16.1. Rings of integers

References: - Cohen, chapter 6.1
- Cohst, chapter V

Let $K=\mathbb{Q}$, $L=\mathbb{Q}[X]/(f)$ a degree n number field with $f\in\mathbb{Z}[X]$ monic irreducible.
In other words, $L=\mathbb{Q}(\alpha)$ for a root α of f.

Q How to determine the ring of integers $\mathcal{O}_L$?
(i.e.: a basis of $\mathcal{O}_L$ as a $\mathbb{Z}$-module).

Rmk f monic, $f(\alpha)=0 \Rightarrow \alpha\in\mathcal{O}_L \Rightarrow \mathbb{Z}[\alpha]\subseteq\mathcal{O}_L$

$\mathbb{Z}[\alpha]\subseteq\mathcal{O}_L$ is an order: a subring of $\mathcal{O}_L$ of finite index.
$\mathbb{Z}[\alpha]=\mathbb{Z}+\mathbb{Z}\alpha+\dots+\mathbb{Z}\alpha^{n-1}$

Rmk $\operatorname{disc}(\mathbb{Z}[\alpha])=\operatorname{disc}(f)$
$\operatorname{disc}(\mathcal{O}_L)=\operatorname{disc}(L)$

Rmk For any orders $R\subseteq S\subseteq\mathcal{O}_L$, we have
$$\operatorname{disc}(R)=\operatorname{disc}(S)\cdot[S:R]^2.$$
(In particular, if $\operatorname{disc}(f)\in\mathbb{Z}$ is squarefree, then $\mathbb{Z}[\alpha]=\mathcal{O}_L$.)

Def Let p be a prime number.
An order $R \subseteq \mathcal{O}_L$ is *p-maximal* if there is no $a \in \mathcal{O}_L$ such that $a \notin R$ but $pa \in R$.

Lemma 16.1.1 R is p-max. if and only if $p \nmid [\mathcal{O}_L : R]$.

Pf $\mathcal{O}_L / R$ is a finite abelian group of order $[\mathcal{O}_L : R]$.
[redacted] an element $(a \bmod R)$ of order p if and only if $p \mid [\mathcal{O}_L : R]$. □

[redacted] **Rmk** In particular, R [redacted] is p-maximal for all p with $p^2 \nmid$ [redacted] $\operatorname{disc}(R)$.

[redacted]

Cor 16.1.2 We have $R = \mathcal{O}_L$ (R is maximal) if and only if R is p-maximal for all p.

~~Now, $\mathcal{O}_L/R$ is a finite abelian group of order k divisible by p. $\Rightarrow$ It contains an element of order p, say $\alpha \bmod R$.~~
~~$\Rightarrow$ $p\alpha \in R$, but $\alpha \notin R$.~~ $\square$

Ex Let $t \in \mathbb{Z}$ be not a square.
$\Rightarrow f(X) = X^2 - t$ is irreducible, $L = \mathbb{Q}(X)/f = \mathbb{Q}(\sqrt{t})$.

W.l.o.g. $\alpha = \sqrt{t}$.

$\operatorname{disc}(f) = 4t$
$\|$
$\operatorname{disc}(\mathbb{Z}[\alpha])$

a) Let $p \neq 2$. Then, $\mathbb{Z}[\alpha]$ is p-maximal iff $p^2 \nmid t$:
If $p^2 \mid t$, then $\frac{\alpha}{p} \in \mathcal{O}_L$ (with min. pol. $X^2 - \frac{t}{p^2}$),

$p \cdot \frac{\alpha}{p} \in \mathbb{Z}[\alpha]$, $\frac{\alpha}{p} \notin \mathbb{Z}[\alpha]$.

b) $\mathbb{Z}[\alpha]$ is 2-maximal iff $t \equiv 1, 3 \bmod 4$:
If $t \equiv 0 \bmod 4$, then $\frac{\alpha}{2} \in \mathcal{O}_L$ like before.
If $t \equiv 1 \bmod 4$, then $\frac{1+\alpha}{2} \in \mathcal{O}_L$ (with min. pol. $X^2 - X - \frac{t-1}{4} \in \mathbb{Z}(X)$)

If $t \equiv 2, 3 \bmod 4$, then the min. pol. of $\frac{r+s\alpha}{2}$ with $r, s \in$
is $X^2 - rX - \frac{s^2 t - r^2}{4}$, which only lies in $\mathbb{Z}(X)$ if r, s are both even.
$\|$
$(X - \frac{r}{2})^2 - \frac{s^2 t}{4}$

Then, $\frac{r+s\alpha}{2} \in \mathbb{Z}[\alpha]$.

Remark The method used in the example ~~[redacted]~~ in principle works for any number field (and can even be used to compute the ring of integers).

$\mathbb{Z}[\alpha]$ is p-maximal if and only if ~~[redacted]~~ the min. pol. of

$v := \frac{1}{p}(r_0 + r_1\alpha + \dots + r_{n-1}\alpha^{n-1})$ with $r_0, \dots, r_{n-1} \in \mathbb{Z}$

has integer coefficients only when $r_0, \dots, r_{n-1}$ are all divisible by p.

Note: ~~[redacted]~~ Since $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_L$, whether $v \in \mathcal{O}_L$ only depends on the values $r_i \bmod p$, so it suffices to check p^n tuples $(r_0, \dots, r_{n-1}) \in \mathbb{F}_p^n$.

($\rightsquigarrow$ exponential running time in both n and $\log p$).

Better approach:

Def The radical of an ideal I of a ring R is the ideal

$$\mathrm{rad}(I) := \{r \in R \mid r^k \in I \text{ for some } k \geq 1\}.$$

Rmk $I \subseteq \mathrm{rad}(I) \subseteq R$.

