In the following lecture we will always consider a ring to be commutative and to have a unit.

Definition -1.1

Let R be a ring. A subset $I \subseteq R$ is called an ideal if $I \subseteq R$ is a subgroup with respect to addition and $a \in R$ and $b \in I$ implies $ab \in I$.

Assume just the first property for $I \subseteq R$. So let $I \subseteq R$ be a subgroup with respect to addition. So we get a homomorphism of abelian groups

$$\begin{aligned} \pi : R &\longrightarrow {}^{R}\!\diagup_{I} \\ a &\longmapsto a + I \end{aligned}$$

and the following lemma:

Lemma -1.2

The abelian group R/I carries a ring structure such that π is a ring homomorphism if and only if I is an ideal.

Proof. Assume R/I carries a well defined multiplication such that π is a ring homomorphism. Let now $a \in R$ and $b \in I$. So it follows that

$$\pi(ab) = \pi(a)\pi(b) = (a + I) \cdot (b + I) = (a + I) \cdot (0 + I) = 0 + I$$

and on the other hand $\pi(ab) = ab + I$. Hence $ab \in I$ and I is an ideal.
Conversely if I is an ideal we can define the multiplication structure on R/I by $(x+I)(y+I) = xy+I$. It is easy to check that this definition does not depend on the chosen representatives $x, y \in R$ and that π becomes a ring homomorphism.

□

Example -1.3

For $n \in \mathbb{N}$ the ideal $n\mathbb{Z} \subset \mathbb{Z}$ results in the quotient ring $\mathbb{Z}/n\mathbb{Z}$.

A common quotient ring we will encounter is given by a subset $M \subset k[T_1, \ldots, T_n]$ and the ideal (M). So the smallest ideal in $k[T_1, \ldots, T_n]$, which contains M. The ring is then $k[T_1, \ldots, T_n]/(M)$.

It turns out that this quotient construction satisfies the following universal property:

Lemma -1.4: Universal property of the quotient ring

Let $R \xrightarrow{\varphi} S$ be a ring homomorphism and $I \subseteq R$ be an ideal. If $\varphi(I) = \{0\}$ then there exists a unique ring homomorphism $\overline{\varphi} : R/I \to S$ such that the following diagram commutes:

$$\begin{tikzcd}
R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & S \\
& R/I \arrow[ur, dashed, "\exists!\,\overline{\varphi}"'] &
\end{tikzcd}$$

Proof. We define the morphism $\overline{\varphi}$ by $\overline{\varphi}(a+I) = \varphi(a)$. First it should be mentioned that if $a, b \in R$ with $a - b \in I$ then

$$\overline{\varphi}(b+I) = \varphi(b) + \varphi(a-b) = \varphi(a) = \overline{\varphi}(a+I)$$

and the definition $\overline{\varphi}$ does not depend on representatives. Second it should be checked that $\overline{\varphi}$ is indeed a ring homomorphism. So we compute for $a, b \in R$ that

$$\overline{\varphi}((a+I)+(b+I)) = \overline{\varphi}(a+b+I) = \varphi(a+b) = \varphi(a)+\varphi(b) = \overline{\varphi}(a+I)+\overline{\varphi}(b+I).$$

The computation for multiplication is analogous. Lastly it is easy to see that $\overline{\varphi}(1+I) = \varphi(1) = 1$ and so $\overline{\varphi}$ is a ring homomorphism. The fact that $\varphi = \overline{\varphi} \circ \pi$ immediately follows from the definition. It only remains to check that $\overline{\varphi}$ is unique with this property. Let $\tilde{\varphi} : R/I \to S$ be another ring homomorphism such that $\varphi = \tilde{\varphi} \circ \pi$. Then it follows that

$$\tilde{\varphi}(a+I) = \varphi(a) = \overline{\varphi}(a+I)$$

and hence that $\overline{\varphi}$ is unique.

□

-1.1 Noetherian rings

Definition -1.5

A ring R is called noetherian if every ideal $I \subseteq R$ is finitely generated. That is for every ideal $I \subseteq R$ there exists a finite subset $M \subseteq R$ such that I is the smallest ideal which contains M. We denote this with $I = (M)$.

This definition is characterized by an eqivalent property stated in the following lemma.

Lemma -1.6: Ascending chain condition

A ring R is noetherian if and only if for every ascending chain

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq I_4 \subseteq \cdots$$

of ideals $I_j \subseteq R$ there exists an index $n \in \mathbb{N}$ such that for all $m \geq n$ we have $I_m = I_n$.

Proof. Assume that R is not noetherian and let $I \subseteq R$ be an ideal that is not finitely generated. Then for every finitely generated ideal $I' \subseteq I$ there exists an element $f \in I \setminus I'$. We construct an ascending chain of ideals by defining $I_0 \coloneqq \{0\}$ and for every $n \in \mathbb{N}$ choosing an elemnt $f_n \in I \setminus I_n$ and setting $I_{n+1} \coloneqq (I_n \cup \{f_n\})$. By definition this is an ascending chain of ideals that at no step has an equality.

Assume now that R is noetherian and consider an ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq I_4 \subseteq \cdots .$$

Then the set $I = \bigcup_{n\in\mathbb{N}} I_n$ is an ideal. For $a, b \in I$ there exists an $n \in \mathbb{N}$ such that $a, b \in I_n$ and hence $a + b \in I_n$ which implies $a + b \in I_n$. Similarly if $a \in R$ and $b \in I$ then there is an $n \in \mathbb{N}$ such that $b \in I_n$ and thus $ab \in I_n$ which implies $ab \in I$.

Due to R being noetherian we get that I is finitely generated. Let $\{f_1, \dots, f_n\} \subset I$ be a finite generating set. We then define

$$.m \coloneqq \max\{l \in \mathbb{N} \mid \exists i \in \{1, \dots, n\} : \ f_i \notin I_l\}.$$

Since for every f_i there exists an index $l \in \mathbb{N}$ such that $f_i \in I_l$ this subset of $\mathbb{N}$ is bounded from above and hence contains a largest element. Now from $I_{m+1} \subseteq I$ and $\{f_1, \dots, f_n\} \subseteq I_{m+1}$ follows $I_{m+1} = I$ and hence

$$I_{m+1} = I_{m+2} = I_{m+3} = I_{m+4} = \cdots .$$

□

There are some ways to easily construct noetherian rings out of known noetherian rings. The following lemma gives one such way.

Lemma -1.7

If $R \xrightarrow{\pi} R'$ is a surjective ring homomorphism and R is noetherian then R' is noetherian.

Proof. Let $I \subseteq R'$ be an ideal. Then $\pi^{-1}(I)$ is an ideal and finitely generated by assumption. Let $\{f_1, \dots, f_n\} \subseteq \pi^{-1}(I)$ be a generating set of $\pi^{-1}(I)$. Then we claim that $I = (\pi(f_1), \dots, \pi(f_n))$. Clearly we have $I \supseteq (\pi(f_1), \dots, \pi(f_n))$, since $\pi(f_i) \in I$ is equivalent to $f_i \in \pi^{-1}(I)$. If $f' \in I$ then there exists $f \in R$ with $\pi(f) = f'$ and so $f \in \pi^{-1}(I)$. Therefore f can be written as $f = \sum_{i=1}^{n} g_i f_i$ with some $g_i \in R$. It follows that $f' = \pi(f) = \sum_{i=1} \pi(g_i)\pi(f_i) \in (\pi(f_1), \dots, \pi(f_n))$.

With the equality shown it follows that I is finitely generated.

□

Another way of finding new noetherian rings is given by the following theorem.

Theorem -1.8: Hilbert's basis theorem

If R is noetherian then $R[T]$ is noetherian.

Before we prove the theorem we formulate a few conclusions from the theorem and the previous lemma. Additionally we need a preliminary lemma in the proof of the theorem.

Corollary -1.9

If R is noetherian and $n \in \mathbb{N}$ then $R[T_1, \ldots, T_n]$ is noetherian. If $I \subset R[T_1, \ldots, T_n]$ is an ideal then $R[T_1, \ldots, T_n]/I$ is noetherian.

