Lecture 7:

Repetition: The subring $I \subseteq R$ is an ideal if

$$r \in R,\ a \in I \Rightarrow ra \in I \text{ and } ar \in I$$

We define: $a \equiv b \pmod{I} \Leftrightarrow a - b \in I$

$$a + I = \{a + i;\ i \in I\} \quad \text{equiv. class w.r.t. } \equiv$$

We get the quotient ring R/I with operations

$$(a+I) + (b+I) = (a+b) + I,\quad (a+I)(b+I) = (ab) + I.$$

First isom. theorem: If $f: R \to S$ homom. and $\ker f = \{a \in R;\ f(a) = 0_S\}$ then $R/\ker f \cong \operatorname{im} f \ (= f(R))$

We also know that:

- $\mathbb{Z}_n \left(\cong \mathbb{Z}/(n)\right)$ is an $\begin{cases}\text{int. domain}\\ \text{field}\end{cases} \Leftrightarrow n$ prime
- $F[x]/(p(x))$ is an $\begin{cases}\text{int. domain}\\ \text{field}\end{cases} \Leftrightarrow p(x)$ irreducible

We want to find analogue of a prime in R:

Def: The ideal P of a commutative ring R is prime if $P \neq R$ and $ab \in P \Rightarrow a \in P$ or $b \in P$.

Ex: In $\mathbb{Z}$: (n) prime ideal $\underset{\uparrow \text{ exercise}}{\Leftrightarrow}$ n prime $\Leftrightarrow \mathbb{Z}/(n)$ field

In $F[x]$: $(p(x))$ prime ideal $\Leftrightarrow p(x)$ irred. $\Leftrightarrow F[x]/(p(x))$ field

Ex: In $\mathbb{Z}[x]$: $(x) = \{x f(x);\ f(x) \in \mathbb{Z}[x]\} = \{\text{pol. with constant term } 0\}$ is a prime ideal: Assume

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots,\quad g(x) = b_0 + b_1 x + b_2 x^2 + \dots$$

$f(x) g(x) \in (x) \Rightarrow a_0 b_0 = 0 \Rightarrow$

$\Rightarrow a_0 = 0$ or $b_0 = 0 \Rightarrow f(x) \in (x)$ or $g(x) \in (x)$.

But note that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is not a field!

first iso. theorem with $\varphi(a_0 + a_1 x + \dots) = a_0$

However, it is an integral domain. □

In general, we have

Theorem: If R comm. ring w. identity and P ideal, then

$$P \text{ prime} \Leftrightarrow R/P \text{ integral domain.}$$

Proof: $\Rightarrow$) We need to show

1. that $1_{R/P} \neq 0_{R/P}$
2. R/P has no zero-divisors.

1: Since P prime we know that $P \neq R$. Thus $1_R \notin P$, since $1_R \in P$ would imply $P = R$.

Now $1_R \notin P \Leftrightarrow 1_R + P \neq 0_R + P$

2: $(a+P)(b+P) = 0_R + P \Leftrightarrow ab + P = 0_R + P$

$\Leftrightarrow ab \in P \underset{\uparrow\, P \text{ prime}}{\Leftrightarrow} a \in P$ or $b \in P \Leftrightarrow a + P = 0_R + P$ or $b + P = 0_R + P$

$\Leftarrow$) Since by assumption $1_{R/P} \neq 0_{R/P}$, it follows that $P \neq R$. Now

$ab \in P \Rightarrow (a+P)(b+P) = ab + P = 0_R + P$

$\underset{\uparrow\, R/P \text{ int. domain}}{\Rightarrow} a + P = 0_R + P$ or $b + P = 0_R + P$

$\Rightarrow a \in P$ or $b \in P$. □

What kind of an ideal ~~I~~ turns R/I into a field?

Def: The ideal M of the ring R is maximal if $M \neq R$ and an ideal J with $M \subseteq J \subseteq R$ $\Rightarrow J = M$ or $J = R$.

Ex: In $\mathbb{Z}$: Assume p prime number and consider ideal J such that $(p) \subseteq J \subseteq \mathbb{Z}$.

