MATH 435 ASSIGNMENT 5

ARNOLD JIADONG YU

1. Chapter 18 Divisibility in Integral Domains

1.1. 1. For the ring $Z[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in Z\}$, where $d \neq 1$ and d is not divisible by the square of a prime, prove that the norm $N(a + b\sqrt{d}) = |a^2 - db^2|$ satisfies the four assertions made preceding Example 1. (This exercise is referred to in this chapter)
proof:

(1)WTS $N(x) = 0$ iff $x = 0$.
($\Rightarrow$) Let $N(x) = 0$, then $a^2 = db^2$. Since $d \neq 1$. If $a \neq 0$ and $a \in Z$, a has unique prime factorization call it $q_1, ..., q_n$ where $q_i \neq q_j$ for $i \neq j$. Then $q_i^2 | d$ for some integer i between 1 and n. But d is not divisible by the square of a prime. A contradiction, then $a = 0 \Rightarrow a = b = 0$. Hence $x = a + b\sqrt{d} = 0$.
($\Leftarrow$) Let $x = 0$, then $a = b = 0$. Hence $|a^2 - db^2| = 0$. i.e. $N(x) = 0$.
(2) $N(xy) = N(x)N(y)$ for all x and y.
Let $a + b\sqrt{d}, s + t\sqrt{d} \in Z[\sqrt{d}]$, then

$$N(a + b\sqrt{d})N(s + t\sqrt{d}) = |a^2 - db^2||s^2 - dt^2|$$
$$= |(a^2 - db^2)(s^2 - dt^2)| = |a^2s^2 - db^2s^2 - dt^2a^2 + d^2b^2t^2|$$

Moreover,

$$N(((a + b\sqrt{d})(s + t\sqrt{d})) = N(as + dbt + (bs + at)\sqrt{d})$$
$$= ||(as + dbt)^2 - d(bs + at)^2 = |a^2s^2 - db^2s^2 - dt^2a^2 + d^2b^2t^2|$$

Hence $N(xy) = N(x)N(y)$ for all x and y.
(3) x is a unit iff $N(x) = 1$.
($\Rightarrow$) Let x be a unit. There exist a $y \in Z[\sqrt{d}]$, s.t. $xy = 1$. Moreover, from part (2), choose $b = 1, N(ab) = N(a \cdot 1) = N(a)N(1) \Rightarrow N(1) = 1$. i.e. $N(xy) = N(1) \Rightarrow N(x)N(y) = 1$. Since $N(x), N(y)$ are both non-negative integer, then $N(x) = 1$.
($\Leftarrow$) Let $N(x) = 1$, then $N(a + \sqrt{b}) = |a^2 - db^2| = 1 \Rightarrow |(a + b\sqrt{d})(a - b\sqrt{d})| = 1$, i.e. $x = a + b\sqrt{d}$ is a unit.
(4) If $N(x)$ is prime, then x is irreducible in $Z[\sqrt{d}]$
If x is irreducible, then x is not a unit and $x = yz \Rightarrow y$ or z is a unit.

Suppose $N(x)$ is prime, and x is not irreducible in $Z[\sqrt{d}]$. Therefore, there exists $y, z \in Z[\sqrt{d}]$, s.t y or z is not unit and $x = yz$. Since y, z are not unit, then $N(y) \neq 1, N(z) \neq 1$ by part 3. Moreover $N(x) = N(yz) = N(y)N(z)$, i.e. $N(x)$ is not prime because it is the product of $N(y), N(z)$ where $N(y) \neq 1, N(z) \neq 1$. A contradiction. Hence x is irreducible in $Z[\sqrt{d}]$.

1.2. 3. Show that the union of a chain $I_1 \subset I_2 \subset ...$ of ideals of a ring R is an ideal of R. (This exercise if referred to in this chapter.)
proof: Let $I = \bigcup I_i$, and $a, b \in I$. Then there exists $k, j \in \mathbb{N}$ such that $a \in I_j, b \in I_k$. WLOG, assume $I_j \subseteq I_k$. i.e. $a - b \in I_k$ since $I_j \subseteq I_k$ and I_j, I_k are ideals. Therefore, $a - b \in I$ since $I_k \in I$.
Let $r \in R$, then ra and ar are in I_j whenever $a \in I_j$ and $r \in R$. Since $I_j \in I$, it follows ra and ar are in I too.
Hence I is an ideal of R.

1.3. 8. Let D be a Euclidean domain with measure d. Prove that u is a unit in D if and only if $d(u) = d(1)$.
proof: ($\Rightarrow$) Suppose u is a unit in D, then $ud = 1$ for some $d \in D$. i.e.

$$d(u) \leq d(ud) = d(1)$$

Moreover

$$d(1) \leq d(1u) = d(u)$$

Therefore, $d(u) = d(1)$.
($\Leftarrow$) Suppose $d(u) = d(1)$, and $u, 1 \in D$ with $1 \neq 0$, then there exists elements q and r in D such that $1 = uq + r$, where $r = 0$ or $d(r) < d(u)$. Moreover,

$$d(u) = d(1) \leq d(1r) = d(r)$$

Then $r = 0$, i.e. $1 = uq$ and u is a unit.
Hence, u is a unit in D if and only if $d(u) = d(1)$.

