Algebra 2

Exercise Sheet 1

Prof. Markus Land
Dr. Maksim Zhykhovich

Summer Semester 2023
25.04.2023

Exercise 1. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of a commutative ring A.
(1) Show that $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$.
(2) Assume that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime (that is $\mathfrak{a} + \mathfrak{b} = A$). Show that $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.
(3) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be pairwise coprime ideals in A. Show that $\prod_{i=1}^n \mathfrak{a}_i = \bigcap_{i=1}^n \mathfrak{a}_i$.

Exercise 2. Let I and J be two ideals of a commutative ring A and $\pi : A \to A/I$ the canonical projection. Show that $\pi(J)$ is an ideal in A/I and

$$(A/I)/\pi(J) \simeq A/(I+J)\,.$$

Exercise 3. Let p be a prime number.
(1) Show that -1 is not a square in $\mathbb{F}_p$ if and only if $p = 3 \mod 4$.
Remark: See Aufgabe 1, Tutoriumsblatt 3 (Algebra 1).
(2) Let $\mathbb{Z}[i]$ be the ring of Gaussian intergers. Show that the ideal (p) is prime if and only if $p = 3 \mod 4$.
Hint: Consider the quotient ring $\mathbb{Z}[i]/(p)$, observe that $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$ and use Exercise 2 and question (1).

Exercise 4. Show that every prime ideal $\mathfrak{p}$ in $\mathbb{Z}[X]$ has one of the following form

(1) $\mathfrak{p} = (0)$.
(2) $\mathfrak{p} = (p)$, where p is a prime number.
(3) $\mathfrak{p} = (f)$, where f is an irreducible polynomial in $\mathbb{Z}[X]$.
(4) $\mathfrak{p} = (p, f)$, where p is a prime number and f a polynomial in $\mathbb{Z}[X]$ irreducible modulo p.

Hint: Show that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ and consider two cases: $\mathfrak{p} \cap \mathbb{Z} \neq (0)$ and $\mathfrak{p} \cap \mathbb{Z} = (0)$.

Exercise sheet 1 (Higher Algebra)

Exercise 1

(we write I and J for $\mathfrak{a}$ and $\mathfrak{b}$ respectively)

(1) $IJ = \{ \sum_{i=1}^{k} a_i b_i \mid a_i \in I, b_i \in J \}$

$\forall i = 1, \dots, k$ $\quad a_i b_i \in I$ and $\in J \Rightarrow a_i b_i \in I \cap J \Rightarrow IJ \subset I \cap J$

(2) I and J are coprime $\Longrightarrow 1 = a + b$ for some $a \in I$ and $b \in J$

To show: $I \cap J \subset IJ$

Let $c \in I \cap J$, then $\quad c = \underbrace{a \cdot c}_{} + \underbrace{b \cdot c}_{} \in IJ \Rightarrow I \cap J \subset IJ$

both $\in IJ$

$\Downarrow (1)$

$I \cap J = IJ$

(3) Induction on n.

$n = 2$ (follows from (2)) Assume $n > 2$.

Let $I = I_1$ and $J = I_2 I_3 \cdot \ldots \cdot I_n$

By induction hypothesis $\quad J = I_2 \cdot \ldots \cdot I_n = I_2 \cap \ldots \cap I_n$.

I and J are coprime (follows from Exercise 1.1, Tutorium Sheet 1)

By question (2) $\quad I_1 \cdot \ldots I_n = I \cdot J \underset{(2)}{=} I \cap J = I_1 \cap I_2 \cap \ldots \cap I_n$.