If $J \neq (p)$ then there exists $a \in J$, $a \notin (p)$

$\Rightarrow p \nmid a \Rightarrow (a, p) = 1 \Rightarrow 1 = up + va$ for some $u, v \in \mathbb{Z}$.

Furthermore $1 = up + va \in J$ since $p \in J$ and $a \in J$.

But $1 \in J \Rightarrow J = \mathbb{Z}$.

Conclusion: (p) is maximal ideal

Note: k not prime number $\Rightarrow k = mn$ with $m, n \neq \pm 1$

$\Rightarrow (k) \subseteq (n) \subseteq \mathbb{Z}$ with $(k) \neq (n)$, (Note that $n \in (n)$ but $n \notin (k)$.) and $(n) \neq \mathbb{Z}$.

Conclusion: (k) is not maximal ideal.

Theorem: R comm. ring with identity, and M ideal. Then

$$M \text{ maximal} \Leftrightarrow R/M \text{ field.}$$

Proof: $\Rightarrow$) As before, $1_{R/M} \neq 0_{R/M}$ since $M \neq R$.

We want to show that every $a + M \neq 0_R + M$ has inverse.

Construct the ideal (check!) $J = \{m + ra;\ r \in R, m \in M\}$.

Clearly $M \subseteq J \subseteq R$, but $J \neq M$ since $a \in J$, $a \notin M$.

M maximal $\Rightarrow J = R \Rightarrow m + ra = 1_R$ for some $m \in M$, $r \in R \Rightarrow$

$$(r+M)(a+M) = ra + M = 1_R + M \Rightarrow (a+M)^{-1} = r + M.$$

$\Leftarrow$) As before, since $1_{R/M} \neq 0_{R/M}$ it follows that $M \neq R$.

Assume J ideal such that $M \subseteq J \subseteq R$. If $J \neq M$ there exists $a \in J$ but $a \notin M \Rightarrow a + M \neq 0_R + M$

$\underset{\uparrow\, R/M \text{ field}}{\Rightarrow} a + M$ has inverse $b + M$

$\Rightarrow (a+M)(b+M) = ab + M = 1_R + M$

$\Rightarrow ab - 1_R = m \in M \Rightarrow 1_R = ab - m \in J$

(note that $a \in J$ and $m \in M \subseteq J$) $\Rightarrow J = R$. □

Ex: $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ not field $\Rightarrow (x)$ not maximal

Ex: $I = \{\text{pol. in } \mathbb{Z}[x] \text{ with } 2 \mid a_0\}$ ideal in $\mathbb{Z}[x]$ with $(x) \subseteq I$ but $(x) \neq I$.

In Lecture 6 we saw that $\mathbb{Z}[x]/I \cong \mathbb{Z}_2$ field

$\Rightarrow I$ maximal ideal.

Corollary: R comm. ring with identity and I ideal. Then

$$I \text{ maximal} \Rightarrow I \text{ prime}$$

Proof: I maximal $\Rightarrow R/I$ field $\Rightarrow R/I$ int. domain (5)

$\Rightarrow I$ prime. □

Groups (Chapter 7):

Def (Group): A set $G \neq \emptyset$ together with operation $\cdot$ is called a group if

① $a \in G, b \in G \Rightarrow ab \in G$ (closure)

② $a\cdot(b\cdot c) = (a\cdot b)\cdot c$ (associative)

③ there is an element $e \in G$ such that $a\cdot e = e\cdot a = a$ for all $a \in G$ (identity)

④ For each $a \in G$ there is $d \in G$ such that $a\cdot d = e$ and $d \cdot a = e$ (inverse)

Def (Abelian): A group G is called abelian (=commutative) if $a\cdot b = b\cdot a$ for all $a, b \in G$.

Notes:
- the identity element e is unique
- the inverse d in ④ is unique, and is written a^{-1}
- by the order of G we mean the number of elements of G, written $|G|$ (can be infinite)
- we can prove a cancellation law
  $$\left.\begin{array}{l} ab = a\cdot c \\ \text{or } b\cdot a = c\cdot a \end{array}\right\} \Rightarrow b = c$$
- often we just write ab instead of $a\cdot b$

Ex: A permutation of a set T is a bijective function $f: T \to T$. For $T = \{1,2,3\}$ we can describe f on the form $\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$ (6)

Composition $f\circ g$: $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$\Rightarrow f\circ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$g\circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

We want to show that the set of all permutations, written S_3, with operation $\circ$ is a group:

① See example above $f, g \in S_3 \Rightarrow f \circ g \in S_3$

② Ass. follows from that composition of functions in general is associative

③ $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

④ True. For example $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \Rightarrow f^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\Rightarrow S_3$ group. But not abelian; see above □

Note: Order of group $|S_3| = 3! = 6$.