1.4. 14. Show that $1 - i$ is an irreducible in $Z[i]$.
proof: Suppose $1 - i$ is not irreducible in $Z[i]$, then $\exists x, y \in Z[i]$ s.t. x, y is not unit and $1 - i = xy$. Consider the norm function,

$$N : Z[i] \to Z_{\geq 0}$$

$$N : a + bi \mapsto a^2 + b^2$$

Then by question 1, we can get

$$N(xy) = N(1 - i) = 2 = N(x)N(y)$$

Since $N(xy) = N(x)N(y)$. Moreover x, y is not unit, then $N(x) \neq 1, N(y) \neq 1$. But $N(x)N(y) = 2$ and both $N(x), N(y)$ are positive integers. i.e $N(x) = 1$ or $N(y) = 1$, a contradiction. Hence $1 - i$ is an irreducible in $Z[i]$

1.5. 28. For a commutative ring with unity we may define associates, irreducible, and primes exactly as we did for integral domains. With these definitions, show that both 2 and 3 are prime in Z_{12} but 2 is irreducible and 3 is not.
proof: Z_{12} is not integral domain since it has zero-divisors. The unit in Z_{12} is $1, 5, 7, 11$. Therefore, $2, 3$ are not unit. Suppose 2 divide ab where $a, b \in Z_{12}$, then $2c = ab$ for some $c \in Z_{12}$. i.e. $ab - 2c = 0 \Rightarrow ab - 2c = 12x$ for some $x \in Z_{12}$. Therefore, $ab = 2c + 12x = 2(c + 6x)$. i.e. $2|a$ or $2|b$.
Suppose 3 divide ab where $a, b \in Z_{12}$, then $3c = ab$ for some $c \in Z_{12}$. i.e. $ab - 3c = 0 \Rightarrow ab - 3c = 12x$ for some $x \in Z_{12}$. Therefore, $ab = 3c + 12x = 3(c + 4x)$. i.e. $3|a$ or $3|b$.
Suppose 2 is not irreducible, then $2 = ab$ for some $a, b \in Z_{12}$, and a, b are nonunits and nonzeros. i.e. $a, b \in \{2, 3, 4, 6, 8, 9, 10\}$.

Z_{12}	2	3	4	6	8	9	10
2	4	6	8	0	4	6	8
3	6	9	0	4	0	3	6
4	8	0	4	0	8	0	4
6	0	4	0	0	0	6	0
8	4	0	8	0	4	0	0
9	6	3	0	6	0	9	6
10	8	6	4	0	8	6	4

By observing the Cayley table, 2 is not inside, therefore such a, b does not exist. Hence 2 is irreducible. By observing the same table, we see $3 = 3 \cdot 9$, i.e. 3 is not irreducible.

1.6. * 36. Show that an integral domain with the property that every strictly decreasing chain of ideals $I_1 \supset I_2 \supset ...$ must be finite in length is a field.
proof:

1.7. 37. An ideal A of a commutative ring R with unity is said to be *finitely generated* if there exist elements $a_1, a_2, ..., a_n$ of A such that $A = \langle a_1, a_2, ..., a_n \rangle$. An integral domain R is said to satisfy the *ascending chain condition* if every strictly increasing chain of ideals $I_1 \subset I_2 \subset ...$ must be finite in length. Show that an integral domain R satisfies the ascending chain condition if and only if every ideal of R is

finitely generated.
proof: ($\Rightarrow$) Prove by contrapositive. Assume every ideal of R is not finitely generated. Let I be an ideal, and $a_0 \in I$. Then $\langle a_0 \rangle \subsetneq I$ since i is not finitely generated. There exists $a_1 \in I \backslash \langle a_0 \rangle$ s.t. $\langle a_0 \rangle \subsetneq \langle a_0, a_1 \rangle$. Continue doing this and find out this strictly increasing chain of ideals is infinite in length. Hence if an integral domain R satisfies the ascending chain condition then every ideal of R is finitely generated.
($\Leftarrow$) Suppose every ideal of R is finitely generated, and there exists a strictly increasing chain of ideals $I_1 \subset I_2 \subset I_3 ...$, WTS it is finite. Let $I = \bigcup I_i$, then I is an ideal. Moreover $I = \langle a_1, ..., a_n \rangle$ where n is finite and I contains all strictly increasing chain of ideals. Then the smallest ideal we can construct is $\langle a_i \rangle$ where $a_i \in I$ for some i between 1 and n. WLOG, assmue it is a_1, since $I_1 \subset I_2$ and $I_1 \neq I_2$, then I_2 is at least $\langle a_i, a_i \rangle$ for $a_i \in I$ and $i \neq 1$.. Continue this process, this will terminate at I. i.e. there will be no more than n ideals that follow strictly increasing chain properties. Since n is finite, then the strictly increasing chain of ideals must be finite.
Hence an integral domain R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.

1.8. * 44. Let F be a field and let R be the integral domain in $F[x]$ generated by x^2 and x^3. (That is, R is contained in every integral domain in $F[x]$ that contains x^2 and x^3.) Show that R is not a unique factorization domain.
proof: