Chapter 0 Review: Rings and fields

§0.1 Basic definitions and properties

Defn ① A ring R is a set together with 2 binary operations $+$ and $\cdot$, (called addition and multiplication) and distinguished elements $0, 1 \in R$ s.t

1) $(R, 0, +)$ is an abelian gp
2) $(R, 1, \cdot)$ is a monoid, (ie $\cdot$ is associative and $1 \cdot a = a \cdot 1 \quad \forall a \in R$)
3) The distributive laws hold

$$(a+b) \cdot c = a \cdot c + b \cdot c$$
$$a \cdot (b+c) = a \cdot b + a \cdot c$$

R is called commutative if $\cdot$ is commutative

② An non-zero elt $a \in R$ is called a zero divisor (Nullteiler) if $\exists\, b \in R$ s.t $b \neq 0$ and $ab = 0$ or $ba = 0$

③ An element is called nilpotent if $\exists\, n \in \mathbb{N}$ s.t $a^n = 0$.

④ An element $a \in R$ is called a unit if $\exists\, b \in R$ s.t $ab = ba = 1$

b is called the inverse of a.

The set of all units in R is denoted by $R^\times$

$(R^\times, 1, \cdot)$ is a group, called group of units in R, (Einheitengruppe)

(5) A ring is called a division ring or a skew field (Schiefkörper) if every non-zero element $a \in R$ has a multiplicative inverse (ie a unit)

(6) A comm. division ring is called a field (Körper).
ie $(R, 0, 1, +, \cdot)$ is a field if
(1) $(R, 0, +)$ is a comm. group
(2) $(R \setminus \{0\}, 1, \cdot)$ is a comm. group
(3) $\forall a, b, c \in R$, $a \cdot (b+c) = ab + ac$

Examples (1) $R = \{0\}$ is called the zero ring
For the zero ring we have $1 = 0$.
$\{0\}$ is not a field. Since in a field we always have $1 \neq 0$.

(2) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all rings
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are also fields.

(3) $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$, $\bar{a} = a + n\mathbb{Z}$, $a \in \mathbb{Z}$
is a comm ring
$\mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow n = p$ a prime

(4) $\mathbb{H} = \{a + b\bar{i} + c\bar{j} + dk \mid a, b, c, d \in \mathbb{R}\}$ w/
$(a + b\bar{i} + c\bar{j} + dk) + (a' + b'\bar{i} + c'\bar{j} + d'k) :=$
$(a + a') + (b + b')\bar{i} + \ldots + (d + d')k$
multiplication defined expanding and using
$\bar{i}^2 = \bar{j}^2 = k^2 = -1$, $\bar{i}\bar{j} = k$, $\bar{j}k = \bar{i}$, $k\bar{i} = \bar{j}$
is a division ring which is not a field

(5) $R = \{ f : [0,1] \to \mathbb{R} \mid f \text{ continuous} \}$
is a ring w/ usual addition and multiplication of functions
0_R = zero function 1_R = the const. function 1.

$R^\times = \{ f \in R \mid f(x) \neq 0 \ \forall x \in [0,1] \}$
For $f \in R^\times$, $f^{-1} = 1/f$

R has many zero divisors: eg $f = \begin{cases} 0 & 0 \le x \le \frac{1}{2} \\ x - \frac{1}{2} & \frac{1}{2} \le x \le 1 \end{cases}$
let $g(x) := f(1-x)$ Then $fg = 0$.

$h(x) = x - \frac{1}{2}$ is neither a unit (It is zero at $x = \frac{1}{2}$) nor a zero divisor. Since if $\exists\ k(x) \in R$ s.t $hk = 0$. Then $k(x) = 0 \ \forall x \neq \frac{1}{2}$ but k is continuous hence $k \equiv 0$.

(6) $R = M_{2\times 2}(\mathbb{R})$ 2×2 matrices w/ real entries is a non-comm ring w/ $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. It contains zero divisors and nilpotent elts

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

(7) With our defn of a ring $2\mathbb{Z}$ is not a ring!

Defn (1) A comm ring w/ $1 \neq 0$ is called an integral domain (Integritätsring, Integritätsbereich) if it has no zero divisors.

Every field is an integral domain (ID)

(2) A subring S of a ring R is a subgroup of $(R, 0, +)$ which is closed under multiplication and $1_R \in S$.

Rmk. There are books in which a ring is defined without assuming that the set R has a multiplicative identity 1_R. and a subring is defined as a s/gp of $(R, 0, +)$ which is closed under multiplication. Rings which has a multp. identity are called Ring w/ 1.

Without the assumption of existence of $1_R \in R$ in the defn of a ring and subring we can have a subring which does not necessarily have 1 and even if it does we don't necessarily have $1_S = 1_R$.

For example (a) $2\mathbb{Z}$ with this definition is a ring and it is a subring of $\mathbb{Z}$ $\mathbb{Z}$ has 1, but $2\mathbb{Z}$ doesn't

ex: Let $R = \mathbb{R} \oplus \mathbb{R}$
$S = \{(r, 0) \mid r \in \mathbb{R}\}$

Both R, S have 1 But $1_R = (1,1)$
$1_R \neq 1_S = (1,0)$.

