Prop 4.2 $K \subseteq L$ fields, char $=0$, $L = K(x)$, $\mathrm{Irr}(x,K) = \prod_{i=1}^{n}(T - x_i)$, $x_1 = x$.
Let $\bar{K}$ be an alg. closed field containing L.
Let $\sigma_i : L \hookrightarrow \bar{K}$ be the K-embeddings defined by $\sigma_i(x) = x_i$.
Then for all $y \in L$, have $\mathrm{Tr}(y) = \sum_{i=1}^{n} \sigma_i(y)$
$N(y) = \prod_{i=1}^{n} \sigma_i(y)$, char poly$(y) = \prod_{i=1}^{n}(T - \sigma_i(y))$

Pf: **Case 1** $L = K(y)$, i.e., y is also a primitive elt
If $\mathrm{Irr}(y,K) = \prod_{i=1}^{n}(T - y_i)$, $y_1 = y$,
By Prop 4.1. $\mathrm{Tr}(y) = \sum y_i$, $N(y) = \prod y_i$, c.poly $(y) = \prod(T - y_i)$
Note we can also use y_i to define the K-emb $\theta_i : L \hookrightarrow \bar{K}$
by $\theta_i(y) = y_i$ $\forall\, 1 \le i \le n$.
This means $\{\sigma_1, \dots, \sigma_n\} = \{\theta_1, \dots, \theta_n\}$, only different order
$\Rightarrow \mathrm{Tr}(y) = \sum y_i = \sum \theta_i(y) = \sum \sigma_i(y)$, Similarly for N and c.poly.

Case 2 $K \subsetneq K(y) \subsetneq L$
$\sigma_i : L \hookrightarrow \bar{K}$, $\Rightarrow \sigma_i|_{K(y)} : K(y) \hookrightarrow \bar{K}$ are K-emb.
Suppose $\gamma_1, \dots, \gamma_m : K(y) \hookrightarrow \bar{K}$ all the different K-emb,
where $m = [K(y) : K]$
Check that: $\{\sigma_1|_{K(y)}, \dots, \sigma_n|_{K(y)}\}$ is $[L : K(y)]$-copies of $\{\gamma_1, \dots, \gamma_m\}$.
$\Rightarrow \mathrm{Tr}_{L/K}(y) = \frac{n}{m}(\gamma_1(y) + \cdots + \gamma_m(y))$ by Prop 4.1
$= \sum_{i=1}^{n} \sigma_i(y)$
Similarly for $N(y)$, ch.poly(y). □

No.

Date

Prop 4.3 A: int dom, $K = \mathrm{Frac}\, A$ char $=0$, $K \subseteq L$ fields. $\chi \in L$, χ int over A. Then coefficients of $\mathrm{Irr}(\chi, K)$ are all integral over A. In particular, $\mathrm{Tr}(\chi)$, $N(\chi)$ are int over A.

Pf Let $\mathrm{Irr}(\chi, K) = \prod_{i=1}^{n} (T - \chi_i) = F(T)$

Claim: χ_i is int over A, $\forall i$. $\subseteq K[T]$

Pf χ int over $A \Rightarrow \exists\ G(T) \in A[T]$ monic, s.t. $G(\chi) = 0$

$\Rightarrow F(T) \mid G(T) \Rightarrow G(\chi_i) = 0 \Rightarrow \chi_i$ int over A.

$\Rightarrow$ Coeff of $F(T)$ are int over A. $\square$

Cor 4.4 Suppose A is int closed in Prop 4.3, then $\mathrm{Irr}(\chi, K) \in A[T]$.

Pf. already have $\mathrm{Irr}(\chi, K) \in K[T]$. $\square$

Ex: $\frac{\sqrt{2}}{2}$ is NOT integral over $\mathbb{Z}$.

Pf. Let $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(\frac{\sqrt{2}}{2})$

Suppose $\frac{\sqrt{2}}{2}$ is int over $\mathbb{Z}$, then $\mathrm{Irr}(\frac{\sqrt{2}}{2}, \mathbb{Q}) \in \mathbb{Z}[T]$

(since $\mathbb{Z}$ PID $\Rightarrow$ int closed)

However, $\mathrm{Irr}(\frac{\sqrt{2}}{2}, \mathbb{Q}) = T^2 - \frac{1}{2} \notin \mathbb{Z}[T]$ $\square$

§5 Discriminant.