Exercise 2

Since $I \subset I+J$, we have a ring homomorphism

$$\varphi : A/_I \longrightarrow A/_{I+J}$$
$$a+I \longmapsto a+(I+J)$$

(see Satz 2.12 Algebra 1 lecture)

Cleary, φ is surjective, ~~so~~ so $\left(A/_I\right)/_{\mathrm{Ker}\,\varphi} \simeq A/_{I+J}$

To show: $\mathrm{Ker}\,\varphi = \pi(J)$, where $\pi : A \to A/_I$

~~Lets~~ Since the composition

$$J \subset A \xrightarrow{\pi} A/_I \xrightarrow{\varphi} A/_{I+J}$$
$$J \ni a \mapsto a \longmapsto a+I \longmapsto a+(I+J) = 0$$

since $a \in I+J$

is trivial, we have $\pi(J) \subset \mathrm{Ker}\,\varphi$

Let $a+I \in \mathrm{Ker}\,\varphi \subset A/_I$

Then $0 = \varphi(a+I) = a+(I+J) \Leftrightarrow a \in I+J \Leftrightarrow a = b+c$, where $b \in I$ and $c \in J$.

But then $a+I = c + \underset{I}{\underset{\cap}{b}} + I = \underset{J}{\underset{\cap}{c}} + I \in \varphi(J) \Rightarrow \mathrm{Ker}\,\varphi \subset \varphi(J)$

It follows that $\mathrm{Ker}\,\varphi = \varphi(J)$ and

$$\left(A/_I\right)/_{\mathrm{Ker}\,\varphi} \simeq A/_{I+J}.$$

Exercise 3

(1) $p = 2$: -1 is a square mod 2

We assume that p is odd.

$|\mathbb{F}_p^{\times 2}| = \frac{p-1}{2}$ (see Aufgabe 1, Tutoriumsblatt 3 Algebra 1)

Recall that $a^{p-1} - 1 = 0 \quad \forall\, a \in \mathbb{F}_p^{\times}$

Hence, for every square $b = a^2$ holds $b^{\frac{p-1}{2}} = 1$

It follows that

$$b \in \mathbb{F}_p^{\times} \text{ is a root of } \underbrace{X^{\frac{p-1}{2}} - 1}_{\deg = \frac{p-1}{2} = |\mathbb{F}_p^{\times 2}|} \in \mathbb{F}_p[X] \iff b \in \mathbb{F}_p^{\times 2}$$

Therefore,

$$-1 \in \mathbb{F}_p^{\times 2} \iff (-1)^{\frac{p-1}{2}} = 1 \text{ in } \mathbb{F}_p \iff \frac{p-1}{2} \text{ is even } \left(\text{note that } -1 \neq 1\right)$$

$\iff p \equiv 1 \mod 4$

and $-1 \notin \mathbb{F}_p^{\times 2} \iff p \equiv 3 \mod 4$

(2) We show first that $\mathbb{Z}[X]/(X^2+1) \simeq \mathbb{Z}[i]$.

Consider the ring homomorphism: $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[i]$, $X \longmapsto i$

To show: $(X^2+1) = \operatorname{Ker}\varphi$

Clearly $(X^2+1) \subset \operatorname{Ker}\varphi$

Let $f(x) \in \operatorname{Ker}\varphi$

By Satz 2.5 (Algebra 1, Division mit Rest), ~~the~~ we have

$$f(x) = q(x)\,(x^2+1) + ax + b$$

for some $q(x) \in \mathbb{Z}[X]$ and $a, b \in \mathbb{Z}$.

$f(x) \in \operatorname{Ker}\varphi \Rightarrow f(i)=0 \Rightarrow ai+b=0 \Rightarrow a=b=0 \Rightarrow f\in(x^2+1)$

It follows that $\operatorname{Ker}\varphi = (x^2+1)$ and $\mathbb{Z}[X]/(x^2+1) \simeq \mathbb{Z}[i]$

