DEDEKIND DOMAINS.

Exercise 1. Let R be a UFD which is not a field. Show that R is a PID if and only if every nonzero prime ideal is maximal (i.e. every nonzero prime is of height 1). [Hint: consider the set Σ of all ideals in R which are not principal]

Exercise 2. Let R be a DVR with maximal ideal $\mathfrak{p}$ and $K = \operatorname{Frac} R$. Let L be a finite separable extension of K of prime degree. Show that the integral closure A of R in L is a DVR if and only if $\mathfrak{p}$ is either inert or totally ramified.

Exercise 3. Let K be a number field and $I \subseteq \mathcal{O}_K$ an ideal.

a) Show that for any $x \in I$ there exists an element $y \in I$ such that $I = (x, y)$. [Hint: use the approximation lemma (exercise 5.5)]

b) Show that there exists an integer $n \in \mathbb{N}$ and $y \in I$ such that $I = (n, y)$.

c) If $x, y \in K$, show that $I = (x, y)$ if and only if $\min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\} = v_{\mathfrak{p}}(I)$ for every prime $\mathfrak{p} \subset \mathcal{O}_K$.

d) Let p be a prime number, $\mathfrak{p} \subset \mathcal{O}_K$ a prime above p and $y \in \mathfrak{p}$. Show that $\mathfrak{p} = (p, y)$ if and only if either $v_p\left(N_{K/\mathbb{Q}}(y)\right) = f_{\mathfrak{p}}$ or $v_p\left(N_{K/\mathbb{Q}}(y + p)\right) = f_{\mathfrak{p}}$.

Exercise 4. Let A be a Dedekind domain, K its fraction field, M a finitely generated A-module, N_K a quotient of $M_K = K \otimes_R M$. Let N be the image of the composite map $M \to M_K \to N_K$.

a) Show that N is a flat R-module.

b) Show that if Q is a quotient of M flat as an R-module and such that $\ker[M_K \to K \otimes_R Q] = \ker[M_K \to N_K]$ then $N = Q$.

Exercise 5. Let $L = \mathbb{Q}(\alpha)$, where $\alpha^3 = 2$. Let $A = \mathbb{Z}[\alpha]$ and write $\mathcal{O}_L$ for the integral closure of $\mathbb{Z}$ in L.

a) Compute $\Delta(1, \alpha, \alpha^2)$.

b) Describe the decompostion of 2, 3, 5, 7 and 31 in L and compute the inertia and ramification degree above these primes.

c) Show that $A_{(p)} = \mathcal{O}_{L,(p)}$ for $p = 2, 3$. [Hint: use exercise 5.8]

d) Conclude that $A = \mathcal{O}_L$.

e) Recall the Hasse-Minkowsky bound: every class in $\operatorname{Pic} \mathcal{O}_L$ contains an integral ideal of norm less or equal to $\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{\mathfrak{d}_{\mathcal{O}_L/\mathbb{Z}}}$ (where in this case $n = 3$ and $r_2 = 1$ is half the number of complex embeddings of L). Conclude that $\operatorname{Pic} \mathcal{O}_L$ is trivial.

f) Compute a generator for each of the primes dividing 5.

SOLUTIONS

Exercise 1. A PID is a Dedekind domain, so every nonzero prime is maximal. Conversely, suppose that R is a UFD in which every nonzero prime is maximal. Forst notice that every maximal ideal $\mathfrak{m} \subset R$ is principal: if $0 \neq x \in \mathfrak{m}$ an irreducible factor y of x must be in $\mathfrak{m}$ and $(y) \subseteq \mathfrak{m}$ must be an equality because every nonzero prime is maximal.
Let now Σ be the set of all ideals in R which are not principal, ordered by inclusion and suppose that $\Sigma \neq \varnothing$. We want to derive a contradiction. As usual, if $I_1 \subseteq I_2 \subseteq \dots$ is a chain in Σ then $I_\infty = \bigcup_{n=1}^{\infty} I_n$ is an ideal. If $I_\infty = (z)$ then $z \in I_n$ for some $n \geq 1$ and then $I_n \subseteq I_\infty = (z) \subseteq I_n$, hence $I_n = I_\infty = (z) \notin \Sigma$. Therefore $I_\infty \in \Sigma$. We may thus apply Zorn's lemma to find a maximal element $I \in \Sigma$. Since $I \neq R = (1)$, it is contained in a maximal ideal: $I \subset \mathfrak{m} = (t)$. If $\{x_\alpha\}$ are generators for I, they are all divisible by t. Write $x_\alpha = t y_\alpha$ and let J be the ideal generated by all the y_α. Then $I = (t)J$, hence J is a proper ideal (since $t \notin I$) and $I \subsetneq J$, with strict strict inclusion because otherwise $J = (t)J = (t^2)J = \dots = (t^n)J = \dots$ hence every element in J would be divisible by t infinitely many times, thus $J = 0$, therefore $I = 0$ would be principal. Since J properly contains a maximal element, $J \notin \Sigma$ so $J = (z)$ hence $I = (t)(z) = (tz)$ is principal, contradiction.