Def: The set of all permutations of $\{1,2,3,\dots,n\}$ is called the symmetric group on n symbols, and is written S_n. We have $|S_n| = n!$ (exercise)

- Study example on page 164-167 by yourself: (7)

  D_n – the dihedral group of degree n

  The group of symmetries of a regular polygon with n sides

Theorem: Any ring is an abelian group with respect to addition.

Proof: Compare axioms for group with axioms for ring with respect to addition.

Note: Not true for multiplication (why?)

Theorem: Let R be a ring with identity. The set of all units in R is a group with respect to multiplication.

Proof: Exercise.

Corollary: The set of non-zero elements of a field is an abelian group under multiplication.

Theorem: In a group G we have:

① $(ab)^{-1} = b^{-1}a^{-1}$

② $(a^{-1})^{-1} = a$

Proof: Exercise

Def: For $a \in G$ we define (8)

$a^n = a\cdot a\cdot a\cdot a \cdot \dots \cdot a$ (n factors)

$a^{-n} = a^{-1}\cdot a^{-1}\cdot a^{-1}\cdot \dots \cdot a^{-1}$ (n factors)

$a^0 = e$

Note: If operation in G is written as addition, then a^n becomes $n\cdot a = a + a + a + \dots + a$

Def: Let $a \in G$. If $a^n = e$ for some $n \geq 1$, then a has finite order. The smallest $n \geq 1$ such that $a^n = e$ is called the order of a, written $|a| = n$.

Ex: $\{1, -1, i, -i\} \subseteq \mathbb{C}$ is a group under multiplication (check!) with identity $e = 1$.

Now

$1^1 = 1$, so $|1| = 1$

$(-1)^1 = -1$, $(-1)^2 = 1$, so $|-1| = 2$

$i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, so $|i| = 4$

similarly $|-i| = 4$

Ex: $G = \mathbb{Z}_6$ group under addition.

$2 = 2$, $2+2 = 4$, $\underbrace{2+2+2 = 0}_{\text{identity under addition}} \Rightarrow |2| = 3$

Exercise:

$|0| = 1$, $|1| = 6$, $|3| = 2$, $|4| = 3$, $|5| = 6$

Theorem: G group, $a \in G$.

1. If a has infinite order, then $i \neq j \Rightarrow a^i \neq a^j$
2. If $|a| = n$, then $a^k = e \Leftrightarrow n \mid k$
3. $|a| = n$ and $n = t \cdot d$ $(d > 0)$ $\Rightarrow |a^t| = d$

Proof: ① Assume the contrary, i.e $a^i = a^j$ with $i > j$

$\Rightarrow e = a^i \cdot (a^i)^{-1} = a^i \cdot (a^j)^{-1} = a^i \cdot a^{-j} = a^{i-j}$

$\Rightarrow$ a has finite order. Contradiction!

② $\Leftarrow)$ $n \mid k \Rightarrow k = tn \Rightarrow a^k = a^{tn} = (a^n)^t = e^t = e$

$\Rightarrow)$ Div. alg. $k = nq + r$ with $r < n$

$\Rightarrow e = a^k = a^{nq+r} = (a^n)^q \cdot a^r = e^q \cdot a^r$
$= e \cdot a^r = a^r$

$r > 0$ would contradict n smallest such that $a^n = e$.
We must have $r = 0 \Rightarrow k = nq \Rightarrow n \mid k$.

③ $(a^t)^d = a^{td} = a^n = e$. We want to show d smallest: $e = (a^t)^k = a^{tk} \overset{②}{\Rightarrow}$

$\Rightarrow \begin{cases} n \mid tk \\ n = td \end{cases} \Rightarrow d \mid k \Rightarrow d \leq k.$ $\square$