Homework 2

due on Thursday, October 1

Study Chapters 7 and 8 of Dummit and Foote. Solve problem 26 to 7.1, problem 39 to 7.4 and the following problems.

Problem 1. Find a greatest common divisor $d(x)$ of the polynomials $p(x) = x^3 + 4x^2 + x - 6$ and $q(x) = x^5 - 6x + 5$ in the ring $\mathbb{Q}[x]$ and find $a(x), b(x) \in \mathbb{Q}[x]$ such that $d(x) = a(x)p(x) + b(x)q(x)$.

Problem 2. Let $K \subseteq L$ be fields. Suppose that $f, g \in K[x]$ and $f|g$ in the ring $L[x]$. Prove that $f|g$ in the ring $K[x]$.

Problem 3. Let R be a unique factorization domain. Let a, b, c be non-zero elements of R. Prove the following:

1. If $c|ab$ and $\gcd(a, c) = 1$ then $c|b$.

2. If $a|c$, $b|c$, and $\gcd(a, b) = 1$ then $ab|c$.

3. If $\gcd(a, c) = 1 = \gcd(b, c)$ then $\gcd(ab, c) = 1$.

4. If $c|a$ and $c|b$ then $c\gcd(a/c, b/c) = \gcd(a, b)$.

5. If m, n are positive integers then $\gcd(a, b) = 1$ iff $\gcd(a^m, b^n) = 1$.

6. If n is a positive integer and $a^n|b^n$ then $a|b$.

7. $\gcd(a, b)\mathrm{lcm}(a, b)$ is associated to ab.

8. $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$ and $\mathrm{lcm}(a, b, c) = \mathrm{lcm}(a, \mathrm{lcm}(b, c))$.

Problem 4. Prove that R_d is Euclidean for $d = 3, 6, 29$. Hint: Show that the absolute value of the norm can be used as Euclidean norm.
Hint: Show that if $0 < a < 2$ and $a \neq 5/4$ then for any b there is an integer m such that $|(b - m)^2 - a| < 1$.

Remark. It can be proved that the absolute value of the norm is an Euclidean function on R_d iff $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. On the other hand, asuming the Extended Riemann Hypothesis, it was proved that for $d > 0$ the ring R_d is a UFD iff it is Euclidean. It is a long standing conjecture that there are infinitely many $d > 0$ for which R_d is a PID. It is known that R_d is a PID iff the absolute value of the norm is a Dedekind-Hasse function on R_d.

Problem 5. Consider the ring $R_{-3} = R = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ of Eisenstein integers, where $\omega = (-1 + \sqrt{-3})/2$ (note that the ω here is slightly different than the one used in class, but the ring is the same). Observe that that $\omega^2 + \omega + 1 = 0$ (so $\omega^3 = 1$).

a) Let p be an odd prime such that -3 is not a square modulo p. Prove that if a, b are integers such that $p | a^2 - ab + b^2$ then $p|a$ and $p|b$. **Hint.** $(2a-b)^2 + 3b^2 = 4(a^2 - ab + b^2)$.

b) Prove that if a, b are integers such that $2|a^2 - ab + b^2$ then $2|a$ and $2|b$.

c) Use a), b) to conclude that if $p = 2$ or p is an odd prime such that -3 is not a square modulo p then pR is a prime ideal. Conclude that pR is maximal.

d) Suppose now p is an odd prime such that -3 is a square modulo p. Prove that pR is not a prime ideal. Conclude that p is not irreducible and $p = a^2 - ab + b^2$ for some integers a, b. Show that the ideal pR is a product of two maximal ideals which are different iff $p \neq 3$. Furthermore, show that if $p \neq 3$ then $p \equiv 1 \pmod{3}$.

e) Prove that every element of R is associated to an element of the form $a + b\omega$ with both a, b non-negative and at least one of a, b even.

f) Suppose now that $p \equiv 1 \pmod{3}$. Prove that -3 is a square modulo p. (Hint: There is an integer whose (multiplicative) order in the group $\mathbb{F}_p^\times$ is 3). Conclude that -3 is a square modulo an odd prime $p > 3$ iff p is a square modulo 3. This is a special case of quadratic reciprocity.

g) Prove that a natural number n is of the form $a^2 + 3b^2$ iff evrery prime divisor of n which is $\equiv 2 \pmod{3}$ appears in n to an even power.

Problem 6. Let d be a square-free integer.

a) Prove that every non-zero ideal of R_d is a product of maximal ideals in a unique (up to order) way.