Defn: $A \subseteq B$ rings, $B = A^{\oplus n}$ as A-mod. For $(x_1, \cdots, x_n) \in B^n$ (i.e. $x_i \in B$), the discriminant of $(x_1, \cdots, x_n)$ is

$$D(x_1, \cdots, x_n) := \det\left(\mathrm{Tr}_{B/A}(x_i x_j)\right).$$

Ex. $A = \mathbb{Q}$, $B = \mathbb{Q}(\sqrt{2})$, then $B = A \oplus A\sqrt{2}) = A^{\oplus 2}$

Take $(\sqrt{2}, 2) \in B^2$, $D(\sqrt{2}, 2) = \det\begin{pmatrix} \mathrm{Tr}\, 2 & \mathrm{Tr}\, 2\sqrt{2} \\ \mathrm{Tr}\, 2\sqrt{2} & \mathrm{Tr}\, 4 \end{pmatrix}$

recall $\mathrm{Tr}(a + b\sqrt{2}) = (a + b\sqrt{2}) + (a - b\sqrt{2}) = 2a$.

$\Rightarrow D(\sqrt{2}, 2) = \det\begin{pmatrix} 4 & 0 \\ 0 & 8 \end{pmatrix} = 32$

Prop 5.1 Suppose $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = T\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ where $T \in \mathrm{Mat}_{n\times n}(A)$, $T = (a_{ij})_{n\times n}$.
Then $D(y_1, \cdots, y_n) = (\det T)^2 \cdot D(x_1, \cdots, x_n)$.

Pf. Check by hand we have matrix eqn,

$$\mathrm{Tr}(y_p y_q) = (a_{p1}, \cdots, a_{pn})\left(\mathrm{Tr}(x_i x_j)\right)_{n\times n}\begin{pmatrix} a_{q1} \\ \vdots \\ a_{qn} \end{pmatrix}$$

take det. □

Rmk: If $(x_1, \cdots, x_n)$ and $(y_1, \cdots, y_n)$ are two bases of the A-mod B, thus $T \in GL_n(A)$. then $\det T \in A^\times$, $\Rightarrow D(y_1, \cdots, y_n)$ and $D(x_1, \cdots, x_n)$ only differ by some unit in A.

Defn: Let $D_{B/A}$ be the principle ideal generated by $D(x_1, \cdots, x_n)$ for any basis of B over A. Call it the discriminant of B over A.

Lem 5.2 Suppose A int dom, and $D_{B/A} \neq (0)$. Then $(x_1, \cdots, x_n)$ is a basis of B as A-mod $\Leftrightarrow D(x_1, \cdots, x_n)$ generates $D_{B/A}$.

Pf: $\Leftarrow$ Prop 5.1 □

Prop. 5.3 $K \subseteq L$ fields, char $= 0$, $L = K[x]$, $[L:K] = n$.
Let $\sigma_i : L \hookrightarrow \bar{K}$ be all the K-emb. $1 \le i \le n$.

① If $(y_1, \dots, y_n)$ is a K-basis of L, then
$$D(y_1, \dots, y_n) = \det\left((\sigma_i(y_j))_{1 \le i,j \le n} \right)^2.$$

② $D(1, x, \dots, x^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{L/K}(F'(x)) \neq 0$
where $F'(T)$ = derivative of $F(T) = \mathrm{Irr}(x, K)$.
(So in particular, $D_{L/K} \neq 0$).

Pf ① $D(y_1, \dots, y_n) = \det\left(\mathrm{Tr}(y_i y_j)\right) = \det\left(\sum_k \sigma_k(y_i y_j)\right)$

$= \det\left(\sum_k \sigma_k(y_i)\sigma_k(y_j)\right) = \det\left(\sigma_k(y_i)\right) \cdot \det\left(\sigma_k(y_j)\right)$

$= \left(\det\left(\sigma_i(y_j)\right)\right)^2$.

② Suppose $F(T) = \prod_{i=1}^{n} (T - x_i)$, $x_1 = x$.

Then $D(1, x, \dots, x^{n-1}) = \det\left(\sigma_i(x^j)\right)^2$ by ①

$= \left(\det\left(x_i^j\right)\right)^2 = \left(\prod_{i<j} (x_i - x_j)\right)^2$ by Vandermonde

$= (-1)^{\frac{1}{2}n(n-1)} \cdot \prod_{i \neq j} (x_i - x_j)$

$= (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} \prod_{j \neq i} (x_i - x_j) = (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} F'(x_i)$

$= (-1)^{\frac{1}{2}n(n-1)} N_{L/K}\left(F'(x)\right)$

since $\sigma_i(F'(x)) = F'(x_i)$.

$\neq 0$ (since x_i are distinct). $\square$

Ex 3.4. (1) $K \subseteq K(x)$, $F(T) = T^2 + aT + b$, deg 2, $F' = 2T + a$

$= (T - x_1)(T - x_2)$

Then $D(1, x) = (-1)^{\frac{1}{2} \times 2} (2x_1 + a)(2x_2 + a)$

$= (-1)[4x_1x_2 + 2a(x_1 + x_2) + a^2]$

$= (-1)(4b + 2a(-a) + a^2)$

$= a^2 - 4b$

(2). $K \subseteq K(x)$, $F(T) = T^3 + aT + b$ (rmk any cubic polynomial can be transformed to this shape). $F'(T) = 3T^2 + a$

$\Rightarrow D(1, x, x^2) = (-1)^{\frac{1}{2} \times 3 \times 2} \left((3x_1^2 + a)(3x_2^2 + a)(3x_3^2 + a) \right)$

$= -\left(27(\Pi x_i)^3 + a \cdot 9 \Sigma x_i^2 x_j^2 + a^2 \cdot 3 \cdot \Sigma x_i^2 + a^3 \right)$.

$\Pi x_i = +b$

$\Sigma x_i^2 x_j^2 = (\Sigma x_i x_j)^2 - 2 \Pi x_i \cdot (\Sigma x_i) = a^2$

$\Sigma x_i^2 = (\Sigma x_i)^2 - 2(\Sigma x_i x_j) = 0 - 2 \cdot a = -2a$

$D = -(27b^2 + 9a \cdot a^2 + 3a^2 \cdot (-2a) + a^3)$

$= -(4a^3 + 27b^2)$

Recall in Prop 5.3②, for $[L:K]=n$, $\mathrm{char}=0$, if $x_1,\cdots,x_n$ is basis of L/K, then $D(x_1,\cdots,x_n)\neq 0$. This means that the bilinear form $(x,y)\mapsto \mathrm{Tr}_{L/K}(xy)$ is non-degenerate, i.e. $\mathrm{Tr}_{L/K}(xy)=0$ for all $y\in L \Leftrightarrow x=0$.

Recall: a bi-linear form on a (fin. dim) vector space V over a field K, is a function $f: V\times V\to K$.
If fix basis $(e_1,\cdots,e_n)$ of V, then

$$f(v,w)=(v_1,\cdots,v_n)\Big(f(e_i,e_j)\Big)_{1\le i,j\le n}\begin{pmatrix}w_1\\ \vdots\\ w_n\end{pmatrix}$$

where $v=\sum v_i e_i$, $w=\sum w_i e_i$.

In our situation, $(x_1,\cdots,x_n)$ is basis, Matrix $=\big(\mathrm{Tr}(x_i x_j)\big)_{1\le i,j\le n}$.
$\det\neq 0 \Leftrightarrow (\mathrm{Tr}(x_i x_j))_{i,j}$ is invertible

Now, $\forall x\in L$, $S_x: y\mapsto \mathrm{Tr}_{L/K}(xy)\in L^\vee := \mathrm{Hom}_K(L,K)$ is a linear form. $S_x=0\Leftrightarrow x=0$.
$\Rightarrow$ get injection: $L\hookrightarrow L^\vee$ $\quad x\mapsto S_x$
Since $\dim_K L=\dim_K L^\vee \Rightarrow$ is bijection.

If $(x_1,\cdots,x_n)$ basis of L/K, Let $(x_1^\vee,\cdots,x_n^\vee)$ the dual basis of $L^\vee$.
If $S_{y_i}=x_i^\vee, \forall i$, Then have $\mathrm{Tr}_{L/K}(x_i y_j)=\delta_{ij}\ \forall i,j$.

Call such $(y_1,\cdots,y_n)$ the dual basis w.r.t. $\mathrm{Tr}_{L/K}$ (always exists because $\mathrm{Tr}_{L/K}$ is non-degenerate)

Thm 5.5. A: an int closed ring, $K = \mathrm{Frac}\, A$. $\mathrm{char}\, K = 0$. L/K, $[L:K] = n$.
A' - int closure of A in L.
Then: A' is an A-submod of a free A-mod of rk n.

Rmk In many applications, can let A = PID, then can get stronger statement (e.g. $A = \mathbb{Z}$, $K = \mathbb{Q}$), But need this weaker assumption for later use.

Pf: Let $L = \langle x_1, \cdots, x_n \rangle_K$

each x_i alg over $K \Rightarrow x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_1 x_i + a_0 = 0$, $a_i \in K = \mathrm{Frac}\, A$
multiply some LCM of denominators of a_i

$\rightsquigarrow$ get some $a_n' x_i^n + a_{n-1}' x_i^{n-1} + \cdots + a_1' x_i + a_0' = 0$, $a_i' \in A$

multiply $(a_n')^{n-1}$

$\Rightarrow (a_n' x_i)^n + a_{n-1}' a_n' (a_n' x_i)^{n-1} + \cdots + a_0' (a_n')^{n-1} = 0$

$\Rightarrow x_i' = a_n' x_i$ is int over A, i.e. $x_i' \in A'$. Do this for all x_i.

Clearly, $L = \langle x_1', \cdots, x_n' \rangle_K$, (now $x_i' \in A'$)

Let $(y_1, \cdots, y_n)$ be the dual basis w.r.t. $\mathrm{Tr}_{L/K}$,
i.e. $\mathrm{Tr}_{L/K}(x_i' y_j) = \delta_{ij}$

Claim: $A' \subseteq \sum_{j=1}^{n} A y_j$

Indeed, let $z \in A'$, then $z = \sum b_j y_j$, $b_j \in K$. WANT: $b_j \in A$

$x_i' \in A'$, $z \in A' \Rightarrow x_i' z \in A' \Rightarrow \mathrm{Tr}(x_i' z) \in A$, by Cor 4.4
(which says $\mathrm{Tr}(x_i' z)$ is int over A)
However, $\mathrm{Tr}(x_i' z) = \sum_{j=1}^{n} b_j \mathrm{Tr}(x_i' y_j) = b_i \Rightarrow b_i \in A$. $\square$

Cor 5.6 Keep notations as in Thm 5.5.
If furthermore A is PID, then $A' =$ free A-mod of rk n.

Pf: $A' \subseteq \sum_{j=1}^{n} A y_j$. (RHS is free)

$\Rightarrow A'$ is free of rk $\leq n$.

But $x_1', \dots, x_n' \in A'$, which is basis of L/K

$\Rightarrow$ rk $A' = n$. □

Ex: $A = \mathbb{Z}$, $K = \mathbb{Q}$,

Cor 5.6 says: for $L/\mathbb{Q}$ an algebraic number field,
ring of integers is a free A-mod of rk $[L:K]$.
(Recall, we calculated A' for L quad fields)

Section 6. Cyclotomic fields

We study a special kind of cyclotomic fields. $K = \mathbb{Q}(\zeta)$, where $\zeta^p = 1$ is a primitive p-th root of unity. (p prime)

Let $F(T) = \frac{T^p - 1}{T - 1} = T^{p-1} + T^{p-2} + \cdots + T + 1$.

Want to show. $\mathrm{Irr}(\zeta, \mathbb{Q}) = F(T)$ $\Leftarrow F(T)$ is irred.

Lemma (Eisenstein's criterion)

Let $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0 \in \mathbb{Z}[T]$,

If $\exists$ some prime p, s.t. $p \mid a_i$, $\forall i$, and $p^2 \nmid a_0$,

then $f(T)$ is irreducible, considered as poly in $\mathbb{Q}[T]$.

Pf. If not, $f(T) = g(T)h(T)$ in $\mathbb{Q}[T]$.

- can suppose $g(T)$, $h(T)$ are both monic.

All roots of $g(T)$, $h(T)$ are int over $\mathbb{Z}$ $\Rightarrow$ coeff of g, h int over $\mathbb{Z}$

$\Rightarrow g(T), h(T) \in \mathbb{Z}[T]$ (since $\mathbb{Z}$ int closed)

modulo p, get $\bar{f}(T) = \bar{g}(T)\bar{h}(T) \in \mathbb{Z}_p[T]/(p) = \mathbb{F}_p[T]$

$T^n = \bar{g}(T)\bar{h}(T)$

$\Rightarrow \bar{g}(T) = T^q$, $\bar{h}(T) = T^{n-q}$ for some $1 \le q \le n-1$

$\Rightarrow g(0) \equiv 0 \pmod p$, i.e. constant term divisible by p

$h(0) \equiv 0 \pmod p$

$\Rightarrow f(0) = a_0 = g(0)h(0)$ divisible by p^2, contradiction. $\square$

Ex $F(T) = T^{p-1} + T^{p-2} + \cdots + T + 1$ is irred in $\mathbb{Q}[T]$

Pf: Let $T = Y + 1$ $\rightsquigarrow F(T) = \frac{T^p - 1}{T - 1} = \frac{(1+Y)^p - 1}{Y} = Y^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} Y^{j-1} = F_1(Y)$

obviously $F(T)$ irr. $\Leftrightarrow F_1(Y)$ irr.

$F_1(Y)$ irr by Eisenstein's criterion, since $p \mid \binom{p}{j}$, $1 \le j \le p-1$, and $\binom{p}{1} = p$. $\square$

Thm 6.2. $K = \mathbb{Q}(\zeta)$, $\zeta^p = 1$, $\zeta \neq 1$, A: ring of integers.
Then $A = \mathbb{Z}[\zeta] = \langle 1, \zeta, \cdots, \zeta^{p-2} \rangle_{\mathbb{Z}}$.

↙NOT p-1!

Pf: $K = \langle 1, \zeta, \cdots \zeta^{p-2} \rangle_{\mathbb{Q}}$. For $x \in A$, $x = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$
WANT: $a_i \in \mathbb{Z}$.

Lem. ① $A(1-\zeta) \cap \mathbb{Z} = p\mathbb{Z}$
② $\forall y \in A$, $Tr(y(1-\zeta)) \in p\mathbb{Z}$

Pf of Lem. ①. $\zeta - 1$ is a root $F_1(Y) = Y^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} Y^{j-1}$.

$\Rightarrow N(\zeta - 1) = (-1)^{p-1} p \Rightarrow N(1-\zeta) = N(-1)N(\zeta-1) = p$.

By Prop 4.2 (note the conjugates of ζ are ζ^i, $1 \le i \le p-1$)

$\Rightarrow N(1-\zeta) = \prod_{i=1}^{p-1} (1-\zeta^i) \in A(1-\zeta)$.

$\Rightarrow A(1-\zeta) \cap \mathbb{Z} \supseteq p\mathbb{Z}$

Note LHS is ideal of $\mathbb{Z}$, it suffices to show $A(1-\zeta) \cap \mathbb{Z} \neq \mathbb{Z}$.
If not, $\Rightarrow (1-\zeta)$ is unit in A.
Impossible, since if $(1-\zeta)t = 1$, for some $t \in A$
$N(1-\zeta), N(t) \in \mathbb{Z}$, but $\underset{\overset{\|}{p}}{N(1-\zeta)} \cdot N(t) = N(1) = 1$.

②: $Tr(y(1-\zeta)) = \sum_{i=1}^{p-1} \sigma_i(y(1-\zeta))$

$= \sum_{i=1}^{p-1} \sigma_i(y)(1-\zeta^i) \in A(1-\zeta)$

also $\subseteq \mathbb{Z}$ since $\mathbb{Z}$ is int closed

$\Rightarrow Tr(y(1-\zeta)) \in A(1-\zeta) \cap \mathbb{Z} = p\mathbb{Z}$. □

Now, $x(1-\zeta) = a_0(1-\zeta) + a_1(\zeta - \zeta^2) + \cdots + a_{p-2}(\zeta^{p-2} - \zeta^{p-1})$
$Tr(\zeta^i) = -1$, $\forall 1 \le i \le p-1$, $\Rightarrow Tr(\zeta^i - \zeta^{i+1}) = 0$ $\forall i \ge 1$
$\Rightarrow Tr(x(1-\zeta)) = a_0 Tr(1-\zeta) = a_0(p-1) + a_0 = pa_0 \in p\mathbb{Z}$ by Lemma,
$\Rightarrow a_0 \in \mathbb{Z}$.

since $\zeta^{-1} = \zeta^{p-1} \in A$, $\Rightarrow \zeta^{-1}(\chi - a_0) \in A$,

$\Rightarrow a_1 + a_2\zeta + \cdots + a_{p-1}\zeta^{p-3} \in A$

Use same argument $\Rightarrow a_1 \in \mathbb{Z}$. Then repeat again....

□

Chapter 3. Dedekind domain.

Section 1. Some preliminaries.

Recall: M: A-mod, TFAE (Noeth. mod)

(a) non-empty collection of submods of M has max elt.

