PROBLEM SET 9

(Hand in all.)

(1) [Jacobson p. 137 #7] Suppose $\mathbb{F}$ is a finite field ($|\mathbb{F}| = q < \infty$). Let $f(x_1, \ldots, x_r) \in \mathbb{F}[x_1, \ldots, x_r]$ be a polynomial of degree $n < r$, the number of indeterminates. Assume $f(0, \ldots, 0) = 0$. Prove that there exist $(a_1, \ldots, a_r) \neq (0, \ldots, 0)$ such that $f(a_1 \ldots, a_r) = 0$. [Hint: Look at the preceding 2 exercises in Jacobson, and include (short) solutions in your answer, since #5 feeds into #6 and you need to use the result of #6 to do #7. For #6, look at the proof of III.G.25 in the notes; for #5, you just need to remember something about the multiplicative group of $\mathbb{F}$.]

(2) (a) Show that for $p \neq 2$, $\left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \underset{(p)}{\equiv} 1$. [Hint: the multiplicative group of a finite field is . . .] (b) Show $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. (c) Let p be a prime of the form $4m + 1$, $m \in \mathbb{Z}$. Show $\left(\frac{-1}{p}\right) = 1$, hence that p is not prime in $\mathbb{Z}[i]$, hence that $p = a^2 + b^2$ ($a, b \in \mathbb{Z}$).

(3) Recall that we know $R = \mathbb{Z}[i]$ is a UFD, so that the primes and irreducibles in R are the same. Find all of them.

(4) [Jacobson p. 146 #3, 4 Show that (a) $\mathbb{Z}[\sqrt{-5}]$ and (b) $\mathbb{Z}[x]$ satisfy the DCC. Also, say which one (or both, or neither) is a UFD.

(5) [Jacobson p. 147 #8] Let p be a prime of the form $4n + 1$ and let q be a prime such that the Legendre symbol $(\frac{q}{p}) = -1$ (cf. III.J.16). Show that $\mathbb{Z}[\sqrt{pq}]$ is not a UFD.

(6) [Jacobson p. 149 #4] Let D be a PID, E a domain containing D as a subring. Show that if g is a GCD of a and b in D, then g is also a GCD of a and b in E.

(7) [Jacobson p. 150 #12] Apply Euclid's algorithm to the polynomials $g = x^3 + x^2 + x - 3$ and $f = x^4 - x^3 + 3x^2 + x - 4$ in $\mathbb{Q}[x]$ to find their GCD.

(8) [Jacobson p. 150 #13, 14, 15 (as one problem). This is too long to type out here, but it is a fantastic problem which uses the Euclidean algorithm for $F[x]$ to provide an explanation of partial fraction decompositions.]

(9) Show (i) $x^5 - 4x + 2$ and (ii) $x^4 + 4x^3 + 10x^2 + 12x + 7$ are irreducible in $\mathbb{Q}[x]$. [Hint: for one of them, apply a linear change of variable.]

(10) [Jacobson p. 154 #3] Show that if p is a prime (in $\mathbb{Z}$) then the polynomial obtained by replacing x by $x + 1$ in $x^{p-1} + x^{p-2} + \cdots + 1 = (x^p - 1)/(x - 1)$ is irreducible in $\mathbb{Q}[x]$. Hence prove that the *cyclotomic polynomial* $x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible in $\mathbb{Q}[x]$.

(11) [Jacobson p. 154 #4] Obtain factorizations into irreducible factors in $\mathbb{Z}[x]$ of the following polynomials: $x^3 - 1$, $x^4 - 1$, $x^5 - 1$, $x^6 - 1$, $x^7 - 1$, $x^8 - 1$, $x^9 - 1$, $x^10 - 1$.

(12) [Jacobson p. 154 #5] Prove that if D is a domain which is not a field then $D[x]$ is not a PID.