Aim Introduce maximal ideals, PIDs, prime factorization and power series rings.

§1 Fields

Lem 1 A ring.

1) For ideal $\mathfrak{a} \subseteq A$: $\mathfrak{a} = A \iff 1 \in \mathfrak{a} \iff \exists$ unit $u \in \mathfrak{a}$.

2) For $x \in A$: $x \in A^\times \iff (x) = A$.

Proof 1) $\Rightarrow$ immediate. $\Leftarrow$ Assume $u \in \mathfrak{a}$ is a unit, $a \in A$ arbitrary.

Then $au^{-1} \cdot u \in \mathfrak{a}$ (ideal property)

2) $(x) = A \overset{1)}{\iff} 1 \in (x) \iff$ Can write $1 = x \cdot y$

$\iff x \in A^\times$. $\square$

Recall A field $\underset{\text{def}}{\iff}$ $A \neq 0$ & $A^\times = A \setminus \{0\}$.

Lem 2 $A \neq 0$ ring. Then

A field $\iff$ $(0), A$ only ideals in A

Proof $\Rightarrow$ Let $\mathfrak{a} \subseteq A$ ideal, $0 \neq x \in \mathfrak{a}$. Then $(x) \subseteq \mathfrak{a}$.

A field $\Rightarrow$ $(x) = A$ (by Lem 1) $\Rightarrow$ $\mathfrak{a} = A$.

$\Leftarrow$ If $0 \neq x \in A$, then $(x) \neq 0$, hence $(x) = A$,

hence $x \in A^\times$. $\square$

Defn An ideal $\mathfrak{m} \subseteq A$ *maximal* $\overset{=}{\text{def}}$ $\mathfrak{m} \neq A$ and no ideal $\mathfrak{a}$ satisfies $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq A$.

Cor 3 $\mathfrak{m} \subset A$ maximal $\iff$ $A/\mathfrak{m}$ is a field.

Proof Let $\mathfrak{a} \subset A$ any ideal, let $\pi : A \to A/\mathfrak{a}$ projection map.

Then $\{\text{ideals } \bar{\mathfrak{b}} \subseteq A/\mathfrak{a}\} \xleftrightarrow{1:1} \{\text{ideals } \mathfrak{a} \subseteq \mathfrak{b} \subseteq A\}$

$$\bar{\mathfrak{b}} \longmapsto \pi^{-1}(\bar{\mathfrak{b}}) \qquad (\ast)$$

$$\pi(\mathfrak{b}) = \mathfrak{b}/\mathfrak{a} \longleftarrow \mathfrak{b}$$

Thus 1st $\mathfrak{m} \neq A \iff A/\mathfrak{m} \neq 0$

2nd For $\mathfrak{m} \neq A$: $\nexists\, \mathfrak{m} \subsetneq \mathfrak{a} \subsetneq A \iff \nexists\, (0) \subsetneq \bar{\mathfrak{a}} \subsetneq A/\mathfrak{m}$

$\overset{\text{Lem 2}}{\iff} A/\mathfrak{m}$ field. $\square$

§2 PIDs

Def <u>Principal ideal domain (PID)</u> $\underset{def}{=}$ integral domain A s.th. every ideal $\mathfrak{a} \subseteq A$ is <u>principal</u>, i.e. $\mathfrak{a} = (f)$ for some $f \in A$.

<u>Examples</u> 1) $\mathbb{Z}$, $K[T]$ with K field

2) $A := \mathbb{C}[\varepsilon]/(\varepsilon^2)$ is no integral domain.

<u>Claim</u> The ideals in A are (0), $(\bar{\varepsilon})$, A where $\bar{\varepsilon} = \varepsilon + (\varepsilon^2)$ residue class of ε.

<u>Proof</u> First note that $A^\times = \{a + b\bar{\varepsilon} \mid a \in \mathbb{C}^\times\}$.

Namely $(a+b\bar{\varepsilon})(a-b\bar{\varepsilon}) = a^2$ shows $\supseteq$ while the implication

$$\left(1 = (a+b\bar{\varepsilon})(c+d\bar{\varepsilon}) = ac + (ad+bc)\bar{\varepsilon} \implies \begin{cases} ac = 1 \\ ad+bc = 0 \end{cases}\right)$$

shows $\subseteq$.

Now let $0 \neq \mathfrak{a} \subseteq A$ ideal. If there is $a+b\bar{\varepsilon} \in \mathfrak{a}$, $a \neq 0$, then $\mathfrak{a} = A$ by Lem 1. O/w, $\mathfrak{a} = \{b\bar{\varepsilon}\} = (\bar{\varepsilon})$. $\square$

Def A <u>principal ideal ring</u> $\underset{def}{=}$ ring A s.th. any ideal $\mathfrak{a} \subseteq A$ is principal.