Proof. The first part of the statement follows from the theorem and induction by n. The second part of the statement follows from the lemma and the first part of the statement. $\square$

Lemma -1.10

Let R be a ring and the ideal $I \subseteq R$ be finitely generated. Let furthermore $M \subseteq I$ be a generating set of I. Then there exists a finite subset $M' \subseteq M$ that generates I

Proof. Let $\{f_1, \ldots, f_m\}$ be a finite generating set for I. Then for every $i \in \{1, \ldots, n\}$ we can write

$$f_i = \sum_{g \in M} b_{ig} g$$

while almost all b_{ig} vanish. So the set

$$M' \coloneqq \{g \in M \mid \exists i \in \{1, \ldots, n\} : \; b_{ig} \neq 0\}$$

is finite and we claim that M' generates I. The inclusion $(M') \subseteq I$ is clear. So assume that $h \in I$. Becuase the f_i generate I it follows that there exist $a_1, \ldots, a_n \in R$ such that

$$h = \sum_{i=1}^{n} a_i f_i = \sum_{i=1}^{n} \sum_{g \in M'} a_i b_{ig} g = \sum_{g \in M'} \left(\sum_{i=1}^{n} a_i b_{ig} \right) g$$

and hence $h \in (M')$ $\square$

Proof of Hilbert's basis theorem. Assume $R[T]$ is not noetherian and let $I \subseteq R[T]$ be an ideal which is not finitely generated. Choose a polynomial $f_1 \in I$ of minimal degree n_1. For every $i \in \mathbb{N}$ choose a polynomial $f_i \in I \setminus (f_1, \ldots, f_{i-1})$ of minimal degree n_i. Note that for $i \leq j$ we get $n_i \leq n_j$. For all $i \in \mathbb{N}$ we denote the leading coefficient of f_i with a_i. Since R is noetherian it follows that $(a_i \mid i \in \mathbb{N}) \subseteq R$ is finitely generated. By Lemma 1.10 there exists an $m \in \mathbb{N}$ such that $(a_1, \ldots, a_m) = (a_i \mid i \in \mathbb{N})$ and in particular there are $b_1, \ldots, b_m \in R$ such that

$$a_{m+1} = \sum_{i=1}^{m} b_i a_i.$$

With that we set

$$g \coloneqq f_{m+1} - \sum_{i=1}^{m} b_i T^{n_{m+1} - n_i} f_i$$

Then we get that the n_{m+1}-th coefficient of g vanishes and hence that g is of lower degree than f_{m+1}. At the same time it must be the case that $g \in I \setminus (f_1, \dots, f_m)$, because if $g \in (f_1, \dots, f_m)$ then

$$f_{m+1} = g + \sum_{i=1}^{m} b_i T^{n_{m+1} - n_i} f_i \in (f_1, \dots, f_m)$$

and that is not the case by the choice of f_{m+1}. But now g being of lower degree than f_{m+1} and $g \in I \setminus (f_1, \dots, f_m)$ contradicts the minimality of n_{m+1}. So the assumption that I is not finitely generated must have been wrong.

$\square$

Remark -1.11

We just showed that $k[T_1, T_2]$ and $\mathbb{Z}[T]$ are noetherian. But even though every ideal I in these rings is finitely generated, we can choose I to require arbitrarily large (finite) generating sets.

Proof. $\square$

-1.2 Units

Definition -1.12

Let R be a ring. We call the elements of the set

$$R^* = \{x \in R \mid \exists y \in R : \ xy = 1\}$$

the units in R.

Remark -1.13

Given $x \in R*$ the corresponding $y \in R$ with $xy = 1$ is unique. We denote this element with x^{-1}.

Proof. Let $y, y' \in R$ with $xy = xy' = 1$. Then we have $y = (xy')y = (xy)y' = y'$. $\square$

Definition -1.14

Let R be a ring. A subset $S \subseteq R$ is called multiplicative if $1 \in S$ and for all $a, b \in S$ it follows that $ab \in S$.

Consider a ring R and a multiplicative subset $S \subseteq R$. The aim is to construct the ring of fractions which have only elements of R as enumerators and elements of S as denominatos.

Lemma -1.15

Define the relation $\sim$ on $R \times S$ by

$$(x, s) \sim (y, t) \quad :\Leftrightarrow \quad \exists u \in S : \; xtu = ysu.$$

Then $\sim$ is an equivalence relation whose equivalence classes we denote by $[(x, s)]_\sim = \frac{x}{s}$.

