Section 3 UFD

Defn A: int dom, $x \in A$

① Call x reducible if $\exists\, a, b \in A$, $a, b \notin A^\times$ (units of A) s.t. $x = ab$; otherwise, call it irreducible.

② Call x a prime element, if $x \mid ab \Rightarrow x \mid a$ or $x \mid b$.
($\Leftrightarrow (x)$ is prime ideal).

Lem 3.1: prime $\Rightarrow$ irred.

Pf: easy.

Rmk: irred $\not\Rightarrow$ prime. In $\mathbb{Z}[\sqrt{-5}]$, 2 is irred, but $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$, so 2 is NOT prime.

In fact: $(2) = (1+\sqrt{-5}, 2)^2$

obvs LHS $\supseteq$ RHS, but RHS $\ni (1+\sqrt{-5})(1-\sqrt{-5}) - 2 \cdot 2 = 2$

Defn A is called UFD (unique factorization domain), if $\forall x \in A$ can be written as $x = p_1 \cdots p_n$ for some $n \geq 0$ where p_i are irreducible elts., and the representation is unique in the sense that if $x = q_1 \cdots q_m$ with q_j irred, then $m = n$, and $\exists$ bijective map $\varphi: \{1, \dots, n\} \to \{1, \dots, m\}$, s.t. $p_i = q_{\varphi(i)} \cdot u_i$ with some $u_i \in A^\times$.

Ex: $\mathbb{Z}$.

$\mathbb{Z}[T]$ (nontrivial, but not too difficult, try prove it yourself).

Thm 3.2: PID $\Rightarrow$ UFD

first, a Lemma

Lem 3.3: A: PID, $x \in A$, TFAE:

(1) (x) prime ideal
(2) (x) max ideal
(3) x irred elt
(4) x prime elt

Pf. (1) $\Leftrightarrow$ (2) ✓

$\Updownarrow$ Lem 3.1 $\Uparrow$ easy.

(4) $\Rightarrow$ (3) □

Pf of Thm 3.2 : Part 1 : representation, i.e., $\forall x$ can be written as $\prod_{i=1}^{n} p_i$

① first, we show $\exists$ irred elt $p \in A$, s.t. $p \mid x$.

If x irred, then $p = x$

If x red $\Rightarrow x = a_1 b_1$, $a_1, b_1 \notin A^\times$

If a_1 irred, then $p = a_1$

if not $x = a_2 b_2 b_1$, $a_2, b_2 \notin A^\times$

iterate, get $(a_1) \subsetneq (a_2) \subsetneq (a_3) \cdots$

thus stops after finite steps. (Noetherian)

② Now $x = p_1 b$, then. similarly (b is reducible) $b = p_2 b_2$, $b_2 = p_3 b_3 \cdots$

$\Rightarrow x = p_1 b = p_1 p_2 b_2 = p_1 p_2 p_3 b_3 \cdots$

again $(b) \subsetneq (b_2) \subsetneq (b_3) \subsetneq \cdots$

thus stops at finite step $\Rightarrow x = \prod_{i=1}^{n} p_i$.

Part 2 : uniqueness of representation.

If $x = p_1 \cdots p_n = q_1 \cdots q_m$, WLOG, $n \le m$.

p_1 irred $\Leftrightarrow$ prime, thus $p_1 \mid q_j$ for some j WLOG, $j = 1$.

$\Rightarrow q_1 = p_1 u_1$ with $u_1 \in A^\times$ since q_1 irred.

$\Rightarrow p_1 \cdots p_n = p_1 u_1 q_2 \cdots q_m \Rightarrow p_2 \cdots p_n = u_1 q_2 \cdots q_m$

iterate: get $1 = u_1 u_2 \cdots u_n q_{n+1} \cdots q_m$

$\Rightarrow n = m$, and $p_i = q_i u_i$. □

Summary: Euclidean $\Rightarrow$ PID $\Rightarrow$ Dedekind $\Rightarrow$ int closed

PID $\Downarrow$ UFD

Dedekind $\Rightarrow$ Noeth

Dedekind $\Rightarrow$ dim = 1

Cor 3.4 A: PID, then for (a) nonzero ideal, $(a) = \prod_{i=1}^{h} (p_i)^{\alpha_i}$ with (p_i) distinct prime ideals with $\alpha_i \geq 1$ integers. The expression is unique, i.e.
if $(a) = \prod_{i=1}^{n} (p_i)^{\alpha_i} = \prod_{j=1}^{m} (q_j)^{\beta_j}$, then $n = m$,
and after reordering $(p_i)^{\alpha_i} = (q_j)^{\beta_j}$.