Let p be a prime number in $\mathbb{Z}$

$$\mathbb{Z}[i]/(p) \simeq \left(\mathbb{Z}[X]/(x^2+1)\right)/(p) \underset{\substack{\uparrow \text{ Exercise 2} \\ \cancel{\text{question}} \\ \cancel{(1)}}}{\simeq} \mathbb{Z}[X]/(p, x^2+1) \simeq$$

$$\underset{\substack{\uparrow \text{ Exercise 2} \\ \cancel{\text{question}} \\ \cancel{(1)}}}{\simeq} \left(\mathbb{Z}[X]/(p)\right)/\underset{\substack{\uparrow \\ \text{considered} \\ \text{as a polynomial} \\ \text{in } \mathbb{Z}[X]/(p) \simeq \mathbb{F}_p[X]}}{(x^2+1)} \simeq \mathbb{F}_p[X]/(x^2+1)$$

$\mathbb{F}_p$ is a field $\Rightarrow$ $\mathbb{F}_p[X]$ is a PID

~~$\mathbb{F}_p[X]$~~

(p) is a prime ideal in $\mathbb{Z}[i]$ $\Leftrightarrow$ $\mathbb{Z}[i]/(p)$ is a domain

$\Updownarrow$

$\mathbb{F}_p[X]/(x^2+1)$ is a domain

$\Updownarrow$

x^2+1 is irreducible in $\mathbb{F}_p[X]$

$\Updownarrow$

x^2+1 has no roots in $\mathbb{F}_p$

$\Updownarrow$

-1 is not a square in $\mathbb{F}_p$

question (1) $\longrightarrow$ $\Updownarrow$

$p = 3 \bmod 4$

Exercise 4

Note that all ideals (1) - (4) are prime.

(consider $\mathbb{Z}[X]/\mathfrak{p}$, in case (4) use Exercise 2)

Note that $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Z}[X]$ is a ring hom.

Denote $\mathfrak{q} := \varphi^{-1}(\mathfrak{p}) = \mathbb{Z} \cap \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $\mathfrak{q}$ is also prime in $\mathbb{Z}$

Hence, $\mathfrak{q} = (p)$ for some prime number $p \in \mathbb{Z}$ or $\mathfrak{q} = (0)$

1. case $\mathfrak{q} = (p)$

Consider $\pi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/_p[X]$ Ring homomorphism.

By Lemma 2.26 (3) from the Lecture, $\pi(\mathfrak{p})$ is a prime ideal in $\mathbb{Z}/_p[X]$

$\Rightarrow$ $\pi(\mathfrak{p}) = (0)$ or $\pi(\mathfrak{p}) = (\bar{f})$, where $\bar{f} \in \mathbb{Z}/_p[X]$ irreducible

$\Downarrow$ $\Downarrow$

$\mathfrak{p} = (p)$ $\mathfrak{p} = (p, f)$, where $\pi(f) = \bar{f}$.

2. case $\mathfrak{q} = (0)$. If $\mathfrak{p} = (0)$ then we are in the case (1)

Assume $\mathfrak{p} \neq (0)$

Take $\tilde{f} \in \mathbb{Z}[X]$, $\tilde{f} \in \mathfrak{p}$

$\mathbb{Z}[X]$ factorial $\Rightarrow$ $\tilde{f}$ = product of irreducible factors $\in \mathfrak{p}$

$\Rightarrow$ at least one factor $f \in \mathfrak{p}$.

$\mathfrak{p}$ prime

The goal is to show that $\mathfrak{p} = (f)$.

Let $g \in \mathfrak{p}$. Assume $f \nmid g$ in $\mathbb{Q}[X]$, then g.c.d $(f, g) = 1$

and $1 = f \cdot q + g \cdot h$ in $\mathbb{Q}[X]$

$\exists$ an integer $c \overset{\neq 0}{\in} \mathbb{Z}$, s.t. cq ~~$\in$~~ and $c.h \in \mathbb{Z}[X]$

Then $c = f.(cq) + g.(ch) \in \mathfrak{p}$ ($\lightning$ since $\mathfrak{p} \cap \mathbb{Z} = (0)$)

We get $g | f$ in ~~and~~ $\mathbb{Q}[x]$ and by Gauss lemma $g | f$ in $\mathbb{Z}[X]$.