Assignment 1

1. Let R be a Dedekind domain and let $I \neq 0$ be an ideal of R.

   (a) If $I = \mathfrak{p}_1 \dots \mathfrak{p}_n$ is the factorisation of I into prime ideals, then $I^{-1} = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_n^{-1}$.

   By Proposition 2.26, $\mathfrak{p}_j^{-1}\mathfrak{p}_j = R$ for $j = 1, \dots, n$. So $(\mathfrak{p}_1^{-1} \dots \mathfrak{p}_n^{-1})(\mathfrak{p}_1 \dots \mathfrak{p}_n) = R$, which tells us that $\mathfrak{p}_1^{-1} \dots \mathfrak{p}_n^{-1} \subseteq I^{-1}$.
   Conversely, suppose $x \in I^{-1}$, then $x \in K$ and $xI \subseteq R$, that is

   $$x\mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq R.$$

   Now we appeal to Proposition 2.26 once more and multiply both sides of this equality by $\mathfrak{p}_1^{-1} \dots \mathfrak{p}_n^{-1}$ to get $xR \subseteq \mathfrak{p}_1^{-1} \dots \mathfrak{p}_n^{-1}$, hence $x \in \mathfrak{p}_1^{-1} \dots \mathfrak{p}_n^{-1}$.

   (b) Show that $II^{-1} = R$.

   This follows directly from part (a) and Proposition 2.26.

2. Let $\mathcal{O}_K$ be the ring of integers in a number field K and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Prove that there exists a unique prime number $p \in \mathbb{Z}$ such that $p \in \mathfrak{p}$.

   As we have seen before, $\mathfrak{p}$ contains a nonzero integer: take any $\gamma \in \mathfrak{p}$, $\gamma \neq 0$, and consider $c = N(\gamma)$, then $c \in I$ and $c \neq 0$. If $c = \pm 1$ then $\mathfrak{p} = \mathcal{O}_K$, contradicting primality. Writing c as a product of prime numbers, we deduce that at least one of these prime numbers, call it p, is in $\mathfrak{p}$. Suppose that there is another prime, call it $q \neq p$, such that $q \in \mathfrak{p}$. Then $1 = \gcd(q, p) \in \mathfrak{p}$, contradicting primality.

3. Let θ be an algebraic integer, let f denote its minimal polynomial over $\mathbb{Q}$, and let $n = \deg f$. Assume that $n > 1$. Let $K = \mathbb{Q}(\theta)$ and let $\sigma_1, \dots, \sigma_n$ be the embeddings of K into $\mathbb{C}$.

   Prove that

   $$\Delta\big(1, \theta, \dots, \theta^{n-1}\big) = (-1)^{\binom{n}{2}} \prod_{j=1}^{n} f'\big(\sigma_j(\theta)\big).$$

   For readability, set $\theta_j = \sigma_j(\theta)$. The elements $\theta_1, \dots, \theta_n$ are the conjugates of θ, in other words the (complex) roots of the minimal polynomial f, that is

   $$f(x) = \prod_{i=1}^{n} \big(x - \theta_i\big).$$

   We can write the derivative of this as

   $$f'(x) = \sum_{i=1}^{n} \frac{f(x)}{\big(x - \theta_i\big)},$$

   so that for any $j = 1, \dots, n$ we have

   $$f'(\theta_j) = \prod_{i \neq j} \big(\theta_j - \theta_i\big).$$

Therefore

$$\prod_{j=1}^{n} f'(\theta_j) = \prod_{j=1}^{n}\prod_{i\neq j}\big(\theta_j-\theta_i\big) = \prod_{j<i}\big(\theta_j-\theta_i\big)\big(\theta_i-\theta_j\big)$$
$$= (-1)^{\binom{n}{2}}\prod_{j<i}\big(\theta_j-\theta_i\big)^2 = (-1)^{\binom{n}{2}}\Delta(1,\theta,\dots,\theta^{n-1}).$$

In the special case of $f(x) = x^n + ax + b$ for fixed $a, b \in \mathbb{Q}$, show that

$$\Delta\big(1,\theta,\dots,\theta^{n-1}\big) = (-1)^{\binom{n}{2}}\big(n^n b^{n-1} + a^n(1-n)^{n-1}\big).$$

We have

$$f'(x) = nx^{n-1} + a = \frac{nx^n + ax}{x},$$

therefore

$$f'(\theta_j) = \frac{n\theta_j^n + a\theta_j}{\theta_j} = \frac{-n(a\theta_j+b)+a\theta_j}{\theta_j} = -\frac{(1-n)a}{\theta_j}\left(\frac{nb}{(1-n)a} - \theta_j\right).$$

Plugging this into the formula we proved above we have (using $\theta_1\dots\theta_n = (-1)^n b$):

$$\Delta(1,\theta,\dots,\theta^{n-1}) = (-1)^{\binom{n}{2}}\frac{(1-n)^n a^n}{b} f\left(\frac{nb}{(1-n)a}\right) = (-1)^{\binom{n}{2}}\left(n^n b^{n-1} + (1-n)^{n-1}a^n\right).$$

4.