Pf: By Thm 3.3. $a = \prod_{i=1}^{N} t_i$ with t_i irred elt
$\Rightarrow (a) = \prod (t_i)$ □.

Define fractional ideals for later use.

Defn: A: int dom, $K = \mathrm{Frac}\, A$. $I \subseteq K$ an A-submod,
If $\exists\ d \in A - \{0\}$, s.t. $d \cdot I \subseteq A$, then call I a fractional ideal.

Ex. ① $I \subseteq A$ ideal (called integral ideals) $d = 1$.
② $A = \mathbb{Z}$. $I = \frac{1}{2}\mathbb{Z}$, $d = 2$ (careful, no mult in I, $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4} \notin I$)
③ I: fin. gen A-mod, Since $I = \sum_{i=1}^{n} A e_i$, $e_i \in K$,
if $d_i e_i \in A$, then let $d = \prod_{i=1}^{n} d_i$. $\Rightarrow dI \subseteq A$.

④ Conversely if A is Noeth ring, any frac ideal $I \subseteq K$ is fin. gen over A. Indeed $dI \subseteq A \Rightarrow I \subseteq \frac{1}{d}A$.
$\frac{1}{d}A$ fin gen $\Rightarrow \frac{1}{d} \cdot A$ Noeth A-mod $\Rightarrow I$ fin gen

⑤. If $I_1, I_2 \subseteq K$ frac ideals, then so are $I_1 I_2$, $I_1 \cap I_2$, $I_1 + I_2$.
In particular, nonzero frac ideals of A form a commutative monoid under multiplication

⑥ A. PID, then $a \in K = \mathrm{Frac}\, A$. $\Rightarrow A \cdot a$ is frac ideal, since $a = \frac{c}{d}$, then $d\, A \cdot a \subseteq A$
Conversely, $I \subseteq K$ frac ideal, $d \cdot I \subseteq A$ ideal $\Rightarrow d \cdot I = (c) \Rightarrow I = \frac{(c)}{d}$
$\Rightarrow I = A \cdot \frac{c}{d}$

Section 4. Ideal decomposition in Dedekind domains

Thm 4.1. (Main Thm on decomposition of Dedekind domains)

A: Dedekind dom. $P = \{\mathfrak{p}, \mathfrak{p} \subseteq A$ nonzero prime ideals$\}$. Then:

(a) If β is nonzero frac ideal of A, then $\beta = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_{\mathfrak{p}}(\beta)}$ uniquely, where $n_{\mathfrak{p}}(\beta) \in \mathbb{Z}$, nonzero for fin. many $\mathfrak{p} \in P$.

(b) The monoid of non-zero frac ideals of A is a group.

Lem 4.2. A: Noeth ring. (including (0)!)

(1) any $I \subseteq A$ ideal contains a product of prime ideals

(2) If A furthermore int dom, then any $(0) \neq I \subseteq A$ contains a product of nonzero prime ideals.

Pf: Only prove (2) (1) is similar).

Let $Q = \{I \subseteq A, I \neq (0), I$ does NOT contain prod of prime ideals$\}$

WANT: Q is empty. If not, then since A Noeth $\Rightarrow \exists$ max element $\beta \in Q$.

β not prime $\Rightarrow \exists\, x, y \in A \setminus \beta,\ xy \in \beta$

$\Rightarrow \beta + A \cdot x,\ \beta + A \cdot y \notin Q$

$\Rightarrow \beta + A \cdot x \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n,\quad \beta + A \cdot y \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_m$

$\Rightarrow \beta \supseteq (\beta + A \cdot x)(\beta + A \cdot y) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m$. Contradiction. $\square$

Lem 4.3: A Dedekind dom. $m \in A$ max ideal.

Let $m' = \{x \in K \mid xm \subseteq A\}$

Then m' is a frac ideal, $m' \supsetneq A$, and $m \cdot m' = A$.

Pf: Clearly m' is A-mod and $A \subseteq m'$.

Take any $d \in m$, then $dm' \subseteq A$, $\Rightarrow m'$ is frac ideal.

*Let us show $m' \neq A$., i.e. $\exists\, x \in K \setminus A$, $x \in m'$.

Let $a \in m \setminus \{0\}$, $\neq$

Lem 4.2 $\Rightarrow A \cdot a \supseteq p_1 \cdots p_n$ prod of prime ideals. Take a minimal n. ($\because$)

$\Rightarrow m \supseteq A \cdot a \supseteq p_1 \cdots p_n \Rightarrow m \supseteq p_i$ for some i, WLOG, $i=1$.

$\Rightarrow m = p_1$ (p_1 is max in A)

Let $\beta = p_2 \cdots p_n$ (possibly $= A$, i.e. $n=1$)

Then $Aa \supset m\beta$, but $A \cdot a \not\supseteq \beta$ (n is minimal))

$\Rightarrow \exists\, b \in \beta$, $b \notin A \cdot a$

$\Rightarrow \frac{b}{a} \in K \setminus A$, and $Aa \supset m\beta \supset mb \Rightarrow A \supseteq m \cdot \frac{b}{a} \Rightarrow \frac{b}{a} \in m'$.

*Finally, let us show $m \cdot m' = A$

Note $1 \in m' \Rightarrow m \subseteq mm' \subseteq A$

It suffices to show $m \neq mm'$.

If otherwise, take any $x \in m'$, $\Rightarrow xm \subseteq m \Rightarrow x^2 m \subseteq xm \subseteq m$.

$\Rightarrow \forall\, d \in m$, $d \cdot x^n \in m$, $\forall n$.

$\Rightarrow A[x] \subseteq K$ is a frac ideal.

$d \cdot A[x] \subseteq A \Rightarrow A[x] \subseteq \frac{1}{d} A \Rightarrow A[x]$ is fin gen A-mod

$\Rightarrow x$ is int over A! $\Rightarrow x \in A$ (A int closed)!

i.e. any $x \in m' \Rightarrow x \in A$, contradicting $m' \supsetneq A$! $\square$

Defn: Denote $m^{-1} := m'$ above. (the inverse frac ideal)

Pf of Thm 4.1:

Step 1: "existence" in (a): i.e. for β, can write $\beta = \prod \mathfrak{p}^{n_{\mathfrak{p}}(\beta)}$

Since $\exists\, d \in A$, $d\beta \subseteq A \Rightarrow \beta = (d\beta)\cdot(Ad)^{-1}$, so can assume β is integral.

Similar as in Lem 4.2.

Let $\Phi := \{ I \subseteq A$ ideals, I can NOT be written as a fin. prod. of prime ideals $\}$.

If Φ nonempty $\Rightarrow \exists$ max elt. α. Since $A = \prod \mathfrak{p}^0$, thus $\alpha \subsetneq A$.

Suppose $\alpha \subseteq \mathfrak{p}$ some max ideal, Let $\mathfrak{p}' = \mathfrak{p}^{-1}$ as in Lem 4.3

Then recall $\mathfrak{p}' \supsetneq A$, and $\mathfrak{p}\mathfrak{p}' = A$.

Claim: $\alpha\mathfrak{p}' \supsetneq \alpha$

Pf: obv $\alpha\mathfrak{p}' \supseteq \alpha$.

If $\alpha\mathfrak{p}' = \alpha$, Then by same argument as in Lem 4.3, can show $\mathfrak{p}' = A$:

(indeed, take any $x \in \mathfrak{p}'$, then $x\alpha \subseteq \alpha$, $x^2\alpha \subseteq x\cdot x\alpha \subseteq x\alpha \subseteq \alpha$ ...

$\Rightarrow \forall\, d \in \alpha$, $d\cdot A[x] \subseteq A$, i.e. $A[x] \subseteq \frac{1}{d} A$ a frac ideal

$\Rightarrow A[x]$ is a fin gen A-mod $\Rightarrow x$ int over $A \Rightarrow x \in A$.)

So now $\alpha \subsetneq \alpha\mathfrak{p}' \subseteq \mathfrak{p}\mathfrak{p}' = A \Rightarrow \alpha\mathfrak{p}' \notin \Phi \Rightarrow \alpha\mathfrak{p}' = \prod \mathfrak{p}_i^{n_i} \Rightarrow \alpha = \mathfrak{p}\cdot\prod \mathfrak{p}_i^{n_i}, \in \Phi$

Contradiction!

Step 2: "uniqueness" in (a).

If $\prod_{\mathfrak{p}\in P} \mathfrak{p}^{n(\mathfrak{p})} = \prod_{\mathfrak{p}\in P} \mathfrak{p}^{m(\mathfrak{p})}$

by moving positive and negative integers (note $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}\mathfrak{p}^{-1} = A$)

get $\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_s^{\beta_s}$ with $\alpha_i > 0$, $\beta_j > 0$.

$\mathfrak{p}_i \supseteq RHS \Rightarrow \mathfrak{p}_i \supseteq \mathfrak{q}_j$ for some $j \Rightarrow \mathfrak{p}_i = \mathfrak{q}_j$

Iterate this process, to show uniqueness.

Step 3: Part (b): Indeed, for $\beta = \prod \mathfrak{p}_i^{\alpha_i}$, $\prod \mathfrak{p}_i^{-\alpha_i}$ is the inverse

□

Now, for α frac ideal, write $\alpha = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_{\mathfrak{p}}(\alpha)}$, $n_{\mathfrak{p}}(\alpha) \in \mathbb{Z}$.

Then ①: $n_{\mathfrak{p}}(\alpha\beta) = n_{\mathfrak{p}}(\alpha) + n_{\mathfrak{p}}(\beta)$

② : $\alpha \subseteq A$ (i.e. α is int ideal) $\Leftrightarrow n_{\mathfrak{p}}(\alpha) \geq 0$, $\forall \mathfrak{p} \in P$.
Pf. $\Rightarrow$: in pf of main thm ; $\Leftarrow$: easy

③ : $\alpha \subseteq \beta \Leftrightarrow n_{\mathfrak{p}}(\alpha) \geq n_{\mathfrak{p}}(\beta)$, $\forall \mathfrak{p}$.
Pf: $\alpha \subseteq \beta \Leftrightarrow \alpha\beta^{-1} \subseteq A \Leftrightarrow n_{\mathfrak{p}}(\alpha\beta^{-1}) \geq 0$, $\forall \mathfrak{p}$

④ $n_{\mathfrak{p}}(\alpha+\beta) = \min\{n_{\mathfrak{p}}(\alpha), n_{\mathfrak{p}}(\beta)\}$, i.e. $\alpha+\beta = \prod \mathfrak{p}^{\min\{n_{\mathfrak{p}}(\alpha), n_{\mathfrak{p}}(\beta)\}}$

Pf: $\alpha+\beta \supseteq \alpha, \beta$, $\Rightarrow n_{\mathfrak{p}}(\alpha+\beta) \leq n_{\mathfrak{p}}(\alpha), n_{\mathfrak{p}}(\beta) \Rightarrow \leq \min\{\}$
Also $\alpha+\beta = \prod \mathfrak{p}^{\min\{\}}\alpha' + \prod \mathfrak{p}^{\min\{\}}\beta'$ with $\alpha', \beta' \subseteq A$
$= \prod \mathfrak{p}^{\min\{\}}(\alpha'+\beta') \subseteq \prod \mathfrak{p}^{\min\{\}}$
$\Rightarrow n_{\mathfrak{p}}(\alpha+\beta) \geq \min\{\}$. □

⑤. $n_{\mathfrak{p}}(\alpha \cap \beta) = \max\{n_{\mathfrak{p}}(\alpha), n_{\mathfrak{p}}(\beta)\}$, i.e. $\alpha \cap \beta = \prod \mathfrak{p}^{\max\{\}}$
Pf: $\alpha\cap\beta \subseteq \alpha, \beta \Rightarrow n_{\mathfrak{p}}(\alpha\cap\beta) \geq n_{\mathfrak{p}}(\alpha), n_{\mathfrak{p}}(\beta) \Rightarrow \alpha\cap\beta \subseteq RHS$
also $RHS \subseteq \alpha, \beta$, by ③, then $RHS \subseteq \alpha\cap\beta$. □

⑥ : $\alpha\beta = (\alpha+\beta)(\alpha\cap\beta)$.
Pf: by ①, ④, ⑤.