§0.2 Ideals, ring homomorphisms, and quotient rings

Let $(R, 0, 1, +, \cdot)$ be a ring
$(S, 0, +)$ a subgp of $(R, 0, +)$
Then $(R/S, 0+S, +)$ is a group.

but under the multiplication
$(a+S)(b+S) := ab+S$
$R/S = \{a+S \mid a \in R\}$ is not always a ring. For R/S to be a ring we need S to be "special".

Defn R a ring, A subset $I \subseteq R$, $I \neq \emptyset$ is a left ideal of R if
① $\forall a, b \in I$, $a+b \in I$
② $rI \subseteq I$ $\forall r \in R$ (I is closed under left multip. w/ elts of R)
Similarly one can defne a right ideal.
w/ ②' $Ir \subseteq I$

I is called (2 sided) ideal of R if it is both a left and right ideal of R. We write $I \trianglelefteq R$

For an ideal I of R, the set of cosets $R/I = \{ a + I \mid a \in R \}$ is a ring called the quotient ring of R by I

Rk R a ring, S a subset of R. Then S is an ideal of R iff the following holds
① S is an additive s/gp of R.
② $\forall r \in R$, $\forall s \in S$, we have $rs \in S$, $sr \in S$

Ex: $\mathbb{Z} < \mathbb{Q}$, is a subring but not an ideal since $1 \in \mathbb{Z}$, but $1 \cdot \frac{1}{3} \notin \mathbb{Z}$.

Rk. In fact if R is a ring then the only ideals of R that contains 1 is R itself

Properties of ideals ① $I, J \trianglelefteq R$ then $I \cap J \trianglelefteq R$

② $IJ := \left\{ \sum_{n=0}^{n} x_i y_i \mid n \in \mathbb{N}, x_i \in I, y_i \in J \right\}$

$IJ \subset I \cap J$, $IJ \trianglelefteq R$

② If X is a non-empty subset of R then $\langle X \rangle := $ the ideal generated by X ie the smallest ideal of R that contains X

$$\langle X \rangle = RXR = \left\{ \sum_i r_i x_i s_i \;\middle|\; \begin{array}{l} r_i, s_i \in R, \\ x_i \in X \end{array} \text{ the sum is finite} \right\}$$

if R is comm. then $\langle X \rangle$ is the collection of all finite sums $\sum_i r_i x_i$, $r_i \in R$, $x_i \in X$

The ideal $\langle a \rangle$, generated by a single element a is called the principal ideal generated by a.

③ Given 2 ideals I, J of R

$I + J := \{ x + y \mid x \in I, y \in J \}$ is an ideal of R

$= \langle I \cup J \rangle$

④ Let R be a ring. We say I and J are relatively prime if $I + J = R$

⑤ A maximal ideal M in a ring R. is a proper ideal (ie $M \neq R$, $M \neq (0)$) that is not contained in any strictly larger ideal

Thm: Every proper ideal I in a ring R is contained in a maximal ideal

Recall: If $\phi : G \to H$ is a group hom then $N = \ker \phi \trianglelefteq G$ and every normal s/gp of G is the kernel of a hom, namely if $\pi : G \to G/N$ the canonical projection

Similar statements holds for ring homomorphism

Defn (1) Let R, S be rings. A ring homomorphism is a map $\varphi: R \to S$ s.t $\forall\ a, b \in R$ we have

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$

(iii) $\varphi(1_R) = 1_S$.

An injective + surjective hom. is called an isomorphism

(2) The kernel of a ring hom $\varphi: R \to S$ is defined as $\ker\varphi := \{r \in R \mid \varphi(r) = 0_S\}$

$\ker\varphi$ is an ideal of φ

$\text{Image}(\varphi) = \{\varphi(a) \mid a \in R\}$ is a subring of S.

Rmk. If one defines rings without assuming that R has 1, then one can define ring hom. without (iii). Then it does not follow that $\varphi(1_R) = 1_S$ even when R, and S have 1.

Isomorphism thms for rings

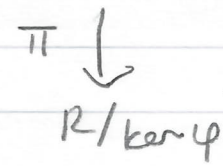
(1) $\varphi: R \to S$ is an onto hom then

$$R/\ker\varphi \cong S$$

(2) Let π be the canonical hom from R to $R/\ker\varphi$

Then $\exists!$ isom $\bar{\varphi}: R/\ker\varphi \to S$ s.t

$\bar{\varphi} \circ \pi = \varphi$:



(3) R be a ring, S a subring of R, I an ideal of R. Then

(a) $S+I := \{a+b \mid a \in S, b \in I\}$ is a subring of R

(b) I is an ideal of $S+I$

(c) $S \cap I$ is an ideal of S and $(S+I)/I \cong S/S \cap I$

(4) Let I, J be ideals of R and suppose $I \subseteq J$. Then J/I is an ideal of R/I and

$$R/J \cong (R/I)/(J/I)$$

(5) Let $\varphi : R \to Q$ be an onto homom. Then there is a one-to-one correspondence between the sets

$A = \{I : I \text{ ideal of } R, \ker\varphi \subset I\}$ and

$B = \{J : J \text{ is an ideal of } Q\}$.