Hint. Uniqueness is easy. For existence assume that the result is false and choose an ideal I maximal among those which are not products of maximal ideals (why does I exist?). Now I is contained in a maximal ideal P. Recall that there is unique prime number p in P and either $P = pR_d$ or $PQ = pR_d$ for some maximal ideal Q. If $I \subseteq pR_d$, consider the ideal $(1/p)I$ (why is it an ideal?). Otherwise consider the ideal $(1/p)IQ$ and prove that it strictly contains I. Proving that $IQ = pI$ is not possible may require some thought (but it is a short argument).

b) Let I be and ideal of R_d. Show that $I^* = \{a : a^* \in I\}$ is also an ideal in R_d and II^* is pricipal.

Problem 7. a) Let $R \subsetneq S$ be two integral domains such that for any $s \in S$ there is $r \in R$ such that $r \neq 0$ and $rs \in R$ and there is a monic polynomial $f \in R[x]$ such that $f(s) = 0$. Prove that R is not a UFD.

b) Let R be a subring of R_d (d a square-free integer). Prove that there is a non-negative integer k such that $R = \{a + kb\omega : a, b \in \mathbb{Z}\}$. Show that R is not a UFD if $k > 1$.

Problem 8. Let $d > 1$ be a positive square-free integer.

a) Let $n > 0$ be a natural number. Prove that there are integers m, k such that $0 < k \leq n$ and $|m + k\sqrt{d}| \leq 1/n$.
Hint: Show that two among the numbers $0, \sqrt{d}, 2\sqrt{d}, \ldots, n\sqrt{d}$ have fractional parts which are no more than $1/n$ apart.

b) Show that if m, k are as in a) then $|m^2 - dk^2| \leq 1 + 2\sqrt{d}$.

c) Consider the set $S = \{m + k\sqrt{d} : m, k \text{ are integers and } |m^2 - dk^2| \leq 1 + 2\sqrt{d}\}$. Prove that S is infinite. Conclude that for some integer M such that $|M| < 1 + 2\sqrt{d}$ the ring R_d has infinitely many elements whose norm is M.

d) Prove that for any integer K the set of ideals of the form aR_d, where a has norm K, is a finite set. Conclude that there are infinitely many elements of norm M in R_d which are pairwise associated. Conclude that the group of units of R_d is infinite.

f) Note that if $u \neq \pm 1$ is a unit of R_d then so are $-u, 1/u, -1/u$ and one of them is bigger than 1. Prove that if $a + b\omega > 1$ is a unit of R_d then a, b are non-negative.

Conclude that among the units of R_d which are bigger than one there is the smallest one, which we denote by w and call the *fundamental unit* of R_d.

g) Prove that if w is the fundamental unit of R_d then $R_d^\times = \{\pm w^k : k \in \mathbb{Z}\}$. Conclude that the groups of units of R_d is isomorphic to the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

h) Find the fundamental unit of R_5.

Remark. Note that our proof of the existence of the fundamental unit (or any non-trivial unit) in R_d is not constructive. There is a simple and very efficient algorithm to compute the fundamental unit which is closely related to the so called continued fraction expansion of the number $\omega - 1$.

Here is a very courious result providing an explicit unit in R_d. Let $D = d$ if $d \equiv 1 \pmod 4$ and $D = 4d$ otherwise. For an integer m relatively prime to D define

$$\chi(m) = \begin{cases} \left(\frac{m}{d}\right), \text{ if } d \equiv 1 \bmod 4 \\ (-1)^{(m-1)/2}\left(\frac{m}{d}\right), \text{ if } d \equiv 3 \bmod 4 \\ (-1)^{\frac{m^2-1}{8}+\frac{m-1}{2}\frac{a-1}{2}}\left(\frac{m}{a}\right), \text{ if } d = 2a. \end{cases}$$

Let $A = \Pi_a \sin\frac{\pi a}{D}$, where a runs over all integers in the interval $(0, D/2)$ which are relatively prime to D and satisfy $\chi(a) = -1$. Similarly, let $B = \Pi_b \sin\frac{\pi b}{D}$, where b runs over all integers in the interval $(0, D/2)$ which are relatively prime to D and satisfy $\chi(b) = 1$. Then $\eta = A/B$ is a unit in R_d and $\eta = w^h$, where w is the fundamental unit and $h > 0$ is an integer called **the class number** of R_d (note that even the fact that $A > B$ is highly non-trivial). R_d is a PID if and only if $h = 1$.