Proof. Form the definition reflexivity and symmetry are clear. Transitivity requires a short calculation. Let $(x, s) \sim (y, t)$ and $(y, t) \sim (z, u)$. so there exist $a, b \in S$ with $xta = ysa$ and $yub = ztb$. It follows that

$$xu(tab) = xta(ub) = ysa(ub) = yub(sa) = ztb(sa) = zs(tab)$$

and so with $tab \in S$ we get $(x, s) \sim (z, u)$. $\square$

Lemma -1.16

For a ring R and a multiplicaive subset $S \subseteq R$ we denote with

$$S^{-1}R = \left\{ \frac{x}{s} \mid x \in R, \; s \in S \right\}$$

the set of equivalence classes from the previous lemma. On this set we define an addition and a multiplication by

$$\frac{x}{s} + \frac{y}{t} = \frac{xt + ys}{st}$$

and

$$\frac{x}{s} \cdot \frac{y}{s} = \frac{xy}{st}$$

respectively. Then $S^{-1}R$ together with thes operations is a ring which we call the localization of R by S.

Proof. It is clear that the addition an multiplication are commutative and associative. Furthermore it is easy to see that $\frac{0}{1}$ is a neutral element with respect to addition and $\frac{1}{1}$ is neutral with respect to multiplication. It remains to check thhat both operations are well-defined and that multiplicaton distributes over addition. Let $(x, s) \sim (x', s')$ and $(y, t) \sim (y', t')$. So there are $u, v \in S$ such that $xs'u = x'su$ and $yt'v = y'tv$. Then we get

$$\frac{x}{s} + \frac{y}{t} = \frac{xt + ys}{st} = \frac{xts't'uv + yss't'uv}{sts't'uv} = \frac{x'sutt'v + y'tvss'u}{sts't'uv} = \frac{x't' + y's'}{s't'} = \frac{x'}{s'} + \frac{y'}{t'}$$

and similarly we compute

$$\frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st} = \frac{xs'uyt'v}{sts't'uv} = \frac{x'suy'tv}{sts't'uv} = \frac{x'y'}{s't'} = \frac{x'}{s'} \cdot \frac{y'}{t'}.$$

To check the distributivity let $x, y, z \in R$ and $s, t, u \in S$. Then we get

$$\frac{x}{s}\left(\frac{y}{t}+\frac{z}{u}\right)=\frac{x(yu+zt)}{stu}=\frac{xyu+xzt}{stu}=\frac{xyus+xzts}{s^2tu}=\frac{xy}{st}+\frac{xz}{su}=\frac{x}{s}\frac{y}{t}+\frac{x}{s}\frac{z}{u}.$$

□

We get that the localization satisfies a universal property.

Lemma -1.17: Universal property of the localization

For a ring R and a multiplicative subset $S \subseteq R$ consider the ring homomorphism

$$\begin{aligned} j : R &\longrightarrow S^{-1}R \\ x &\longmapsto \frac{x}{1} \end{aligned}$$

If $\varphi : R \to R'$ is a ring homomorphism such that $\varphi(S) \subseteq (R')^*$ then there exists a unique ring homomorphism $\overline{\varphi} : S^{-1}R \to R'$ such that the diagram

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "j"'] & & R' \\ & S^{-1}R \arrow[ur, dashed, "\exists!\,\overline{\varphi}"'] & \end{tikzcd}$$

commutes.

Proof. First we construct the homomorphism $\overline{\varphi}$. Since for every $s \in S$ the image $\varphi(s)$ is invertible in R' we define

$$\overline{\varphi}\left(\frac{x}{s}\right)=\varphi(x)\varphi(s)^{-1}.$$

Then clearly

$$\varphi(x)=\varphi(x)\varphi(1)^{-1}=\overline{\varphi}\left(\frac{x}{1}\right)=\overline{\varphi}(j(x)).$$

