Dr. Marques Sophie
Office 519

Number theory

Spring Semester 2013
marques@cims.nyu.edu

Problem Set #5

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

$$\mathfrak{a} + \mathfrak{b} = \prod_i \mathfrak{p}_i^{min(e_i,f_i)} \text{ and } \mathfrak{a} \cap \mathfrak{b} = \prod_i \mathfrak{p}_i^{max(e_i,f_i)}.$$

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

Exercise 5 p 23 of [N]:
The quotient ring $\mathcal{O}/\mathfrak{a}$ of a Dedekind domain by an ideal $\mathfrak{a} \neq 0$ is a principal ideal domain.
Solution:
By Chinese remainder theorem, it is enough to prove the result for $\mathfrak{a}$ of the form $\mathfrak{p}^n$ where $\mathfrak{p}$ is a prime ideal. The ideal of $\mathcal{O}/\mathfrak{a}$ are in bijection with the ideals of $\mathcal{O}$ dividing $\mathfrak{p}^n$, that is $\mathfrak{p}^i$ for $i = 0, ..., n$. So the proper ideal of $\mathcal{O}/\mathfrak{a}$ are exactly $\mathfrak{p}/\mathfrak{p}^n$, .. , $\mathfrak{p}/\mathfrak{p}^n$. Let now $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$. Then, $\mathfrak{p}^\mu = (\pi^\mu) + \mathfrak{p}^n$ for any $\mu = \{1, .., n\}$, 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 $\mathfrak{a}$ be a nonzero ideal of a Dedekind domain $\mathcal{O}$. Then, $\mathcal{O}/\mathfrak{a}$ is a PID, in particular, for $a \neq 0$ in $\dashv$ we have that $(a)/\mathfrak{a}$ is principal so that there is $b \in \mathcal{O}$ such that $(a)/\mathfrak{a} = (b)$ so that $(a) + (b) = \mathfrak{a}$.
Direct proof: Let $\mathfrak{a} = \prod_i \mathfrak{p}_i^{f_i}$ as a finite product and choose $a \in A$ with $v_{\mathfrak{p}_i}(a) = f_i$, so that $(a) = I \prod \mathfrak{q}_i^{e_i}$, also a finite product where the $\mathfrak{q}_i$ are different from all $\mathfrak{p}_i$. Choose $b \in A$ with $v_{\mathfrak{p}_i}(b) = f_i + 1$ and $v_{\mathfrak{q}_i} = 0$ (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

$$L_i(x_1, ..., x_n) = \sum_{j=1}^{n} a_{i,j} x_j, \ i = 1, ..., n$$

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* $A\mathbb{Z}^n = a_1\mathbb{Z} + ... + a_n\mathbb{Z}$ *where the* $a's$ *are the columns of* A *linearly independent since* $det(A) \neq 0$. *Then* $det(A\mathbb{Z}^n) = |det(A)|$, *so that* $vol(\mathcal{C}) = (2^n c_1...c_n)/|det(A)|$. *Now, consider the lattice* $\Gamma = \mathbb{Z}^n$, *then* $2^n vol(\Gamma) = 2^n <$ $vol(\mathcal{C})$ *and by Minkowski's lattice point theorem, there is* $x \in \mathbb{Z}^n$ *nonzero with* $x \in \mathcal{C}$.