Rmk If R is noetherian, then $\mathrm{rad}(I)^m \subseteq I$ for some $m \geq 1$.

Ex $\mathrm{rad}(\underbrace{p_1^{e_1} \cdots p_n^{e_n}\mathbb{Z}}_{\subseteq \mathbb{Z}}) = p_1 \cdots p_n \mathbb{Z}$.

Lemma 16.1.3 Let R be an order in a number field of degree n.

Then, $J_p(R) := \mathrm{rad}(pR) = \{r \in R \mid r^v \in pR\}$ for any $v \geq n$.

Pf "$\geq$" clear

"$\subseteq$" R is a $\mathbb{Z}$-module, $R \cong \mathbb{Z}^n$.

$\Rightarrow R/pR$ is an n-dimensional $\mathbb{F}_p$-vector space.

Let $r \in J_p(R)$. $\Rightarrow r^k \in pR$ for some $k \geq 1$.

$\Rightarrow$ The mult. by r map $m_r : R/pR \to R/pR$ is nilpotent.

$\Rightarrow$ Its n-th power is the zero map.

$\Rightarrow r^n \in pR$

$\Rightarrow r^v \in pR \ \forall v \geq n$. □

Rmk $R/pR \to R/p^sR$, $x \mapsto x^{p^s}$ is an $\mathbb{F}_p$-linear map for all $s \geq 0$.

If $p^s \geq n$, then $J_p(R)/pR$ is the kernel of this map according to the lemma.

Hence, we can efficiently compute $J_p(R)$.

Lemma 16.2.4 Let $J_p(R) = \mathrm{rad}(pR)$ as before and

let $T_p(R) := \{ x \in L \mid xJ_p(R) \subseteq J_p(R) \}$

Then,

a) $T_p(R)$ is an order in $\mathcal{O}_L$.

b) $R \subseteq T_p(R) \subseteq \frac{1}{p} \cdot R$

c) $R = T_p(R)$ if and only if R is p-maximal.

pf b) $R \subseteq T_p(R)$ is clear because $J_p(R)$ is an ideal of R.

If $x \in T_p(R)$, then $xp \in J_p(R) \subseteq R$ because $p \in J_p(R)$.

$\Rightarrow T_p(R) \subseteq \frac{1}{p} \cdot R$

a) Since $R \subseteq T_p(R)$ is an order, it suffices to show that $T_p(R) \subseteq \mathcal{O}_L$.

Let $x \in T_p(R)$.

R is a free $\mathbb{Z}$-module of rank n.

$\Rightarrow$ So is its ideal $J_p(R)$ (a submodule of finite index).

$\Rightarrow$ The multiplication by x map $m_x : J_p(R) \to J_p(R)$ is represented by an integral $n \times n$-matrix.

Its char. pol. $g(X)$ is a monic integral pol. of deg. n and $g(m_x) = 0$. $\Rightarrow g(x) = 0$.

$\Rightarrow x$ is integral $\Rightarrow x \in \mathcal{O}_L$.

c) "$\subseteq$" clear from def.

"$\supseteq$" Assume $x \in \mathcal{O}_L$, $x \notin R$.

Let $m \geq 1$ be sufficiently large that $J_p(R)^m \subseteq pR$.

Then, $x \cdot J_p(R)^m \subseteq R$.

"$\Rightarrow$" Consider the p-maximal order

$$R_p = \{x \in \mathcal{O}_L \mid p^k x \in R \text{ for some } k \geq 0\}.$$

$(R \subseteq R_p \subseteq \mathcal{O}_L)$.

Since R is a finitely generated $\mathbb{Z}$-module, there is a number $k \geq 0$ such that $p^k \cdot R_p \subseteq R$.

Also, pick $m \geq 1$ so that $\underbrace{J_p(R)}_{\text{rad}(pR)}{}^m \subseteq pR$.

$$\Rightarrow R_p \cdot J_p(R)^{km} \subseteq R_p \cdot p^k R \subseteq R.$$

Assume that R is not p-maximal.

$\Rightarrow R_p \neq R$, so in part. $R_p \notin R$.

$\Rightarrow$ There is a largest integer $i \geq 0$ (with $i < km$) such that $R_p \cdot J_p(R)^i \notin R$.

$\Rightarrow R_p \cdot J_p(R)^{i+1} \subseteq R$.

Let $x \in R_p \cdot J_p(R)^i$, but $x \notin R$.

$\Rightarrow x J_p(R) \subseteq R_p J_p(R)^{i+1} \subseteq R$.

For any $y \in J_p(R)$, we have

$$(xy)^{i+m+1} = \underbrace{\underbrace{x^{i+m+1}}_{\in R_p} \cdot \underbrace{y^{i+1}}_{\in J_p(R)^{i+1}}}_{\in R} \cdot \underbrace{y^m}_{\in J_p(R)^m \subseteq pR} \in pR,$$

so $xy \in \text{rad}(pR) = J_p(R)$.

Hence, $x \in T_p(R)$. But $x \notin R$, so indeed $R \neq T_p(R)$. $\square$

Rmk This gives a procedure for computing the ring of integers:

Start with $R = \mathbb{Z}[\alpha]$.
For every p with $p^2 \mid \mathrm{disc}(\bullet f)$:
    Keep replacing R by $T_p(R)$ until it stops changing.
Return R.

(T_p can also be computed by linear algebra mod p)

Note: If $R \subsetneq T_p(R)_{\mathfrak{p}} (\subseteq \frac{1}{p} \cdot R)$, then $p \mid [T_p(R) : R]$.

$\Rightarrow$ $\mathrm{disc}(R)$ always decreases by a factor of at least $\frac{1}{p^2}$.

See the references for details!