§5. Norm of an ideal.

In this section: $K/\mathbb{Q}$ fin. ext. $A \subseteq K$ ring of integers

write $N(x) = N_{K/\mathbb{Q}}(x)$ for $x \in K$.

Prop 5.1: $x \in A$, $x \neq 0$, then $|N(x)| = \text{card}\,(A/Ax)$.

Pf: first note $N(x) \in \mathbb{Z}$, since $\mathbb{Z}$ is int closed.

Also, we know A is a fin. free $\mathbb{Z}$-mod of rk n

$xA \subseteq A$ sub-$\mathbb{Z}$-mod $\Rightarrow \exists$ basis $e_1, \dots, e_n$ of A,

s.t $xA = \bigoplus_{i=1}^{n} \mathbb{Z} c_i e_i$, s.t $c_1 | c_2 | \cdots | c_n$, $c_i \in \mathbb{Z}$,

$$\Rightarrow \text{Card}\,(A/Ax) = \text{Card}\left(\bigoplus_{i=1}^{n} \mathbb{Z}e_i / \mathbb{Z}c_i e_i\right) = \prod_{i=1}^{n} c_i \in \mathbb{Z}$$

Now, let $u: A \to Ax$ where $e_i \mapsto c_i e_i$ a hom of $\mathbb{Z}$-mod

$\Rightarrow \det(u) = c_1 \cdots c_n$.

Let $v: Ax \to Ax$, where $c_i e_i \mapsto x e_i$ a hom of $\mathbb{Z}$-mod

note $Ax = \langle c_1 e_1, \dots, c_n e_n \rangle_{\mathbb{Z}} = \langle x e_1, \dots, x e_n \rangle_{\mathbb{Z}}$

$\Rightarrow v \in GL_n(\mathbb{Z}) \Rightarrow \det v = \pm 1$

Now, $v \circ u = m_x : A \hookrightarrow Ax \to Ax$ $\quad e \mapsto x \cdot e$

$\Rightarrow N(x) = \det(m_x) = \det(v) \cdot \det(u) = \pm c_1 \cdots c_n$.

$\Rightarrow |N(x)| = \text{Card}\,(A/Ax)$. $\square$

Defn: For $\alpha \subseteq A$ ideal, define $N(\alpha) := \text{Card}\,(A/\alpha)$

note: ① when $\alpha = Ax$ principle $\Rightarrow N(Ax) = \text{Card}\,(A/Ax) = |N(x)|$

② $N(\alpha)$ is always finite, since for any $x \in \alpha$, have

$\text{Card}\,(A/\alpha) \leq \text{Card}\,(A/Ax)$.

Prop 5.2 : If $\alpha, \beta \subseteq A$, then $N(\alpha\beta) = N(\alpha)N(\beta)$.

Pf: By decomposition of ideals in Dedekind domains, and some easy induction, can assume $\beta = \mathfrak{m}$ is a max ideal.

i.e. WANT : $N(\alpha\mathfrak{m}) = N(\alpha)N(\mathfrak{m})$ for $\mathfrak{m}$ max ⊛.

Since $\alpha\mathfrak{m} \subseteq \alpha \subseteq A \Rightarrow \mathrm{Card}(A/\alpha\mathfrak{m}) = \mathrm{Card}(A/\alpha) \cdot \mathrm{Card}(\alpha/\alpha\mathfrak{m})$

$$N(\alpha\mathfrak{m}) = N(\alpha) \cdot \mathrm{Card}(\alpha/\alpha\mathfrak{m})$$

Thus for ⊛ $\Leftarrow \mathrm{Card}(A/\mathfrak{m}) = \mathrm{Card}(\alpha/\alpha\mathfrak{m})$

Now, $A/\mathfrak{m}$ is a field ! (Rmk: a finite field)

$\alpha/\alpha\mathfrak{m}$ is an $A/\mathfrak{m}$-mod, i.e, a vec. space over $A/\mathfrak{m}$.

It suffices to show that $\alpha/\alpha\mathfrak{m}$ is 1-dim over $A/\mathfrak{m}$.

