Lecture 14: Review of rings

§7.1, 7.3 of [DF]
§1-6 of [R2]

A ring is a set R with binary ops $+$ and $\cdot$ where

1) $(R,+)$ is an abelian gp.
2) Mult is associative: $a\cdot(b\cdot c) = (a\cdot b)\cdot c$
3) Distributive: $a\cdot(b+c) = a\cdot b + a\cdot c$ and $(a+b)\cdot c = a\cdot c + b\cdot c$

$\forall a,b,c$ in R.

R is commutative when $a\cdot b = b\cdot a$ for all $a,b \in R$.

R has an identity when $\exists\, 1 \in R$ with $1\cdot a = a = a\cdot 1$ for all $a \in R$.

[Basically all rings we'll encounter will have a 1; Most will be commutative.]

Ex: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}[x]$ [Query for more]

Non-commutative: R comm with 1, consider

$$M_{n\times n}(R) = \{ n\times n \text{ matrices with entries in } R \}.$$

$$\mathbb{H} = \{ a+bi+cj+dk \mid a,b,c,d \in \mathbb{R} \}$$

where $1, i, j, k$ multiply as in Q_8.

One focus for us: $\mathbb{Z}[i] = \{ a+bi \mid a,b \in \mathbb{Z} \} \subseteq \mathbb{C}$

$$\mathbb{Z}[\sqrt{2}] = \{ a+b\sqrt{2} \mid a,b \in \mathbb{Z} \} \subseteq \mathbb{R}.$$

Trivial ring: $R = \{0\}$. Q: Does it have a unit?

A: Yes, but is the only ring where $1 = 0$.

R ring with 1.

unit: $a \in R$ where $\exists b \in R$ with $ab = ba = 1$.
(b unique, write a^{-1}). $R^\times = \{\text{units in } R\}$, a group under mult.

zero divisor: nonzero $a \in R$ where $\exists b \neq 0 \in R$ with $ab = 0$.

Ex: 2 in $\mathbb{Z}/6\mathbb{Z}$. Ex: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_{2\times 2}(\mathbb{Q})$.

division ring: $R^\times = R \setminus \{0\}$ and $1 \neq 0$.
Ex: $\mathbb{H}$. $(a+bi+cj+dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$

field: commut. divison ring. Ex: $\mathbb{Q}$, $\mathbb{F}_p$, $\mathbb{C}$.

An integral domain is a commutative R where $1 \neq 0$ and R has no zero divisors.

Ex: $\mathbb{Z}$, field, $\mathbb{Z}[x]$, $\mathbb{Z}[i]$ ✓ as subring of a field.

In an int domain R, say $r \in R$ is irreducible when $r = a \cdot b \Rightarrow$ one of a, b is a unit.

Unique factorization: Any $r \in R$ is $r_1 r_2 \cdots r_n$ with r_i irreducible, in an essentially unique way

Ex: $R = \mathbb{Z}$ $\quad 6 = 2 \cdot 3 = 3 \cdot 2 = (-2)(-3) = (-3)(-2)$

Fun facts: $\mathbb{Z}[i]$ has unique factorization, but $\mathbb{Z}[\sqrt{5}i] = \mathbb{Z}[\sqrt{-5}]$ does not!

$$6 = \underbrace{2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})}_{\text{all irreducible.}}$$

[Motivation: Many facts about number theory can be understood in terms of factoring in such rings]

A ring homomorphism $\phi : R \to S$ is a fn where

$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)$

Usual notions of image, kernel, isomorphism.

Suppose $I \subseteq R$ is a subgp of $(R, +)$. Then I is a

- left-ideal if $r \cdot I = \{r \cdot x \mid x \in I\} \subseteq I$ for all $r \in R$.
- right-ideal if $I \cdot r = \{x \cdot r \mid x \in I\} \subseteq I$ for all $r \in R$.
- two-sided ideal when both a left and right ideal.

[When R is commutative, these are all the same notion.]

Note: If $\phi: R \to S$ is a ring homom, then $\ker(\phi)$ is a two-sided ideal. (ideals like normal subgps.)

Construction: Suppose $I \subseteq R$ is a 2-sided ideal. Let R/I be the quotient group of $(R,+)$ by its subgp I. (Write $a+I \in R/I$, and for $a, b \in R$ have $(a+I)+(b+I) = (a+b)+I$). Define a product on R/I by $(a+I)(b+I) = (ab)+I$.

Works because I is a 2-sided ideal. Have quotient ring hom $\pi: R \to R/I$.

Q: What's $\ker(\pi)$? A. I.

Fun fact: Ideals first appeared as "ideal numbers" used to restore unique factorization in the likes of $\mathbb{Z}[\sqrt{-5}]$.