Exercise 2. A is a DVR if and only if it is local, whence a unique prime $\mathfrak{q} \subset A$ above the maximal ideal $\mathfrak{p} \subset R$. Therefore $\mathfrak{p}A = \mathfrak{q}^e$ and from the formula $ef = [L : K]$ and the fact that $[L : K]$ is a prime, we conclude that A is a DVR if and only if either $e = [L : K]$ or $f = [L : K]$.

Exercise 3. Factor the ideals $(x) = \prod_{i=1}^{r} \mathfrak{q}_i^{a_i} = \prod_{i=1}^{r} \mathfrak{q}_i^{b_i} = I$, with $b_i \leq a_i$ for all $i = 1, \dots, r$. In view of the approximation lemma (exercise 5.5), we may find $y \in \mathcal{O}_K$ such that $v_{\mathfrak{q}_i}(y) = b_i$. Thus $y \in I$. Put $J = (x, y)$ and compute:

$$v_{\mathfrak{q}_i}(J) = \min\{v_{\mathfrak{q}_i}(x), v_{\mathfrak{q}_i}(y)\} = \min\{a_i, b_i\} = b_i \qquad i = 1, \dots, r$$

$$v_{\mathfrak{q}}(J) = \min\{v_{\mathfrak{q}}(x), v_{\mathfrak{q}}(y)\} = \min\{0, v_{\mathfrak{q}}(y)\} = 0 \qquad \mathfrak{q} \notin \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$$

therefore $(x, y) = J = I$. Since $I \cap \mathbb{Z} = (n)$ (as $\mathbb{Z}$ is a PID), we can take $n = x \in I$ as generator.

Recall that $N(\mathfrak{p}) = p^{f_\mathfrak{p}}$. Writing $(y) = \prod_{i=1}^{r} \mathfrak{q}_i^{v_{\mathfrak{q}_i}(y)}$, with $\mathfrak{q}_1 = \mathfrak{p}$, we have that

$$N_{K/\mathbb{Q}}(y) = \prod_{i=1}^{r} N(\mathfrak{q}_i)^{v_{\mathfrak{q}_i}(y)} = \prod_{i=1}^{r} (\mathfrak{q}_i \cap \mathbb{Z}))^{v_{\mathfrak{q}_i}(y) f_{\mathfrak{q}_i}} = p^{v_\mathfrak{p}(y) f_\mathfrak{p}} \prod_{i=2}^{r} (\mathfrak{q}_i \cap \mathbb{Z}))^{v_{\mathfrak{q}_i}(y) f_{\mathfrak{q}_i}} \tag{1}$$

Hence, if $v_p\left(N_{K/\mathbb{Q}}(y)\right) = f_\mathfrak{p}$ then necessarily $v_\mathfrak{p}(y) = 1$ and $\mathfrak{q}_i \nmid p\mathcal{O}_K$ for $i = 2, \dots, r$. Therefore $\min\{v_\mathfrak{q}(p), v_\mathfrak{q}(y)\} = v_\mathfrak{q}(\mathfrak{p})$ for every prime $\mathfrak{q} \subset \mathcal{O}_K$ and by c) we conclude that $\mathfrak{p} = (p, y)$. Similarly, if $v_p\left(N_{K/\mathbb{Q}}(y + p)\right) = f_\mathfrak{p}$, we conclude $\mathfrak{p} = (p, y + p) = (y, p)$.
Conversely, suppose $\mathfrak{p} = (p, y)$. Then $\min\{v_\mathfrak{p}(p), v_\mathfrak{p}(y)\} = 1$ and $\min\{v_\mathfrak{q}(p), v_\mathfrak{q}(y)\} = 0$ for every other prime $\mathfrak{q} \mid p\mathcal{O}_K$. This second condition forces $v_\mathfrak{q}(y) = 0$ for every $\mathfrak{q} \mid p\mathcal{O}_K$, $\mathfrak{q} \neq \mathfrak{p}$. Hence, if $v_\mathfrak{p}(y) = 1$, from equation (1) we get $v_p\left(N_{K/\mathbb{Q}}(y)\right) = f_\mathfrak{p}$. On the other hand, if $v_\mathfrak{p}(y) > 1$, then $v_\mathfrak{p}(p) = 1$, thus $1 \leq v_\mathfrak{p}(y + p) \leq \min\{v_\mathfrak{p}(p), v_\mathfrak{p}(y)\} = 1$ while $0 \leq v_\mathfrak{q}(y + p) \leq \min\{v_\mathfrak{q}(p), v_\mathfrak{q}(y)\} = 0$ for $\mathfrak{q} \neq \mathfrak{p}$ above p. Therefore $v_\mathfrak{p}(y + p) = 1$ and $v_\mathfrak{q}(y + p) = 0$ for every other prime $\mathfrak{q} \mid p\mathcal{O}_K$ and again we conclude $v_p\left(N_{K/\mathbb{Q}}(y)\right) = f_\mathfrak{p}$.

Exercise 4. N is flat because it is torsion-free, since it is a submodule of the K-vector space N_K.

If $\ker[M_K \to K \otimes_R Q] = \ker[M_K \to N_K]$ then $N_K = K \otimes_R Q$. Moreover, if Q is flat, the natural map $Q \to K \otimes_R Q$ is injective, so Q and N can be seen as submodules of N_K, and both coincide with the image of M,

Exercise 5. The minimal polynomial of α if X^3-2, hence that of α^2 is Y^3-4. Therefore $\Delta(1,\alpha,\alpha^2) = -N_{L/\mathbb{Q}}(3\alpha^2) = -3^3 N_{L/\mathbb{Q}}(\alpha^2) = -2^2 3^3$. Only 2 and 3 may ramify, and 3 ramifies for sure, as it appears with odd exponent. Moreover, $A\left[\frac{1}{6}\right] = \mathcal{O}_L\left[\frac{1}{6}\right]$.

$X^3-2 \equiv (X-3)(X^2+3X+9) \bmod 5$, and the quadratic factor is irreducible. Therefore $5\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$, with $e_1 = e_2 = f_1 = 1$ and $f_1 = 2$.

X^3-2 is irreducible mod 7, therefore 7 is inert in L.

$X^3-2 \equiv (X-4)(X-7)(X+11) \bmod 31$. Therefore 31 splits completely in L.

If we knew that $A = \mathcal{O}_L$, we would have $\mathcal{O}_L/2\mathcal{O}_L \cong \mathbb{Z}[X]/(2,X^3) \cong \mathbb{F}_2[X]/(X^3)$, hence $\mathcal{O}_L/(\alpha) \cong \mathbb{F}_2$ and thus (α) would be the only prime dividing two, totally ramified. Similarly mod 3, as $X^3-2 \equiv (X+1)^3$, so $(\alpha+1)$ is the only prime above 3 (notice $N_{L/\mathbb{Q}}(\alpha+1) = 3$), again totally ramified. However we can compute the decomposition of 2 and 3 withouth knowing that $A = \mathcal{O}_L$ as follows.
Write $(\alpha) = \prod_{i=1}^r \mathfrak{m}_i^{a_i}$. Since $(\alpha)^3 = 2\mathcal{O}_L$, the $\mathfrak{m}_i$ are primes dividing 2. Put $2\mathcal{O}_L = \prod_{i=1}^r \mathfrak{m}_i^{e_i}$. From $(\alpha)^3 = 2\mathcal{O}_L$ we get $3\left(\sum_{i=1}^r a_i f_i\right) = \sum_{i=1}^r e_i f_i = 3$. Looking for solutions $a_i \in \mathbb{N}$, the only possibility is $r = 1 = f_1 = a_1$ and $e_1 = 3$.
Similarly, putting $(\alpha+1) = \prod_{i=1}^r \mathfrak{n}_i^{b_i}$, from $(\alpha+1)^3 = 3\mathcal{O}_L$, we get that the $\mathfrak{n}_i$ are primes dividing 3 and $3\left(\sum_{i=1}^r b_i f_i\right) = \sum_{i=1}^r e_i f_i = 3$. Looking for solutions $a_i \in \mathbb{N}$, the only possibility is $r = 1 = f_1 = a_1$ and $e_1 = 3$.