Futhermore it follows immediately form the fact that φ is a ring homomorphism that $\overline{\varphi}$ is also one. It remains to check that φ is well-defined. Let $(x, s) \sim (x', s')$ by the element $u \in S$. Then we get

$$\overline{\varphi}\left(\frac{x}{s}\right)=\varphi(x)\varphi(s)^{-1}=\varphi(xs'u)\varphi(ss'u)^{-1}=\varphi(x'su)\varphi(ss'u)^{-1}=\varphi(x')\varphi(s')^{-1}=\overline{\varphi}\left(\frac{x'}{s'}\right).$$

Let $\tilde{\varphi}$ be another homomorphism that makes the diagram commute. Then it follows that

$$\overline{\varphi}\left(\frac{x}{s}\right)=\varphi(x)\varphi(s)^{-1}=\tilde{\varphi}\left(\frac{x}{1}\right)\tilde{\varphi}\left(\frac{s}{1}\right)^{-1}=\tilde{\varphi}\left(\frac{x}{1}\right)\tilde{\varphi}\left(\frac{1}{s}\right)=\tilde{\varphi}\left(\frac{x}{s}\right).$$

□

Similarly to the quotient ring the localization also preserves the property of being noetherian.

Lemma -1.18

If R is a noetherian ring and $S \subseteq R$ is a multiplicative subset then $S^{-1}R$ is noetherian.

Proof. From Hilbert's basis theorem it follows that $R[T]$ is noetherian. Considering the surjective homomorphism $R[T] \to S^{-1}R$, which sends constants $x \in R[T]$ to x and sends T to $\frac{1}{s}$ we get that $S^{-1}R$ is noetherian. $\square$

-1.3 Prime ideals and maximal ideals

Definition -1.19

Let R be a ring. An ideal $I \subseteq R$ is called a prime ideal if the quotient ring R/I is a domain.

We have the following equivalent characterization of prime ideals:

Lemma -1.20

Let R be a ring. An ideal $I \subseteq R$ is a prime ideal if and only if for all $a, b \in R$ with $ab \in I$ it follows $a \in I$ or $b \in I$.

Proof. Let first R/I be a domain and $a, b \in R$ be such that $ab \in I$. Then it follows that in the quotient R/I we have $(a+I)(b+I) = ab + I = 0 + I$ and because R/I is a domain it follows that $a + I = 0 + I$ or $b + I = 0 + I$. Hence $a \in I$ or $b \in I$.

Conversely assume that $I \subseteq R$ is a prime ideal and let $(a+I)(b+I) = 0 + I$. So it follows that $ab \in I$ and because I is prime we have $a \in I$ or $b \in I$. So $a + I = 0 + I$ or $b + I = 0 + I$ making R/I a domain.

$\square$

Definition -1.21

Let R be a ring. An ideal $I \subseteq R$ is called maximal if $I \neq R$ and for all ideals $J \subseteq R$ with $I \subseteq J$ it follows that $J = I$ or $J = R$.

Remark -1.22

For any ideal $I \subseteq R$ the projection homomorphism

$$\begin{aligned} \pi : R &\longrightarrow {}^{R}\!/\!_{I} \\ x &\longmapsto x + I \end{aligned}$$

induces a bijection between the set of ideals $J \subseteq R$ with $I \subseteq J$ and the set of ideals of the quotient ring R/I. This happens by mapping an ideal $\overline{J} \subseteq R/I$ to $\pi^{-1}(\overline{J})$. It is easy to check that this is a homomorphism and that the inverse map is given by mapping an ideal $I \subseteq J \subseteq R$ to $\pi(J)$, which is an ideal because the projection is surjective.

This remark becomes useful in formulating the following important characterization of maximal ideals.

Lemma -1.23

Let R be a ring and $I \subseteq R$ be an ideal. Then I is maximal if and only if the quotient ring R/I is a field.

Proof. Assume that I is maximal. This is the case if and only if there only exist two ideals $J \subseteq R$ with IJ. By the previous remark this is equivalent to R/I only having two ideals, which must be $(0), (1) \subseteq R/I$. This is the case if and only if R/I is a field. $\square$

Theorem -1.24

If R is a ring and $R \neq 0$ then R contains a maximal ideal.

Proof. Let $\mathcal{M}$ be the set of all ideals $I \subseteq R$, which are not R itself. Then we get that $M \neq \varnothing$ $\square$