Problem Set #5

Let prove first a result extending the one of \( \mathbb{Z} \), if \( a = \prod_i p_i^{e_i} \) and \( b = \prod_i p_i^{f_i} \) where the \( p_i \)'s are maximal ideal, then

\[
\begin{align*}
a + b &= \prod_i p_i^{\min(e_i,f_i)} \\
a \cap b &= \prod_i p_i^{\max(e_i,f_i)}.
\end{align*}
\]

Note that \( a + b \) is the smallest ideal containing \( a \) and \( b \) and \( a \cap b \) is the smallest ideal contained in \( a \) and \( b \). The results follows then from the fact, that \( \prod_i p_i^{e_i} \subseteq \prod_i p_i^{f_i} \) if and only if \( e_i \geq f_i \), for all \( i \).

Exercise 5 p 23 of [N]:
The quotient ring \( \mathcal{O}/a \) of a Dedekind domain by an ideal \( a \neq 0 \) is a principal ideal domain.

Solution:
By Chinese remainder theorem, it is enough to prove the result for \( a \) of the form \( p^n \) where \( p \) is a prime ideal. The ideal of \( \mathcal{O}/a \) are in bijection with the ideals of \( \mathcal{O} \) dividing \( p^n \), that is \( p^i \) for \( i = 0, \ldots, n \). So the proper ideal of \( \mathcal{O}/a \) are exactly \( p^i / p^n \), \( \ldots \), \( p^i / p^n \). Let now \( \pi \in p \setminus p^2 \). Then, \( p^\mu = (\pi^\mu) + p^n \) for any \( \mu = \{1, \ldots, n\} \), since they have the same prime factorization (see above for prime factorization of the sum). So, that we have the result.

Exercise 6 p 23 of [N]
Every ideal of a Dedekind domain can be generated by two elements.

Solution:
Let \( a \) be a nonzero ideal of a Dedekind domain \( \mathcal{O} \). Then, \( \mathcal{O}/a \) is a PID, in particular, for \( a \neq 0 \) in \( \mathcal{O} \) we have that \( (a)/a \) is principal so that there is \( b \in \mathcal{O} \) such that \( (a)/a = (b) \) so that \( (a) + (b) = a \).

Direct proof: Let \( a = \prod_i p_i^{f_i} \) as a finite product and choose \( a \in A \) with \( v_{p_i}(a) = f_i \), so that \( (a) = I \prod_i q_i^{e_i} \), also a finite product where the \( q_i \) are different from all \( p_i \). Choose \( b \in A \) with \( v_{p_i}(b) = f_i + 1 \) and \( v_{q_i} = 0 \) (always possible by chinese remainder theorem). Then, \( I = (a) + (b) \) (see above for prime factorization of the sum).

Exercise 3 p 28 of [N] (Minkowski’s Theorem on Linear forms).
Let

\[
L_i(x_1, \ldots, x_n) = \sum_{j=1}^{n} a_{i,j}x_j, \quad i = 1, \ldots, n
\]
be a real form such that $\det(a_{i,j})$, and let $c_1, ..., c_n$ be positive real number such that $c_1, ..., c_n > |\det(a_{i,j})|$. Show that there exist integers $m_1, ..., m_n \in \mathbb{Z}$ such that

$$|L_i(m_1, ..., m_n)| < c_i, \ i = 1, ..., n$$

Solution:
Let $\mathcal{C} = \{x \in \mathbb{R}^n : |\sum a_{i,j}x_j| < c_j, \ 1 \leq i \leq n\}$. Note that $|\sum a_{i,j}x_j| < c_j, \ 1 \leq i \leq n$ is equivalent to $Ax = c$ where $x = (x_1, ..., x_n)^t$ and $c = (c_1, ..., c_n)^t$. Consider the lattice $AZ^n = a_1\mathbb{Z} + ... + a_n\mathbb{Z}$ where the $a$'s are the columns of $A$ linearly independent since $\det(A) \neq 0$. Then $\det(AZ^n) = |\det(A)|$, so that $\text{vol}(\mathcal{C}) = (2^n c_1 ... c_n)/|\det(A)|$. Now, consider the lattice $\Gamma = Z^n$, then $2^n\text{vol}(\Gamma) = 2^n < \text{vol}(\mathcal{C})$ and by Minkowski’s lattice point theorem, there is $x \in \mathbb{Z}^n$ nonzero with $x \in \mathcal{C}$. 