(b) $M_1 \subseteq M_2 \subseteq \cdots M_n \subseteq \cdots$ stablizes

(c) any submod is fin. gen.

Recall: Chap 2, Thm 5.5: A: int closed ring, $K = \mathrm{Frac} A$, $\mathrm{char} K = 0$.
L/K, $(L:K) = n$, A' = int closure of A in L.
Then: A' is an A-submod of a free A-mod of rk n.

Quick recall Pf: $L = \langle x_1, \cdots, x_n \rangle_K$
$\rightsquigarrow$ construct $x_i' \in A'$, s.t. $L = \langle x_1', \cdots, x_n' \rangle_K$
$(y_1, \cdots, y_n)$ the dual basis of $(x_1', \cdots, x_n')$ w.r.t. $Tr_{L/K}(xy)$.
Then $A' \subseteq \sum_{j=1}^{n} A y_j$ $\square$

Prop 1.1: A, K, A', L as in Chap 2, Thm 5.5 above. (In particular, A is int closed).
If furthermore A is a Noeth ring, then so is A'.

Pf. Chap 2. Thm 5.5 above $\Rightarrow$ A' is Noeth A-mod.
A' is Noeth ring $\Leftrightarrow$ $I' \subseteq A'$ ideals are fin gen over A'
but $I' \subseteq A'$ are also A-submod of A'
$\Rightarrow I'$ fin gen over A $\Rightarrow$ also fin. gen over A'. $\square$.

Cor. $(A = \mathbb{Z}, K = \mathbb{Q})$. Rings of integers of number fields are Noeth. rings.

Recall. $\mathfrak{p} \subseteq A$ prime $\Leftrightarrow$ "$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$"
$\Leftrightarrow$ "$x \notin \mathfrak{p}, y \notin \mathfrak{p} \Rightarrow xy \notin \mathfrak{p}$"
$\Leftrightarrow$ The set $A \setminus \mathfrak{p}$ is stable under multiplication
$\Leftrightarrow$ $A/\mathfrak{p}$ is int domain.

No

Date

Lem 1.2. $A \subseteq B$ rings, $\mathfrak{p} \subseteq B$ prime, then $\mathfrak{p}' = \mathfrak{p} \cap A \subseteq A$ is prime.

Pf: $A/\mathfrak{p}' \hookrightarrow B/\mathfrak{p}$ = int domain. $\square$.

Lem 1.3. $\mathfrak{p} \subseteq A$ prime. $\alpha_1 \cdots, \alpha_n \subseteq A$ ideals, $\mathfrak{p} \supseteq \alpha_1 \cdots \alpha_n$, then $\mathfrak{p} \supseteq \alpha_i$ for some i.

Pf. If not, take $a_i \in \alpha_i$, s.t. $a_i \notin \mathfrak{p}$. then $a_1 \cdots a_n \notin \mathfrak{p}$. $\square$

Section 2. Dedekind domains.

Defn: A: int domain. Call it Dedekind domain if it is:
- Noeth ring
- int closed
- any non-zero prime ideal is maximal.

Ex: any field; $\mathbb{Z}$; any PID

Thm 2.1 A: Dedekind dom, $K = \mathrm{Frac}A$, char $= 0$, $[L:K] = n$ fin ext, A': int closure of A in L. Then A' is also Dedekind dom.

Pf: A' is Noeth ring by Prop 1.1.

A' is int closed by defn.

For $(0) \neq \mathfrak{p}' \subseteq A'$ prime, then $\mathfrak{p} = \mathfrak{p}' \cap A \subseteq A$ prime.

Choose any $x \in \mathfrak{p}'$, $x \neq 0$, consider integral eqn of min deg

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad a_i \in A$$

then $a_0 \neq 0$, and $a_0 \in \mathfrak{p}' \cap A = \mathfrak{p} \Rightarrow \mathfrak{p} \neq (0) \Rightarrow \mathfrak{p}$ max in A

$A'/\mathfrak{p}'$ is int over $A/\mathfrak{p}$ (easy to check, also in HW2)

apply Chap 2, Prop 1.5 to conclude $A'/\mathfrak{p}'$ is field $\Rightarrow \mathfrak{p}'$ is max in A'. □

Cor: ($A = \mathbb{Z}$, $K = \mathbb{Q}$). Rings of integers in number fields are Dedekind. dom.

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 $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$, $\therefore$ 2 is NOT prime.

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

obv: 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