{x^5+x^4+2x^2+x}_{f(x)} = \underbrace{(x^3+2x^2+1)}_{q(x)}\underbrace{(x^2-x-1)}_{g(x)} + \underbrace{2x+1}_{r(x)}$$

If g is monic (highest coefficient is 1), can divide by $g(x)$ even over $R[x]$, R a ring. If g is not monic, need top coefficient of g to be invertible in R

$\mathbb{Z}[x]$. Can we divide $f(x) = x^2-1$ by $g(x) = 2x+1$?

$$
\begin{array}{r|l}
 & \tfrac{1}{2}x + \ldots \\
\hline
2x+1 & x^2 - 1
\end{array}
$$

$\frac{1}{2}$ is not in $\mathbb{Z}$ $\quad$ cannot put $\frac{1}{2}x$ there.

For this reason, restrict to a field F and polynomials in $F[x]$.

Thm $F[x]$ is a principal ideal domain (PID), for a field F.

Proof Take an ideal $I \subset F[x]$. If $I = (0)$, it is principal. $I = \{0\}$ or $I = (0)$.

If $I \neq (0)$, choose a polynomial $m(x) \in I$ of the smallest degree.

$(m(x)) \subset I$. Assume the inclusion is proper take $f(x) \in I \setminus (m(x))$.
$\uparrow$ ideal generated by $m(x)$.

Divide $f(x)$ by $m(x)$ with a remainder.

$$f(x) = q(x)m(x) + r(x) \quad , \deg r(x) < \deg m(x) \quad \text{or } r(x) = 0.$$

$$\deg 0 = -\infty.$$

$r(x) \in I$ since $r(x) = \underset{\overset{\cap}{I}}{f(x)} - q(x)\underset{\overset{\cap}{I}}{m(x)}$.

Contradiction with choice of $m(x)$. (least degree in I)

Corollary Any ideal in $F[x]$ has the form $(m(x))$ or (0), where $m(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ is a monic polynomial.

Exercise: For different monic polynomials $m_1(x), m_2(x)$ ideals $(m_1(x))$, $(m_2(x))$ are distinct.

<u>Divisibility</u> $r, s \in R$ say r divides s, $r \mid s$ if $\exists\, r' \in r$ $rr' = s$

$r \mid s \iff s \in (r)$ -principal ideal. generated by r.

$r \mid 0$ $\forall r \in R$, $0 \mid r$ iff $r = 0$, r unit (invertible) iff $r \mid 1$

<u>Def</u>

F field, $f(x), g(x) \in F[x]$. The gcd (greatest common divisor) of $f(x), g(x)$ is a polynomial $d(x)$ s.t.

(1) $d \mid f$, $d \mid g$

(2) if $c \mid f$, $c \mid g \Rightarrow c \mid d$ $\qquad d = (f, g)$

(3) d is monic

Say that f, g are relatively prime if $(f, g) = 1$

gcd is unique: if d, d' are gcds

$d \mid d'$, $d' \mid d$, $F[x]$ is a domain $\Rightarrow d, d'$ differ by a unit (see homework)

$(F[x])^* = F^*$

<u>Thm</u> gcd exists.

<u>Proof</u> Consider ideal $I = (f(x), g(x)) = \{a \cdot f + b \cdot g \mid a(x), b(x) \in F[x]\}$

Ideal I is principal ($F[X]$ is a PID), $I = (d(x))$

we can choose monic $d(x)$, unless $I = (0) \Rightarrow f(x) = g(x) = 0$.

$\Rightarrow f(x) = d(x) h(x)$, $d \mid f$, $d \mid g$

if $c \mid f$, $c \mid g \Rightarrow f = cc'$, $g = cc''$ $\qquad d = af + bg = acc' + bcc'' = c(ac' + bc'')$

$\Rightarrow c \mid d$.

Lemma (Euclid) Let F be a field, $p(x) \in F[x]$ not a product of polynomials of smaller degree. If $p(x) \mid q_1(x) \dots q_n(x)$ then $p(x) \mid q_j(x)$ for some j.

$$\underbrace{p(x)}_{f(x)} \quad \underbrace{q_1(x)}_{g(x)} \underbrace{q_2(x) \dots q_n(x)}_{h(x)}$$

Proof Induction on $n \geq 2$

Show that if $(f(x), g(x)) = 1$ and $f \mid gh$ then $f \mid h$

$1 = a(x) f(x) + b(x) g(x)$ some a, b.

$h(x) = a(x) f(x) h(x) + b(x) g(x) h(x)$

$h = afh + b\underbrace{gh}$, $f \mid gh$, $gh = fk \Rightarrow$

$h = afh + bfk = (ah + bk) f \quad \Rightarrow f \mid h$

$\gcd(p(x), q_1(x)) =$ either 1 or $p(x)$ ← up to element of $F^{\times}$, to rescale to monic

if $p(x)$, $p(x) \mid q_1(x)$ done.

To get gcd, $(f(x), g(x))$ ideal → $d(x)$ monic generator of ideal

$(f(x), g(x)) = (f(x)) + (g(x))$ sum of ideals.

Exercise I, J ideals in $R \Rightarrow I + J = \{ i + j \mid i \in I, j \in J \}$ are ideals in R
$I \cap J$

$$\underset{f(x), g(x)}{\text{polynomials}} \longrightarrow \underset{(f(x)), (g(x))}{\text{principal ideals}} \longrightarrow \underset{(f(x)) + (g(x)) = (f(x), g(x))}{\text{sum of ideal}} \longrightarrow \underset{(d(x)) \uparrow \text{monic}}{\text{generator of sum}}$$

$a_n x^n + \dots + a_0 = a_n (x^n + a_{n-1} a_n^{-1} x^{n-1} + \dots + a_0 a_n^{-1})$

$a_n \in F^{\times}$; monic

rescaling monic polynomials by elements of $F^{\times}$ gets all nonzero polynomials

To compute $\gcd(f, g)$, repeatedly divide with a remainder

let $\deg f \geq \deg g$.

$$f = q_1 g + \underset{\text{remainder}}{r_1} \qquad \deg(r_1) < \deg(g)$$

$$g = q_2 r_1 + \underset{\text{remainder}}{r_2} \qquad \deg(r_2) < \deg(r_1)$$

$$r_1 = q_3 r_2 + r_3 \qquad \deg(r_3) < \deg(r_2)$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$

$$r_n = q_{n+2} r_{n+1}$$

no remainder, **done**

before (f, g) ← bigger deg

now (g, r_1) ← bigger deg

Exercise: (f, g) and (g, r_1) have the same gcd

	remainder
(f, g)	r_1
(g, r_1)	r_2
(r_1, r_2)	r_3
$\vdots$	
(r_n, r_{n+1})	0.

r_{n+1} ↑ **gcd**

Example 1) $F = \mathbb{Z}/3 = \mathbb{F}_3$

$f(x) = x^3 + 2x^2 + 2x + 1$, $g(x) = x^2 - x + 1$. Find $\gcd(f(x), g(x))$

	remainder
$(x^3+2x^2+2x+1,\ x^2-x+1)$	$x+1$
$(x^2-x+1,\ x+1)$	0

$$
\begin{array}{r|l}
 & x \\
\hline
x^2-x+1 & x^3+2x^2+2x+1 \\
 & -\ x^3-x^2+x \\
\hline
 & \cancel{3x^2}+x+1 \quad 3=0
\end{array}
$$

$\gcd(f(x), g(x)) = x+1$

monic ✓

$$
\begin{array}{r|l}
 & x+1 \\
\hline
x+1 & x^2-x+1 \\
 & -\ x^2+x \\
\hline
 & -2x+1 \\
 & \ \ \shortparallel \\
 & x+1 \\
 & -\ x+1 \\
\hline
 & 0
\end{array}
$$

2) $F = \mathbb{F}_2 = \{0, 1\}$

$f(x) = x^4 + x^2$, $g(x) = x^3 + x^2 + 1$

	remainder
$(x^4+x^2,\ x^3+x^2+1)$	x^2+1
$(x^3+x^2+1,\ x^2+1)$	x
$(x^2+1,\ x)$	1

↑

$\gcd(f(x), g(x)) = 1$

f, g are relatively prime.

$$
\begin{array}{r|l}
 & x+1 \\
\hline
x^3+x^2+1 & x^4 \quad\quad +x^2 \\
 & -\ x^4+x^3+x^2 \\
\hline
 & x^3 \\
 & -\ x^3+x^2+1 \\
\hline
 & x^2+1
\end{array}
$$

$$
\begin{array}{r|l}
 & x+1 \\
\hline
x^2+1 & x^3+x^2 \quad +1 \\
 & -\ x^3 \quad\quad +x \\
\hline
 & x^2+x+1 \\
 & -\ x^2 \quad\quad +1 \\
\hline
 & x
\end{array}
$$

Prop (long division with remainder) Let $f \in F[x]$, $f \neq 0$, $g \in F[x]$. Then there exist unique polynomials $q, r \in F[x]$, with either $r = 0$ or $\deg r < \deg f$ such that

(or declare $\deg 0 = -\infty$)

$$g = qf + r$$

Corollary Let $f \in F[x]$, $f \neq 0$. Then every coset $g + (f)$ has a unique representative $r = 0$ or $\deg r < \deg f$

Proof write $g = f \cdot q + \overset{\text{remainder}}{r}$ $r = 0$ or $\deg r < \deg f$

$r - g = fq \in (f)$

$r \in g + (f)$ coset, since $r - g \in (f)$

such r is ✓unique: if $r_1 + (f) = r_2 + (f)$ $\Rightarrow r_1 - r_2 \in (f)$, but $\deg r_1 < \deg f$, $\deg r_2 < \deg f$

$\Downarrow$

$\deg(r_1 - r_2) < \deg f \Rightarrow r_1 = r_2$.