Lem 4 A integral domain, $f, g \in A$. Then

$$(f) = (g) \iff \exists \text{ unit } u \text{ s.th. } g = u \cdot f.$$

Proof $\Rightarrow$ $(f) = (g)$ means we can write $g = uf$, $f = v \cdot g$ with $u, v \in A$.

Then $f = u \cdot v \cdot f$, which implies $(1 - uv) \cdot f = 0$

A integral domain $\Rightarrow$ $f = 0$ or $(1 - uv) = 0$.

In first case also $g = 0$, so $f = 1 \cdot g$.

In second case, $uv = 1$, so u a unit.

$\Leftarrow$ If $g = u \cdot f$ w/ u unit, then $f = u^{-1} g$.

Thus $f \in (g)$ and $g \in (f)$, so $(f) = (g)$. $\square$

In ptic A PID. Then $\{\text{ideals in } A\} \xrightarrow{1:1} A/A^\times$.

$$(f) \longleftarrow\!\mapsto f$$

Examples Every $\mathfrak{a} \subseteq \mathbb{Z}$ uniquely of form $n \cdot \mathbb{Z}$ w/ $n \geq 0$

Every $\mathfrak{a} \subseteq K[T]$ uniquely of form (f), f <u>monic</u>.

Defn A integral domain. $p \in A$ <u>prime</u> $\overset{=}{\text{def}}$

$$p \neq 0,\ p \notin A^\times \ \&\ p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

<u>Thm 5</u> A a PID, $0 \neq f \in A$. Then there exists a unit $u \in A^\times$, prime elements $p_1, \dots, p_r \in A$ and exponents $e_1, \dots, e_r \geq 1$ s.th.

$$f = u \cdot p_1^{e_1} \cdots p_r^{e_r} \quad \text{(Prime factorization of } f\text{.)}$$

Furthermore, we may assume that $p_i \nmid p_j$ if $i \neq j$, in which case the pairs (p_i, e_i) are unique up to reordering and up to replacing p_i by $u_i \cdot p_i$ with $u_i \in A^\times$.

<u>Proof</u> We need some auxiliary statements first, that are however interesting in themselves.

<u>Step 0</u> If $f \in A^\times$, then $f = f$ is the unique prime factorization. (If $p \mid f$, then $p \mid f f^{-1} = 1$, so p is a unit and hence no prime element.)

Thus from now on $f \notin A^\times$.

Step 1 Given $f \in A \setminus A^\times$, there exists a maximal ideal $\mathfrak{m}$ with $f \in \mathfrak{m}$.

Proof •) Define a chain of ideals as follows:

$$\mathfrak{a}_0 = (f), \quad \mathfrak{a}_{i+1} = \begin{cases} \mathfrak{a}_i & \text{if } \mathfrak{a}_i \text{ maximal} \\ \text{s.th. } \mathfrak{a}_i \subsetneq \mathfrak{a}_{i+1} \subsetneq A & \text{otherwise} \end{cases}$$

Note $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$

•) The union $\mathfrak{b} = \bigcup_{i \geq 0} \mathfrak{a}_i$ is again an ideal (check this!)

A PID $\Longrightarrow$ Can write $\mathfrak{b} = (g)$.

•) Then $g \in \mathfrak{a}_i$ for some i and thus

$$(g) \subseteq \mathfrak{a}_i \subseteq \mathfrak{b} = (g), \quad \text{so}$$

$\mathfrak{a}_i = \mathfrak{a}_{i+1} = \cdots$. This means that $\mathfrak{a}_i$ is maximal.

$\square$ Step 1.

<u>Step 2</u> Let $\mathfrak{m} = (p)$ be an ideal in PID A.

Assume $\mathfrak{m} \neq 0$. Then $\mathfrak{m}$ maximal $\iff$ p prime element.

<u>Proof</u> $\Rightarrow$ •) $\mathfrak{m} \neq 0$ + maximal $\Rightarrow$ $p \neq 0$, $p \notin A^{\times}$.

•) Assume $p \mid ab$. This means $\overline{ab} = 0$ in $A/\mathfrak{m}$.

$A/\mathfrak{m}$ is a field (by Cor 3), so this implies

$\overline{a} = 0$ or $\overline{b} = 0$, hence $a \in \mathfrak{m}$ or $b \in \mathfrak{m}$

which means $p \mid a$ or $p \mid b$. Hence p is prime.

$\Leftarrow$ •) Assume $(p) \subseteq \mathfrak{n}$ is a maximal ideal

that contains p (use Step 1). We want to

see $(p) = \mathfrak{n}$.

•) A PID $\Rightarrow$ Can write $\mathfrak{n} = (q)$. By first half

of this proof, q is prime. By the Lem 6

below, $(p) = (q)$ and we are done. $\square$

Lem 6 A integral domain, $p, q \in A$ prime elements s.th. $p \mid q$. Then also $q \mid p$, meaning $q = \text{unit} \cdot p$.

Proof $p \mid q$ means we may write $q = x \cdot p$.

Then q prime implies $q \mid x$ or $q \mid p$.

Claim $q \mid x$ impossible.

Indeed, $x = q \cdot y$ implies $q = q \cdot y \cdot p$, hence $(1 - yp) \cdot q = 0$. Since A is integral domain, this implies $1 = yp$. But p is not a unit by assumption, so this is impossible, proving the claim $\square$

We conclude that $q \mid p$. Lem 4 now implies $q = \text{unit} \cdot p$ as stated $\square$

Step 3 Given $0 \neq f \in A \setminus A^\times$, there exists a prime factorization as in the theorem.

<u>Proof</u> Similar to Step 1, define a sequence of elements in the following way:

$$f_0 = f, \quad f_{i+1} = \begin{cases} f_i & \text{if } f_i \in A^\times \\ f_i/p_i & \text{if } f_i \notin A^\times \text{ and if} \end{cases}$$

(p_i) is a max. ideal that contains f_i
(use Step 1)

As in Step 1, the chain

$$(f_0) \subseteq (f_1) \subseteq (f_2) \subseteq \dots$$

becomes stationary. Say $(f_{n-1}) \subsetneq (f_n) = (f_{n+1})$.

Then $f_n \in A^\times$ (by defn. of the sequence of f_i),

$$f = f_n \cdot p_0 \cdots p_{n-1},$$

and the p_i are prime (Step 2).

Using Lem 6, we group the p_i w.r.t. the equivalence relation $p_i \sim p_j$ if $p_i \mid p_j$.

$$\Longrightarrow \quad f = u \cdot (p_1')^{e_1} \cdots (p_r')^{e_r} \quad \text{with } p_i' \nmid p_j' \text{ if } i \neq j.$$

Step 4 Uniqueness as claimed in theorem.

Assume $u \cdot p_1^{e_1} \cdots p_r^{e_r} = v \cdot q_1^{f_1} \cdots q_s^{f_s}$.

Induct over $\sum_{i=1}^{r} e_i =: n$.

·) If $n = 0$, i.e. $u = v \cdot q_1^{f_1} \cdots q_s^{f_s}$, then all factors on RHS are units, hence $s = 0$.

·) If $n > 0$, using prime property of p_1, there is $1 \leq j \leq s$ s.th. $p_1 \mid q_j$. By Lem 6, this means $q_j = w \cdot p_1$ for some $w \in A^\times$.
As A is an integral domain, we may divide by p_1 and obtain

$$u p_1^{e_1 - 1} p_2^{e_2} \cdots p_r^{e_r} = v \cdot w \cdot q_1^{f_1} \cdots q_j^{f_j - 1} \cdots q_s^{f_s}$$

Now conclude by induction. $\square$ Thm

Cor 7 A a PID, not a field. Then

$$\{\text{max ideals} \subset A\} \xrightarrow{1:1} \{\text{prime elements } p \in A\}/A^\times$$

$$(p) \longmapsto p$$

Defn A any ring, $\mathfrak{a}, \mathfrak{b} \subseteq A$ ideals.

Sum: $\mathfrak{a} + \mathfrak{b} \underset{def}{=} \{a+b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} = (\mathfrak{a} \cup \mathfrak{b})$

Product: $\mathfrak{a} \cdot \mathfrak{b} \underset{def}{=} (a \cdot b \mid a \in \mathfrak{a}, b \in \mathfrak{b})$

Cor 8 In a PID, we can define the greatest common divisor (gcd) and the least common multiple (lcm) of any two non-zero elements.

They satisfy:

$$(f) \cdot (g) \overset{(*)}{=} (f \cdot g)$$

$$(f) + (g) = (\gcd(f,g))$$

$$(f) \cap (g) = (\operatorname{lcm}(f,g))$$

Rmk $(*)$ in fact true in any ring.