If not, then ∃ non-trivial sub-vector space, which is of shape. $\beta/\alpha\mathfrak{m} \subsetneq \alpha/\alpha\mathfrak{m}$

$\Rightarrow \alpha\mathfrak{m} \subsetneq \beta \subsetneq \alpha$.

But this is impossible!

Since $\forall \mathfrak{p}$, $n_{\mathfrak{p}}(\alpha) + n_{\mathfrak{p}}(\mathfrak{m}) \geq n_{\mathfrak{p}}(\beta) \geq n_{\mathfrak{p}}(\alpha)$

for $\mathfrak{p} \neq \mathfrak{m}$, $n_{\mathfrak{p}}(\mathfrak{m}) = 0 \Rightarrow n_{\mathfrak{p}}(\alpha) = n_{\mathfrak{p}}(\beta)$

$\mathfrak{p} = \mathfrak{m}$, $n_{\mathfrak{m}}(\alpha) + 1 \geq n_{\mathfrak{m}}(\beta) \geq n_{\mathfrak{m}}(\alpha) \Rightarrow n_{\mathfrak{m}}(\beta) \in \{n_{\mathfrak{m}}(\alpha), n_{\mathfrak{m}}(\alpha)+1\}$

$\Rightarrow \beta = \alpha$ or $\alpha\mathfrak{m}$. Contradiction □

Chapter 4. Ideal class group.

A Dedekind domain, $I(A)$: group of all non-zero frac ideals.
A frac ideal is called a principle frac ideal if it is $A \cdot x$ for some $x \in K$; they form a subgp of $I(A)$, denoted as $P(A)$

Define $C(A) := I(A)/P(A)$, called the ideal class group.
(elts in $C(A)$ are called ideal classes)
Note: $C(A) = \{1\} \Leftrightarrow A$ is PID.

Main Thm of Chapter: For $K/\mathbb{Q}$ fin. ext, A = ring of integers, $C(A)$ is a finite group.
Rmk ① call $\#|C(A)|$ the class number of K.
② For general Dedekind domain, possible $\#|C(A)| = +\infty$.

§0. Why do we care?

* Technical level: $\#|Cl(A)|$ measures how far A is not a PID.
(PID is too good).

Class number formula: $\lim_{s\to 1}(s-1)\zeta_K(s) = \dfrac{2^{r_1}\cdot(2\pi)^{r_2}\cdot \mathrm{Reg}_K \cdot h_K}{w_K\cdot\sqrt{|D_K|}}$, $h_K = \#|Cl(A)|$.

$K=\mathbb{Q}$, $\zeta_K(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$

analytic objects $\overset{\text{link}}{\longleftrightarrow}$ arithmetic (algebraic) objects

BSD conj: $L'(E,s)|_{s=1} = \dfrac{\# \cdot Ш(E)}{\#}$

In fact, pf of our Main Thm uses some (basic) complex analysis, which a priori, is quite surprising (we are using analysis to study purely algebraic objects!)

* What is "good mathematics"?
Almost always, are those linking different areas.
Within ANT:
BSD conj: analysis $\longleftrightarrow$ algebra

Fermat's Last Thm $\in$ Langlands program: group theory $\longleftrightarrow$ representation thy

algebraic geometry
(algebra $\longleftrightarrow$ geometry)

What to learn after this course: Galois theory: field extension $\longleftrightarrow$ group thy.

or: Ask ME!

* Strategy of Pf: A common strategy to prove finiteness of a set in ANT.

Define a certain function: $f: S \to \mathbb{R}^{>0}$.

Show ① For any $h \in \mathbb{R}^{>0}$,
$\{s \in S,\ f(s) \leq h\}$ is a finite set.

② $\exists\ H \in \mathbb{R}^{>0}$, s.t. $f(s) < H$, $\forall s \in S$.

Rmk: In certain situations, ② does not hold; but ① still gives useful info.

§1. Some analysis about lattices.

Recall: Let $X=\mathbb{R}^n$ with usual topo,

- $K\subseteq X$ called compact if $\forall\ K=\bigcup_{i=0}^{\infty} K_i$ open covering, $\exists$ finite subcovering $K=\bigcup_{k=1}^{N} K_{i(k)}$. ($\Leftrightarrow$ closed and bounded)
- $D\subseteq X$ called discrete if $\forall$ K cpt, $D\cap K$ is finite set
- If $H\subseteq\mathbb{R}^n$ an additive subgp, and discrete, then call it a discrete subgp of $\mathbb{R}^n$.
  Ex: $H=\mathbb{Z}^i$, $1\le i\le n$.