$\deg f = n$

Cosets of (f): represented by 0 and all polynomials of degree $< n$

Example $\deg f = 2$ quadratic polyn. $f(x) = b_2 x^2 + b_1 x + b_0$ $b_2 \neq 0$

cosets $F[x]/(f)$ have the form $a_0 + a_1 x + (f)$ for all pairs (a_0, a_1), $a_i \in F$, $i = 0, 1$.

take $\{1, x\}$ and form all 'linear combinations' $a_0 \cdot 1 + a_1 x$

$\deg f = 3$ cubic polyn $f = b_3 x^3 + \dots + b_0$ $b_3 \neq 0$

cosets $F[x]/(f)$ $a_0 + a_1 x + a_2 x^2 + (f)$

'basis' $1, x, x^2$ cosets are parametrized by (a_0, a_1, a_2) $a_i \in F$.

this if $\{a_0+a_1x+ \quad +a_{n-1}x^{n-1}\}$ $\deg f = n$

as $\underbrace{\text{'residues'}}_{\text{all possible}}$ modulo f. These are exactly elements of

$F[x]/(f(x))$

$\underline{\text{Example}}$. 1) $F=\mathbb{Q}$, $f(x)=x^2+x+1$.

$R=\mathbb{Q}[x]/(x^2+x+1)$ elements are polynomials of deg at most 1

$a_0+a_1x \qquad a_0,a_1\in\mathbb{Q}$

To multiply in R, multiply as polynomials, then take a remainder for division by x^2+x+1

divide by x^2+x+1

$$(2+x)(1-3x)=\underbrace{2-5x}_{\text{ok}}-\underset{\substack{\uparrow\\ \text{need to reduce}}}{3x^2}=2-5x-3(-x-1)=2-5x+3x+3=$$
$$=-2x+5$$

$x^2=-x-1$ in the quotient ring

$2+x+(f(x))$

$1-3x+(f(x))$

$(2+x)(1-3x)=-2x+5$ in $\mathbb{Q}[x]/(x^2+x+1)$.

$x\cdot x=x^2=-x-1$ in R/I

$$\begin{array}{r|l} & -3 \\ \hline x^2+x+1 & -3x^2-5x+2 \\ + & 3x^2+3x+3 \\ \hline & 0 \quad -2x+5 \end{array}$$

2) $F=\mathbb{F}_2$ $\{0,1\}$

$f(x)=x^2+x+1$

$R=\mathbb{F}_2[x]/(x^2+x+1)$ $\qquad 0,1,x,x+1$ 4 elements.

$x(x+1)=x^2+x=-1=1 \pmod 2$

$x+1=x^{-1}$ in R.

$(x+1)^{-1}=x$

Each nonzero element is invertible!

This is a field with four elements

$\mathbb{F}_4\simeq\mathbb{F}_2[x]/(x^2+x+1)$

Divide by linear polynomial $x-a$.

$f(x) \in F[x]$ $\qquad f = (x-a)g + c$ ← remainder, a 'constant'

evaluate $\qquad ev_a : F[x] \longrightarrow F \qquad f(x) \longmapsto f(a)$

$\qquad\qquad x \longmapsto a \qquad (x-a)g(x)+c \longmapsto (a-a)g(a)+c =$

$\Rightarrow f(a) = c \qquad\qquad = 0 \cdot g(a) + c = c$

$f(x) = (x-a)g(x) + f(a)$

when $f(x)$ is divided by $(x-a)$, the remainder is $f(a)$

$F[x]/(x-a)$ cosets are $b \in F$. constant polynomials

$F[x]/(x-a) \simeq F$ as rings

$h(x) + (x-a) \longmapsto h(a)$ bijection, respect ring structure

$b + (x-a) \longleftarrow b$

$\mathbb{R}[x]/(x-3) \simeq \mathbb{R}$ isomorphism

$2 \longmapsto 2$

$10 \longmapsto 10$

$x \longmapsto 3$

$\vdots$

Comparison

$\mathbb{Z}$ | $F[x]$ F a field

Both are PIDs

$\mathbb{Z}^* = \{1, -1\}$ invertible (unit) elements $(F[x])^* = F^*$

$n \longleftrightarrow -n$ same principal ideal $(n) = (-n)$ positive number

$f(x) \longleftrightarrow a f(x)$ $a \in F^*$ nonzero 'constant' monic polynomial

$n = mk$ factorization $f = gh$ $f(x) = g(x)h(x)$

prime p
$2, 3, 5, 7, 11, 13 \ldots$

monic irreducible polynomial
$f(x) = a^n + \ldots$

$\{\pm 1\}$ are not primes (invertible elements)

$a \in F^*$ are not irreducible polynomials (unit (invertible elements))

$n = p_1 \ldots p_k$
prime factorization. p_i - primes

monic
$f(x) = p_1(x) \ldots p_k(x)$
monic irreducible polynomials

$-n = (-1)\, p_1 \ldots p_k$
unit primes

$f(x) = a_n \cdot p_1(x) \ldots p_k(x)$
monic irreducible

$\gcd(n, m)$ $\gcd(f, g)$

$\operatorname{lcm}(n, m)$ $\operatorname{lcm}(f, g)$

coprime n, m
$1 = an + bm$ some a, b

coprime $f(x), g(x)$
$1 = a(x)f(x) + b(x)g(x)$ some $a(x), b(x)$