MAT 534: HOMEWORK 7

DUE TH, OCT 23

1. Prove that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

2. Determine the greatest common divisor in $\mathbb{Q}[x]$ of $a(x) = x^3 + 4x^2 + x - 6$ and $b(x) = x^5 - 6x + 5$ and write it as a linear combination of $a(x)$ and $b(x)$.

3. (a) Prove that every $a \in \mathbb{Z}$ can be uniquely written in the form

$$a = \pm p_1^{n_1} \dots p_k^{n_k} (q_1\overline{q_1})^{m_1} \dots (q_l\overline{q_l})^{m_l}$$

where $p_i \in \mathbb{Z}$ are integers which are prime(=irreducible) as elements of $\mathbb{Z}[i]$, and $q_i \in \mathbb{Z}[i]$ are irreducible elements of $\mathbb{Z}[i]$ which are not in $\mathbb{Z}$.

(b) Prove that a prime number $p \in \mathbb{Z}_+$ remains irreducible in $\mathbb{Z}[i]$ iff equation $a^2+b^2 = p$ has no integer solutions. (Hint: $a^2 + b^2 = (a + bi)(a - bi)$.) Deduce from this that prime numbers of the form $4k + 3$ remain irreducible in $\mathbb{Z}[i]$. (In fact, it is known that a prime integer number is irreducible in $\mathbb{Z}[i]$ iff it has the form $4k + 3$.)

(c) Assuming the statement given in the previous part, prove that for a positive integer n the following statements are equivalent:

- n can be written as sum of two squares of integer numbers
- n can be written in the form $n = z\overline{z}$, $z \in \mathbb{Z}[i]$.
- In the prime factorization for n (in $\mathbb{Z}$), each prime factor of the form $4k+3$ has even exponent.

4. Let $p \in \mathbb{Z}_+$ be a prime number of the form $p = 4k + 1$, and let $p = \pi\overline{\pi}$ be its factorization into irreducibles in $\mathbb{Z}[i]$ (see previous problem).

(a) Prove that $\mathbb{Z}[i]/(p)$ is a finite ring, with $\mathbb{Z}[i]/(p) = p^2$.

(b) Use Chinese Remainder Theorem to prove that $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

5. Consider the ring $R = \mathbb{Z}[\sqrt{-5}]$.

(a) Prove that elements $2, 3, 1 \pm \sqrt{-5}$ are irreducible in R. [Hint: if $2 = zw$, then $N(z)N(w) = N(2) = 4$, where $N(z) = z\overline{z} \in \mathbb{Z}_+$.]

(b) Show that R is not UFD because $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

(c) Define the ideals

$$I = (2, 1 + \sqrt{-5})$$
$$J = (3, 2 + \sqrt{-5})$$
$$J' = (3, 2 - \sqrt{-5})$$

Prove that these idelas are prime (see hint in in Exercise 8, p. 293 in the book).

(d) Prove that $(2) = I^2$, $(3) = JJ'$, $(1 - \sqrt{-5}) = IJ$, $(1 + \sqrt{-5}) = IJ'$. Deduce from this that both factorizations $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. give the same presentation for (6) as a product of prime ideals: $(6) = I^2JJ'$.

6. Dummit and Foote, p. 267, problem 5.