(a) Prove that any number field of degree 2 is of the form $\mathbb{Q}(\sqrt{d})$ for some squarefree $d \in \mathbb{Z}$.

Let K be a number field of degree 2 and let $\{1, \alpha\}$ be a $\mathbb{Q}$-basis for K. Write $\alpha^2 \in K$ in terms of this basis:

$$\alpha^2 = c + b\alpha,$$

then α is a root of the polynomial $x^2 - bx - c$, in other words $\alpha = \frac{b\pm\sqrt{b^2+4c}}{2} \in \mathbb{Q}(\sqrt{d})$, where d is the squarefree part of $b^2 + 4c$.
So $K \subseteq \mathbb{Q}(\sqrt{d})$, but the latter has degree 2 over $\mathbb{Q}$ so must have degree 1 over K, in other words $K = \mathbb{Q}(\sqrt{d})$.

(b) Prove that if $d_1 \neq d_2 \in \mathbb{Z}$ are squarefree, then the fields $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$ are not isomorphic.

Let's say that a rational number $d \neq 0, 1$ is squarefree if, when written in lowest terms, neither its numerator nor its denominator are divisible by the square of a prime number. Certainly $\sqrt{d} \notin \mathbb{Q}$ for any squarefree rational number d.
Now suppose we have an isomorphism $\varphi\colon \mathbb{Q}(\sqrt{d_1}) \to \mathbb{Q}(\sqrt{d_2})$ and let $a + b\sqrt{d_2} = \varphi(\sqrt{d_1})$. Then we must have $\big(a + b\sqrt{d_2}\big)^2 = d_1$, in other words

$$a^2 + 2ab\sqrt{d_2} + b^2 d_2 = d_1.$$

Since $\sqrt{d_2} \notin \mathbb{Q}$, this implies $ab = 0$.
If $a = 0$ then $b^2 d_2 = d_1$ so $b^2 = \frac{d_1}{d_2}$, which is only possible if $d_1 = d_2$, but that is false by hypothesis.
If $b = 0$ then $a^2 = d_1$, also a contradiction.

(c) Fix d squarefree and let $K = \mathbb{Q}(\sqrt{d})$. Compute the discriminant of the ring of integers $\mathcal{O}_K$.

We have seen in the lectures that an integral basis for $\mathcal{O}_K$ is given by

$$\begin{cases} 1, \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4 \\ 1, \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

In the first case the minimal polynomial of $\theta = \sqrt{d}$ is $x^2 - d$, so by Question 3 above we get $\Delta_K = \Delta(1, \theta) = 4d$.
In the second case the minimal polynomial of $\theta = \frac{1+\sqrt{d}}{2}$ is $x^2 - x - \frac{d-1}{4}$, so we get $\Delta_K = \Delta(1, \theta) = d$.

5. The following is an alternative construction of the ideal class group of a Dedekind ring R.

(a) We say that two ideals I and J of R are *equivalent* if $aI = bJ$ for some nonzero $a, b \in R$. Prove that this is indeed an equivalence relation.

Clearly $1I = 1I$ so $I \sim I$.
If $I_1 \sim I_2$ so $a_1 I_1 = a_2 I_2$ then $a_2 I_2 = a_1 I_1$ so $I_2 \sim I_1$.
Suppose $I_1 \sim I_2$, say $a_1 I_1 = a_2 I_2$. Suppose also that $I_2 \sim I_3$, say $b_2 I_2 = b_3 I_3$. Then

$$(a_1 b_2) I_1 = b_2 (a_1 I_1) = b_2 (a_2 I_2) = a_2 (b_2 I_2) = a_2 (b_3 I_3) = (a_2 b_3) I_3,$$

so $I_1 \sim I_3$.

(b) Suppose $I_1 \sim I_2$ and $J_1 \sim J_2$. Prove that $I_1 J_1 \sim I_2 J_2$.

Say $a_1 I_1 = a_2 I_2$ and $b_1 J_1 = b_2 J_2$. Then $(a_1 b_1)(I_1 J_1) = (a_1 I_1)(b_1 J_1) = (a_2 I_2)(b_2 J_2) = (a_2 b_2)(I_2 J_2)$, so $I_1 J_1 \sim I_2 J_2$.

Use this to show that ideal multiplication defines an abelian group structure on the set $\widetilde{\mathrm{Cl}}(R)$ of equivalence classes of nonzero ideals of R.

We define the group operation by $[I][J] := [IJ]$. The property proved above shows that this operation is well-defined (independent of choice of representatives of the equivalence classes).
The associativity and commutativity follow from the corresponding properties of multiplication of ideals, which in turn follow from the corresponding properties of multiplication of elements of R.
The identity element is the class $[R]$, as $IR = I$ for all ideals I.
Checking that every class is invertible uses some nontrivial results. Consider a class $[I]$. We know that I^{-1} is a fractional ideal of R, so there exists $d \in R$ such that $J := dI^{-1}$ is an ideal in R. We also know that $II^{-1} = R$, so $IJ = dII^{-1} = dR$, in other words $[I][J] = [R]$.