§3 Power series

A any ring.

$$A[\![T]\!] := \prod_{i=0}^{\infty} A \cdot T^i = A^{\mathbb{Z}_{\geq 0}}$$ <u>power series</u> <u>ring over A</u>

$$= \left\{ \text{possibly infinite expressions } \sum_{i=0}^{\infty} a_i \cdot T^i \right\}$$

<u>Rmk</u> 1) The difference between the infinite direct sum $\bigoplus_{i=0}^{\infty} A \cdot T^i$ and the infinite product $\prod_{i=0}^{\infty} A \cdot T^i$ is that in the former all but fin many coefficents are required to vanish.

2) One may define $A[\![T_1, \dots, T_{n-1}, T_n]\!] := A[\![T_1, \dots, T_{n-1}]\!][\![T_n]\!]$

and $$A[\![T_i, i \in I]\!] = \bigcup_{J \subseteq I \text{ finite}} A[\![T_j, j \in J]\!]$$

just as with polynomial rings.

3) If A is reduced (resp. integral domain), then $A[\![T_i, i \in I]\!]$ is so as well.

Prop 9 A power series $f = \sum_{i \geq 0} a_i T^i \in A[\![T]\!]$ is a unit $\iff$ $a_0 \in A^\times$ is a unit.

Proof $\Rightarrow$ $(a_0 + a_1 T + \ldots)(b_0 + b_1 T + \ldots) = a_0 b_0 +$ higher terms,

so $A[\![T]\!] \to A$, $\sum_{i \geq 0} a_i T^i \mapsto a_0$ is a

ring map. Then it sends units to units.

$\Leftarrow$ Assume a_0 is a unit. To show: f is a unit.

Equivalently, $a_0^{-1} f$ is a unit, so we may assume $f = 1 - g \cdot T$ with $g \in A[\![T]\!]$.

The elements $h_n := 1 + gT + (gT)^2 + \cdots + (gT)^n \in A[\![T]\!]$

have the following properties:

$\cdot)$ $h_n \equiv h_{n+1} \mod (T^{n+1})$ i.e. the coefficients in degrees $0, 1, \ldots, n$ agree.

$\cdot)$ $h_n \cdot f = 1 - (gT)^{n+1}$.

Let h_∞ be the power series with $h_\infty \equiv h_n \mod (T^{n+1})$ $\forall n$

<u>Claim</u> $h_\infty \cdot f = 1$.

<u>Proof</u> Can write $h_\infty = h_n + \varepsilon_n \cdot T^{n+1}$. Thus

$$h_\infty \cdot f = (h_n + \varepsilon_n T^{n+1}) f = 1 - (gT)^{n+1} + \varepsilon_n \cdot f \cdot T^{n+1}$$
$$\equiv 1 \mod (T^{n+1}).$$

This holds for all n, meaning $h_\infty \cdot f - 1 \in \bigcap_{n \geq 1} (T^n)$.

But $\bigcap_{n \geq 0} (T^n) = (0)$, so $h_\infty \cdot f = 1$. $\square$

<u>Example</u> •) $(1-T)^{-1} = 1 + T + T^2 + T^3 + \ldots$

•) $(1+T)^{-1} = 1 - T + T^2 - T^3 \pm \ldots$

•) $F(T) = 1 + T + 2T^2 + 3T^3 + 5T^4 + \ldots$ Fibonacci

Then $F(T) = T F(T) + T^2 F(T) + 1$

$$\Rightarrow (1 - T - T^2)^{-1} = F(T)$$

<u>Exercise</u> Prove that $1 + T \in \mathbb{Q}[\![T]\!]^\times$ has a square root.

Prop 10 K field. The ideals of $K[\![T]\!]$ are (0) and (T^n), $n \geq 1$.

In ptic, $K[\![T]\!]$ is a PID w/ unique (up to unit) prime element T. Its unique max ideal is (T).

Proof If $\mathfrak{a} \neq (0)$, let $0 \neq f = \sum_{i=n}^{\infty} a_i \cdot T^i$ with $a_n \neq 0$

be s.th. n is minimally possible. Then $f = T^n \cdot$ unit

by Prop 9. Moreover, $T^n \mid g$ $\forall g \in \mathfrak{a}$ by minimality,

so $\mathfrak{a} = (T^n)$. Clearly, (T) is maximal. $\square$

Defn A ring. Jacobson radical $\underset{def}{=}$ $\mathrm{Jac}(A) = \bigcap_{\substack{\mathfrak{m} \subset A \\ \text{max ideal}}} \mathfrak{m}$.

Ex $\mathrm{Jac}(K[\![T]\!]) = (T)$.

$\mathrm{Jac}(\mathbb{Z}) = (0)$, $\mathrm{Jac}(K[T]) = (0)$

$\mathrm{Jac}(\mathbb{C}[\varepsilon]/(\varepsilon^2)) = (\varepsilon)$.