Lem 1.1 $\mathbb{R}^n\supseteq X_1\supseteq X_2\supseteq\cdots\supseteq X_n\supseteq\cdots$ where X_i cpt (compact) and non-empty.
Then $X_i=\bigcap_{n=1}^{\infty} X_n$ is also non-empty and cpt.

Pf: X is cpt since closed and bded.
Consider $Y_n=X_1\setminus X_n$. then $\bigcup_{n=2}^{\infty} Y_n=X_1\setminus\bigcap_{n=2}^{\infty} X_n$

if $\bigcap_{n=2}^{\infty} X_n=\phi\Rightarrow\bigcup_{n=2}^{\infty} Y_n$ is an open cover of X_1.

$\Rightarrow\exists$ finite cover $Y_{k_1}\cup\cdots\cup Y_{k_s}=X_1$
$\Rightarrow X_{k_1}\cap\cdots\cap X_{k_s}=\phi$ contradiction. □

Thm 1.2: $H\subseteq\mathbb{R}^n$ discrete subgp. Then H is generated (as a $\mathbb{Z}$-mod) by r vectors which are linearly independent over $\mathbb{R}$.
In particular, $r\le n$, and $H\simeq\mathbb{Z}^{\oplus r}$.

Pf: Let $(e_1,\cdots,e_r)\in H$ which are lin indep over $\mathbb{R}$, and suppose r is max possible (so $r\le n$).

Let $P=\left\{x\in\mathbb{R}^n \;\middle|\; x=\sum_{i=1}^{r}\alpha_i e_i,\ 0\le\alpha_i\le 1\right\}$

P is cpt, $\Rightarrow P \cap H =$ finite

For $x \in H$, $x = \sum_{i=1}^{r} \lambda_i e_i$, $\lambda_i \in \mathbb{R}$ (bec r is max)

for $j \in \mathbb{Z}^{>0}$, consider $jx = \sum j\lambda_i e_i$

let $x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i = \sum_{i=1}^{r} \{j\lambda_i\} e_i$

here $a \in \mathbb{R}$, $[a] = \begin{cases} a & \text{if } a \in \mathbb{Z} \\ m & \text{if } m \le x < m+1 \end{cases}$, and $\{a\} = a - [a]$.

Now $x_j \in P \cap H$, $\forall j$, since $P \cap H =$ finite

$\Rightarrow \exists\, k \neq j$, $x_k = x_j \Rightarrow \sum j\lambda_i e_i - \sum [j\lambda_i] e_i$
$= \sum k\lambda_i e_i - \sum [k\lambda_i] e_i$

$\Rightarrow j\lambda_i - [j\lambda_i] = k\lambda_i - [k\lambda_i]$, $\forall i$

$\Rightarrow \lambda_i = \dfrac{[j\lambda_i] - [k\lambda_i]}{j-k} \in \mathbb{Q}$.

i.e. $x \in \langle e_1 \cdots e_r \rangle_{\mathbb{Q}} \Rightarrow H \subseteq \langle e_1 \cdots e_r \rangle_{\mathbb{Q}}$ ⊛

Perhaps better to prove fin. gen. over $\mathbb{Z}$ first, before proving ⊛

Now, $x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$ $x_1 \in P \cap H$, $e_i \in P \cap H$

$\Rightarrow H \subseteq \sum_{f_t \in P \cap H} \mathbb{Z} \cdot f_t$, $\Rightarrow H$ is fin. gen over $\mathbb{Z}$

$\Rightarrow H = \mathbb{Z}^{\oplus s} \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$.

but $H \subseteq \langle e_1 \cdots e_r \rangle_{\mathbb{Q}} \Rightarrow$ no torsion $\Rightarrow H = \mathbb{Z}^{\oplus s}$, and $s \le r$.
But $\bigoplus_{i=1}^{r} \mathbb{Z} e_i \subseteq H \Rightarrow s \ge r \Rightarrow s = r$, $H \simeq \mathbb{Z}^{\oplus r}$. □