Lecture 3

Homomorphism and isomorphism (3.3):

Def: R, S rings. The function $f: R \to S$ is a *homomorphism* if

(i) $f(a+b) = f(a) + f(b)$ for all $a, b \in R$

(ii) $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in R$

Ex: The function $f: \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(a) = [a]$ is a homom.:

$$f(a+b) = [a+b] \overset{\uparrow}{=} [a] + [b] = f(a) + f(b)$$
$$f(a \cdot b) = [a \cdot b] \overset{\uparrow}{=} [a] \cdot [b] = f(a) \cdot f(b)$$

$\uparrow$ def. of add. and mult. in $\mathbb{Z}_n$.

Homomorphisms preserves structures of rings:

> **Theorem:** Let R, S be rings and $f: R \to S$ a homomorphism.
>
> 1. $f(0_R) = 0_S$
> 2. $f(-a) = -f(a)$ for all $a \in R$
> 3. A subring of $R \Rightarrow f(A)$ subring of S
>
> **Note:** $f(A) = \{ s \in S \mid s = f(r) \text{ for some } r \in A \}$

Proof: ①: $0_S + \cancel{f(0_R)} = f(0_R) = f(0_R + 0_R) \underset{\text{hom.}}{=} f(0_R) + \cancel{f(0_R)}$

$\overset{\text{cancellation}}{\Rightarrow} f(0_R) = 0_S$

②: $f(a) + f(-a) \underset{\text{hom.}}{=} f(a + (-a)) = f(0_R) \underset{①}{=} 0_S$

$\underset{\text{def.}}{\Rightarrow} f(-a) = -f(a)$

③: Clearly $f(A) \neq \emptyset$. Show that $a, b \in f(A) \Rightarrow \begin{cases} a-b \in f(A) \\ ab \in f(A) \end{cases}$.

We have $a = f(u)$, $b = f(v)$ for some $u, v \in A$.

- $a - b = f(u) - f(v) = f(u) + (-f(v)) \underset{②}{=} f(u) + f(-v) = \underset{\text{hom.}}{=} f(\underbrace{u + (-v)}_{\in A}) \in f(A)$
- $ab = f(u) f(v) \underset{\text{hom.}}{=} f(\underbrace{uv}_{\in A}) \in f(A)$ $\square$

Def: $f: R \to S$.

f *injective* if $r_1 \neq r_2 \Rightarrow f(r_1) \neq f(r_2)$

f *surjective* if $f(R) = S$

f *bijective* if f both injective and surjective

> **Theorem:** Let R, S be rings and $f: R \to S$ a *surjective* homom.
>
> 1. R has identity $1_R \Rightarrow S$ has identity 1_S and $f(1_R) = 1_S$
> 2. $a \in R$ unit in $R \Rightarrow f(a) \in S$ unit in S and $f(a)^{-1} = f(a^{-1})$

Proof: ①: Take any $s \in S$. f surj. $\Rightarrow s = f(r)$ for some $r \in R$.

$\Rightarrow s \cdot f(1_R) = f(r) \cdot f(1_R) \underset{\text{hom.}}{=} f(r \cdot 1_R) = f(r) = s$

Similarly $f(1_R) \cdot s = s$. Conclusion $f(1_R) = 1_S$.

②: $f(a) \cdot f(a^{-1}) \underset{\text{hom.}}{=} f(a \cdot a^{-1}) = f(1_R) \underset{①}{=} 1_S$

Sim. $f(a^{-1}) \cdot f(a) = 1_S$. Conclusion $f(a)^{-1} = f(a^{-1})$ $\square$

Def: R, S rings. A *bijective* homomorphism $f: R \to S$ is called an *isomorphism*. If there exists an isomorphism, then we say that R and S are *isomorphic* and write $R \cong S$.

Note: $R \cong S$ means R and S are basically the *same ring*.

Note: $\cong$ *eq. relation*, i.e.

(i) $R \cong R$

(ii) $R \cong S \Rightarrow S \cong R$

(iii) $R \cong S, S \cong T \Rightarrow R \cong T$

Ex: (Earlier example) $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ was shown to be a *field*. In fact $K \cong \mathbb{C}$.

Proof: Consider $f: K \to \mathbb{C}$ defined by $f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a + bi$.

- f is injective and surjective (check!) $\Rightarrow f$ *bijective*
- $f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) = f\left(\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}\right) = (a+c) + (b+d)i = (a+bi) + (c+di) = f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) + f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right)$
- $f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) = f\left(\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}\right) = ac - bd + (ad+bc)i$

$f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) \cdot f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) = (a+bi)(c+di) = ac - bd + (ad+bc)i$

$\Rightarrow f$ *homom.*

Conclusion f *isomorphism*. $\square$

Ex: Let $2\mathbb{Z} = \{\text{even integers}\}$. Define $f: \mathbb{Z} \to 2\mathbb{Z}$ by $f(x) = 2x$. We see that f injective and surj. Is f an homomorphism?

- $f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$ Ok
- $f(xy) = 2xy \neq (2x) \cdot (2y) = f(x) \cdot f(y)$ No!

$\Rightarrow f$ not homom.

Note: We can see that $\mathbb{Z} \not\cong 2\mathbb{Z}$ since they have *different ring properties*. For example $\mathbb{Z}$ has identity, $2\mathbb{Z}$ has not.

Polynomial rings (4.1–4.3)

Polynomial with coeff. in a ring R:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \quad a_i \in R.$$

The *indeterminate* x is considered a *symbol*, i.e. not an element of R. If $a_n \neq 0_R$, then $\deg p(x) = n$.

If $p(x) = a_0 \in R$ ($a_0 \neq 0_R$), then $p(x)$ *constant* polynomial (degree 0).

Zero polynomial $p(x) = 0_R$ has no degree.

> **Theorem:** $R[x] = \{\text{pol. with coeff. in } R\}$ with the usual pol. operations $+$ and $\cdot$ is a *ring*.

Ex: In $\mathbb{Z}_6[x]$ we have

$$(2x^3 + 3x^2 + x)(3x^2 + 4) = 6x^5 + 9x^4 + 11x^3 + 12x^2 + 4x = 0 + 3x^4 + 5x^3 + 0 + 4x = 3x^4 + 5x^3 + 4x$$

Note that, in general, $\deg(p(x)q(x)) \le \deg p(x) + \deg q(x)$.

Theorem: If R int. domain, then $\deg(p(x)q(x)) = \deg p(x) + \deg q(x)$

Theorem: If R int. domain, then $R[x]$ int. domain.

Proofs: Exercise

Now we let $R = F$ field:

> Theorem (Division Algorithm): Let $f(x), g(x) \in F[x]$, $g(x) \neq 0$. Then there exist unique $q(x), r(x) \in F[x]$ such that
>
> $$f(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x) \text{ or } r(x) = 0.$$

Proof: Existence: Induction over $\deg f(x)$.

If $\deg f(x) < \deg g(x)$ (or $f(x)=0$), then $q(x)=0$ and $r(x)=f(x)$.

If $\deg f(x) \ge \deg g(x)$, then

$$f(x) = a_n x^n + \text{lower}, \qquad m \le n$$
$$g(x) = b_m x^m + \text{lower},$$

and $h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$ has lower degree than $f(x)$.
← F field

By induction $h(x) = q_1(x)g(x) + r(x) \Rightarrow$

$$f(x) = h(x) + a_n b_m^{-1} x^{n-m} g(x) = \underbrace{\left(q_1(x) + a_n b_m^{-1} x^{n-m}\right)}_{= q(x)} g(x) + r(x)$$

where $\deg r(x) < \deg g(x)$ or $r(x) = 0$.

Uniqueness: Assume $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$,
$\deg r_1(x), \deg r_2(x) < \deg g(x)$ or $r_1(x), r_2(x) = 0$

$$\Rightarrow (q_1(x) - q_2(x))g(x) = \underbrace{r_2(x) - r_1(x)}_{\text{degree} < \deg g(x) \text{ (or 0)}}$$

Only possibility is $q_1(x) = q_2(x)$, and thus $r_1(x) = r_2(x)$. □

Def: $g(x), f(x) \in F[x]$. Then

$$g(x) \mid f(x) \overset{\text{def.}}{\Longleftrightarrow} \text{there exists } q(x) \in F[x] \text{ s.t. } f(x) = q(x)g(x)$$

Properties:
- $g(x) \mid f(x) \Rightarrow \deg g(x) \le \deg f(x)$
- $g(x) \mid f(x) \Rightarrow c \cdot g(x) \mid f(x)$ for all $c \in F$, $c \neq 0$.

Def: $f(x) \in F[x]$ monic if leading coefficient $a_n = 1$.

Def (GCD): Assume $f(x), g(x) \in F[x]$ (not both $=0$).
If $d(x) \in F[x]$ satisfies

1. $d(x) \mid f(x)$ and $d(x) \mid g(x)$ (common divisor)
2. $c(x) \mid f(x)$ and $c(x) \mid g(x) \Rightarrow \deg c(x) \le \deg d(x)$ (greatest)
3. $d(x)$ monic

then $d(x)$ is called greatest common divisor of $f(x), g(x)$, written $d(x) = (f(x), g(x))$

> Theorem: $(f(x), g(x))$ is unique. There exist $u(x), v(x)$ such that $(f(x), g(x)) = u(x)f(x) + v(x)g(x)$.

"Proof": Copy proof in $\mathbb{Z}$. $(f(x), g(x))$ is the monic polynomial of smallest degree that can be written $(f(x), g(x)) = u(x)f(x) + v(x)g(x)$.

Also for $F[x]$ we have an Euclidean Algorithm for finding $(f(x), g(x))$ and polynomials $u(x), v(x)$.

Def: $f(x)$ and $g(x)$ are relatively prime if $(f(x), g(x)) = 1$.

Theorem:

$$\left.\begin{array}{l} f(x) \mid g(x)h(x) \\ (f(x), g(x)) = 1 \end{array}\right\} \Rightarrow f(x) \mid h(x).$$

Proof: Copy proof in $\mathbb{Z}$.

Repetition: $f(x)$ unit in $R[x]$ if there exists $g(x)$ such that $f(x)g(x) = g(x)f(x) = 1$.

> Theorem: F field. $f(x) \in F[x]$ unit $\Leftrightarrow f(x) \in F$, $f(x) \neq 0$.

Proof: $\Leftarrow$) obvious since F field

$\Rightarrow$) $f(x)g(x) = 1 \Rightarrow \deg(f(x)) + \deg(g(x)) = \deg 1 = 0$
(F field ⇒ F int. dom.)

$\Rightarrow \deg f(x) = \deg g(x) = 0 \Rightarrow f(x) \in F$,

and clearly $f(x) \neq 0$ since F has no zero-divisors. □

Exercise: R int. domain. Show $f(x)$ unit in $R[x] \Leftrightarrow f(x)$ unit in R.

Unique factorization in $F[x]$:

Def: $p(x) \in F[x]$, $\deg p(x) \ge 1$, is called irreducible if $p(x) = f(x)g(x) \Rightarrow f(x) \in F$ or $g(x) \in F$ (analogue of a prime).

Ex: All polynomials of degree 1, i.e. $p(x) = ax + b$, are irreducible.

Ex: $x^2 + 1$ is irr. over $\mathbb{R}$, but over $\mathbb{C}$ it is reducible since $x^2 + 1 = (x+i)(x-i)$.

> Theorem: $p(x) \in F[x]$, $\deg p(x) \ge 1$. The follow. are equivalent:
>
> 1. $p(x)$ irreducible
> 2. $p(x) \mid f(x)g(x) \Rightarrow p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Proof: 1 ⇒ 2: $p(x) \nmid f(x) \Rightarrow (p(x), f(x)) = 1 \underset{\text{Theorem}}{\Rightarrow} p(x) \mid g(x)$.

2 ⇒ 1: $p(x) = f(x)g(x) \Rightarrow p(x) \mid f(x)g(x)$
$\Rightarrow p(x) \mid f(x)$ or $p(x) \mid g(x)$

Assume $p(x) \mid f(x)$. Then $f(x) = h(x)p(x) \Rightarrow$

$$p(x) = f(x)g(x) = h(x)p(x)g(x) \Rightarrow$$

$\deg p(x) = \deg h(x) + \deg p(x) + \deg g(x) \Rightarrow \deg g(x) = 0 \Rightarrow g(x) \in F$ □

Theorem: Every $f(x) \in F[x]$, $\deg f(x) \geq 1$, is a product of irreducible polynomials, unique up to ordering and constant factors.

Proof: Copy situation in $\mathbb{Z}$.