From exercise 5.8, we now that $\Delta(1,\alpha,\alpha^2)\cdot\mathcal{O}_L \subseteq A$, so if $a+b\alpha+c\alpha^2 \in \mathcal{O}_L$, the denominator of the coefficients $a,b,c \in \mathbb{Q}$ divides 108. We look first for elements in $\mathcal{O}_L$ of the form $\frac{1}{2}(a+b\alpha+c\alpha^2)$, with $a,b,c \in \{0,1\}$. Since $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha) = \mathrm{Tr}_{L/\mathbb{Q}}(\alpha^2) = 0$, we get $\mathrm{Tr}_{L/\mathbb{Q}}\left(\frac{1}{2}(a+b\alpha+c\alpha^2)\right) = \frac{3a}{2}$, an integer only for $a = 0$. We also have $N_{L/\mathbb{Q}}(\frac{\alpha}{2}) = \frac{2}{8} \notin \mathbb{Z}$ and $N_{L/\mathbb{Q}}(\frac{\alpha^2}{2}) = \frac{4}{8} \notin \mathbb{Z}$, so we only need to check whether $\frac{\alpha+\alpha^2}{2} \in \mathcal{O}_L$. Computing the matrix of multiplication by this element in the basis $\{1,\alpha,\alpha^2\}$ we get

$$N_{L/\mathbb{Q}}\left(\frac{\alpha+\alpha^2}{2}\right) = \det\begin{pmatrix} 0 & 1 & 1 \\ \frac{1}{2} & 0 & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix} = \frac{3}{4} \notin \mathbb{Z} \quad \Longrightarrow \quad \frac{\alpha+\alpha^2}{2} \notin \mathcal{O}_L.$$

We conclude that $A\left[\frac{1}{3}\right] = \mathcal{O}_L\left[\frac{1}{3}\right]$. We could apply the same technique to prove that there are no elements in $\mathcal{O}_L$ of the form $\frac{1}{3}(a+b\alpha+c\alpha^2)$, with $a,b,c \in \{0,1,2\}$ to conclude that $A = \mathcal{O}_L$, but that is much longer as the trace does note provide useful information in this case. An alternative method (which we could also ahave used to prove that $A_{(2)} = \mathcal{O}_{L,(2)}$) is to notice that our computations above give that $(\alpha+1)\mathcal{O}_{L,(3)}$ is the only maximal ideal. Clearly $(\alpha+1)\mathcal{O}_{L,(3)} \cap A_{(3)} = (\alpha+1)A_{(3)}$, which is therefore a prime, in fact maximal by corollary 3.2.2. Moreover it is the only maximal ideal in $A_{(3)}$ by Kummer's lemma. Therefore $A_{(3)}$ is a local noetherian domain with principal maximal ideal: by proposition 5.1.5 it is a DVR, hence it is integrally closed, so coincides with its integral closure $\mathcal{O}_{L,(3)}$.

From Hasse-Minkowsky we get that every class in $\mathrm{Pic}\,\mathcal{O}_L$ contains an integral ideal of norm strictly less than 3. Since the only prime of norm 2 is principal, we conclude that $\mathrm{Pic}\,\mathcal{O}_L = \{1\}$.

Recall that if $\mathfrak{q} \subset \mathcal{O}_L$ is a prime ideal such that $\mathfrak{q}\cap\mathbb{Z} = q\mathbb{Z}$ with inertia degree f then $N(\mathfrak{q}) = q^f$. If $\beta \in \mathcal{O}_L$ then $\beta\mathcal{O}_L$ is divisible only by primes whise norm divides $N_{L/\mathbb{Q}}(\beta)$. By Kummer's lemma, the primes above 5 are $\mathfrak{q}_1 = (5,\alpha-3)$ and $\mathfrak{q}_2 = (5,\alpha^2+3\alpha+9)$. We have $N(\mathfrak{q}_i) = 5^i$. To find a generator of $\mathfrak{q}_1$ it suffices thus to find $\beta_1 \in \mathcal{O}_L$ such that $N_{L/\mathbb{Q}}(\beta_1) = 5$. Since $5\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2$, a generator for $\mathfrak{q}_2$ is then given by $\beta_2 = \frac{5}{\beta_1}$. Computing the matrix of multiplication by an element $y = a+b\alpha+c\alpha^2$ in the basis $\{1,\alpha,\alpha^2\}$ we get

$$N_{L/\mathbb{Q}}(y)) = \det\begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix} = a^3+2b^3+4c^3-6abc.$$

We immediately see a solution of $a^3+2b^3+4c^3-6abc = 5$ by taking $a = c = 1$ and $b = 0$, i.e. $\beta_1 = 1+\alpha^2$. Then $\beta_2 = \frac{5}{\beta_1} = 1+2\alpha-\alpha^2$.