(c) Prove that $\widetilde{\mathrm{Cl}}(R)$ is isomorphic to $\mathrm{Cl}(R)$ as groups.

Just for the duration of this solution, write $\{J\}$ for the coset of the fractional ideal J in $\mathrm{Cl}(R)$. Consider the map $\varphi\colon \widetilde{\mathrm{Cl}}(R) \to \mathrm{Cl}(R)$ given by $\varphi([I]) = \{I\}$.
This is well-defined: if $J \sim I$ so that $bJ = aI$, then $\{J\} = \{\frac{a}{b} I\} = \{\frac{a}{b} R\}\{I\} = \{I\}$.
It is a group homomorphism by the definition of multiplication of (fractional) ideals.
It is surjective: given a class $\{J\}$ for some fractional ideal J, there exists $d \in R$ such that $I := dJ$ is an ideal of R, and $\varphi([I]) = \{I\} = \{dJ\} = \{dR\}\{J\} = \{J\}$.
It is injective: suppose I_1, I_2 are ideals of R such that $\{I_1\} = \{I_2\}$. Then there exists $\frac{a_2}{a_1} \in K = \mathrm{Frac}(R)$ such that $I_1 = \frac{a_2}{a_1} I_2$ as fractional ideals. Therefore $a_1 I_1 = a_2 I_2$, which is now an identity of ideals and says that $[I_1] = [I_2]$.

6. Let R be a Noetherian integral domain with fraction field K. Prove that $J \subseteq K$ is a fractional ideal of R if and only if it is a finitely-generated R-submodule of K.

   If J is a fractional ideal of R then there exists a nonzero $d \in R$ such that $dJ \subseteq R$. Let $I = dJ$, then I is an ideal of R, and since R is Noetherian we know that I is finitely generated as an ideal, say
   $$I = a_1R + \cdots + a_nR, \qquad a_j \in R.$$
   But then
   $$J = \frac{1}{d}\, I = \frac{a_1}{d}\, R + \cdots + \frac{a_n}{d}\, R$$
   is a finitely-generated R-submodule of K.
   Conversely, suppose
   $$J = \frac{a_1}{b_1}\, R + \cdots + \frac{a_n}{b_n}\, R, \qquad a_j \in R, b_j \in R \setminus \{0\}.$$
   Let $d = b_1 \dots b_n \in R$, then $dJ \subseteq a_1R + \cdots + a_nR \subseteq R$. So J is a fractional ideal.

7. Let K be a number field and $\beta \in K$. Let $m_\beta \colon K \to K$ denote the $\mathbb{Q}$-linear transformation given by $m_\beta(x) = \beta x$. Prove that
   $$|N(\beta)| = |\det(m_\beta)|.$$

   Take a $\mathbb{Q}$-basis $\omega_1, \dots, \omega_n$ for K. Let M_β be the matrix representation of m_β with respect to this basis, then
   $$\begin{bmatrix} \beta\omega_1 \\ \vdots \\ \beta\omega_n \end{bmatrix} = M_\beta \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_n \end{bmatrix}$$
   Therefore
   $$\Delta(\beta\omega_1, \dots, \beta\omega_n) = \det(M_\beta)^2 \Delta(\omega_1, \dots, \omega_n).$$
   On the other hand
   $$\begin{aligned} \Delta(\beta\omega_1, \dots, \beta\omega_n) &= \det\big(\sigma_i(\beta\omega_j)\big)^2 \\ &= \det\big(\sigma_i(\beta)\sigma_i(\omega_j)\big)^2 \\ &= \sigma_1(\beta)^2 \dots \sigma_n(\beta)^2 \det\big(\sigma_i(\omega_j)\big)^2 \\ &= N(\beta)^2 \Delta(\omega_1, \dots, \omega_n). \end{aligned}$$
   So $|N(\beta)| = |\det(M_\beta)|$.

8. Let $R = \mathbb{C}[X, Y]/(Y^2 - X^3)$. Is R a Dedekind domain?

   No, R is not a Dedekind domain because it is not integrally closed.
   Let $x \in R$ be the image of X and let $y \in R$ be the image of Y. Consider $t = \frac{y}{x} \in K = \operatorname{Frac} R$. Suppose $t \in R$, then t can be represented as a polynomial of degree 1 in y (using the relation $y^2 = x^3$), so
   $$t = f(x)y + g(x) \qquad \Rightarrow \qquad y = f(x)xy + g(x)x.$$
   Lifting this to $\mathbb{C}[X, Y]$, we get
   $$Y - f(X)XY - g(X)X = h(X, Y)(Y^2 - X^3),$$
   which is contradictory because (modulo some trivial corner cases) the degree in Y on the left is 1, while the degree in Y on the right is 2.
   So $t \notin R$. However $t^2 - x = \frac{y^2}{x^2} - x = \frac{y^2 - x^3}{x^2} = 0$, which is a monic equation with coefficients in R, so t is integral over R.