Math 80220 Algebraic Number Theory
Problem Set 2

Andrei Jorza

Due Friday, February 9

You may use the fact that in a Dedekind domain every ideal can be factored uniquely as a product of prime ideals.

1. Show that every PID is integrally closed and conclude that $\mathbb{Z}[\sqrt{-163}]$ is not a Euclidean domain.
2. Show that 2 and 3 are irreducible elements of $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ and that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]^\times = \{\pm 1\}$. (Recall that we used this in lecture.)
3. Show that $14 = 2 \cdot 7 = (1+\sqrt{-13})(1-\sqrt{-13})$ are two distinct factorizations into irreducible elements of $\mathbb{Z}[\sqrt{-13}]$. What is the factorization of 14 into prime ideals of $\mathbb{Z}[\sqrt{-13}]$?
4. If R is a Dedekind domain, $\mathfrak{p}$ is a prime ideal of R and I is any ideal let $v_\mathfrak{p}(I)$ be the exponent of $\mathfrak{p}$ in the unique factorization of I into prime ideals. If $x \in R$ then $v_\mathfrak{p}(x) = v_\mathfrak{p}((x)R)$.
   (a) Suppose R is a Dedekind domain, $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are prime ideals of R and $e_1, \dots, e_n \in \mathbb{Z}$. Use the Chinese Remainder Theorem to show that there exists $x \in \operatorname{Frac} R$ such that $v_{\mathfrak{p}_i}(x) = e_i$ for all i.
   (b) Conclude that if R is a Dedekind domain with finitely many prime ideals then R is a PID.
   (c) Suppose R is a Dedekind domain with finitely many prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. Show that R is a Euclidean domain with Euclidean function $d(r) = \sum v_{\mathfrak{p}_i}(r)$. [Hint: reduce to the case when m and n are coprime and then use the Chinese Remainder Theorem to find the residue r coprime to all prime ideals $\mathfrak{p}_i$ not dividing n.]

   Remark 1. Suppose R is a Dedekind domain and I is an ideal of R. Let $R_{(I)}$ be the subring of $\operatorname{Frac}(R)$ consisting of fractions $\frac{m}{n}$ whose denominators are coprime to I. Then the prime ideals of $R_{(I)}$ are precisely the (finitely many) prime ideals dividing I.

   The remaining two exercises are standard in Algebra 3 and I include them for fun. You don't have to write them up.
5. The Euclidean domain (necessarily a PID) $\mathbb{Z}[\zeta_3]$.
   (a) If p is a prime $\equiv 2 \pmod 3$ and $p \mid x^2 + xy + y^2$ with $x, y \in \mathbb{Z}$ show that $p \mid x, y$. [Hint: $p - 1 \equiv 1 \pmod 3$.]
   (b) If p is a prime $\equiv 1 \pmod 3$ show that $p \mid a^2 + a + 1$ for some integer a. [Hint: $\mathbb{F}_p^\times$ is cyclic.]
   (c) If $p \equiv 1 \pmod 3$ is a prime in $\mathbb{Z}$ which is also a prime in $\mathbb{Z}[\zeta_3]$ then p cannot divide $a^2 + a + 1 = (a - \zeta_3)(a - \zeta_3^2)$ and conclude that p is reducible. Deduce that $p = x^2 + xy + y^2$ for some $x, y \in \mathbb{Z}$.
   (d) Suppose $n = 3^k \prod_{p \equiv 1 \pmod 3} p^{n_p} \prod_{q \equiv 2 \pmod 3} q^{m_q}$ is a positive integer. Show that $x^2 + xy + y^2 = n$ has solutions with $x, y \in \mathbb{Z}$ only if m_q are all even in which case the solutions can be enumerated as
   $$x - y\zeta_3 = u(1-\zeta_3)^k \prod_{p \equiv 1 \pmod 3} (a_p - b_p\zeta_3)^{u_p}(a_p - b_p\zeta_3^2)^{n_p - u_p} \prod_{q \equiv 2 \pmod 3} q^{m_q/2}$$

where $u \in \mathbb{Z}[\zeta_3]^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$, $p = a_p^2 + a_p b_p + b_p^2$ and $0 \le u_p \le n_p$. Conclude that the number of solutions is $6(d_+(n) - d_-(n))$ where $d_\pm(n)$ is the number of divisors of n which are $\equiv \pm 1 \pmod 3$.

6. The Euclidean domain (necessarily a PID) $\mathbb{Z}[i]$.

   (a) If p is a prime $\equiv 3 \pmod 4$ and $p \mid x^2 + y^2$ for $x, y \in \mathbb{Z}$ show that $p \mid x, y$. [Hint: $(p-1)/2$ is odd!]

   (b) If $p \equiv 1 \pmod 4$ show that $p \mid a^2 + 1$ for some a. [Hint: Either use the fact that $\mathbb{F}_p^\times$ is cyclic or show that $a = \left(\frac{p-1}{2}\right)!$ works.]

   (c) Show that if p a prime $\equiv 1 \pmod 4$ is also prime in $\mathbb{Z}[i]$ then p cannot divide $a^2+1 = (a+i)(a-i)$ and conclude that p cannot be prime in $\mathbb{Z}[i]$. Deduce that $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.

   (d) Suppose $n = 2^k \prod_{p \equiv 1 \pmod 4} p^{n_p} \prod_{q \equiv 3 \pmod 4} q^{m_q}$ is a positive integer. Show that $x^2 + y^2 = n$ has solutions with $x, y \in \mathbb{Z}$ only if m_q are all even in which case the solutions can be enumerated as

$$x + iy = u(1+i)^k \prod_{p \equiv 1 \pmod 4} (a_p + b_p i)^{u_p} (a_p - b_p i)^{n_p - u_p} \prod_{q \equiv 3 \pmod 4} q^{m_q/2}$$

   where $p = a_p^2 + b_p^2$, $u \in \{\pm 1, \pm i\}$ and $0 \le u_p \le n_p$. Conclude that the number of solutions is $4(d_+(n) - d_-(n))$ where $d_\pm(n)$ is the number of divisors of n which are $\equiv \pm 1 \pmod 4$.