MATH 371 – Homework 7– October 25, 2013

1. Let R be a unique factorization domain, with fraction field F (if you want, you can assume $R = \mathbb{Z}$ and $F = \mathbb{Q}$, but also try the general case). Let $p(x) \in R[x]$. (Recall that we have proved that the ring $F[x]$ of polynomials in a single variable over a field is a unique factorization domain).

(a) Suppose $p(x) = a(x)b(x)$for a pair of nonconstant polynomials $a(x), b(x) \in F[x]$ (so p is reducible in $F[x]$). Show that there is an element $d \in R$ and polynomials $A(x), B(x) \in R[x]$ such that $dp(x) = A(x)B(x)$.

(b) Assume that the element d in part (a) is not a unit of R. Then d has a factorization as $d = p_1p_2 \cdots p_k$ into primes in R which is unique up to order and multiplication by units. Explain why $\langle p_i \rangle \subset R$ is a prime ideal in R. Further, explain why $\langle p_i \rangle \subset R[x]$ (where this time $\langle p_i \rangle$ means all *polynomial* multiples of p_i) is a prime ideal in $R[x]$.

(c) Explain why $(R/\langle p_i \rangle)[x] \cong R[x]/\langle p_i \rangle$, where on the left $\langle p_i \rangle \subset R$ and on the right $\langle p_i \rangle \subset R[x]$, and then show that $R[x]/\langle p_i \rangle$ is an integral domain.

(d) Prove that it must be the case that either $p_i \mid A(x)$ or $p_i \mid B(x)$ in $R[x]$, and so we can cancel p_i from both sides of $dp(x) = A(x)B(x)$ within $R[x]$.

(e) Explain why this implies that $p(x)$ can be factored into $p(x) = \overline{A}(x)\overline{B}(x)$, where $\overline{A}(x), \overline{B}(x) \in R[x]$.

(This fact, namely if p is reducible in $F[x]$ then it is reducible in $R[x]$ is sometimes called *Gauss's lemma*.)

---

2. (a) Using problem 1, show that if R is a unique factorization domain with fraction field F, and p is a polynomial such that the greatest common divisor of all the coefficients of p is 1 (this happens for instance if p is monic) then p is irreducible in $R[x]$ if and only if p is irreducible in $F[x]$.

(b) Suppose $p(x)$ is a polynomial in $R[x]$. After factoring out the greatest common divisor of the coefficients, so $p(x) = dq(x)$, explain why $q(x)$ has a unique (up to order and multiplying by units in R) factorization in $R[x]$ (given what you know about $F[x]$), and so p has a unique factorization in $R[x]$.

(c) Explain why this implies that, for an integral domain R, R is a unique factorization domain if and only if $R[x]$ is.

(d) Show that this implies that if R is a unique factorization domain, then so is $R[x_1, \ldots, x_n]$ for any (finite) number of variables $x_1, \ldots, x_n$.

---

3. (a) Let R be a ring, and I an ideal of R. Show that $I[x]$ polynomials with coefficients in I is an ideal of $R[x]$, and that $R[x]/I[x] \cong (R/I)[x]$. Explain why, if I is a prime ideal of R then $I[x]$ is a prime ideal of $R[x]$.

(b) Now suppose R is an integral domain, I is a proper ideal of R and $f(x)$ is a non-constant monic polynomial in $R[x]$. Prove that if $f(x)$ (actually, the image of f) cannot be factored into two polynomials of lower degree in $(R/I)[x]$ then $f(x)$ is irreducible in $R[x]$.

(c) Show that for all $k \geqslant 2$, $f(x) = x^k + x + 1$ is irreducible in $\mathbb{Z}[x]$ (consider the image of f in $\mathbb{F}_2[x]$).

(d) Suppose p is a prime number (in $\mathbb{Z}$) and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ be a monic polynomial of degree $n \geqslant 1$. Suppose that $p \mid a_i$ for all $i = 0, 1, \ldots, n-1$ but p^2 does not divide a_0. Prove that f is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$. (Consider the reduction of f mod p.)

(e) Show that $x^4 + 10x + 5$ is irreducible in $\mathbb{Z}[x]$.

(f) Show that if p is prime, then the cyclotomic polynomial $\Phi_p(x)$ is irreducible in $\mathbb{Z}[x]$ (Apply part (d) to $\Phi_p(x+1)$).

(e) Generalize part (d) to an arbitrary integral domain ("Let P be a prime ideal of the integral domain R...") and prove it.

---

4. Let $R = \mathbb{F}_2[x]/\langle x^3 + 1\rangle$ and let $\alpha = [x] \in R$.

(a) Find an irreducible factorization of $x^3 + 1$ in $\mathbb{F}_2[x]$.

(b) How many elements does R have? Write down the multiplication rule for elements of R.

(c) Which elements of R are units? What group is R^*?

---

5. Suppose F is a (the) finite field with p^n elements and $E \subseteq F$ is a finite field with p^m elements.

(a) Prove that $m \mid n$ (view F as a vector space over E).

(b) If $a \mid b$, for $a, b \in \mathbb{N}$, prove that $x^{p^a} - x \mid x^{p^b} - x$ in $\mathbb{Z}[x]$.

(c) If $m \mid n$, prove that F contains a subfield with p^m elements explicitly by showing that $\{x \in F \mid x^{p^m} = x\}$ is a subfield of F with p^m elements.

---

6. (a) How many monic irreducible polynomials of degree 3 are there in $\mathbb{F}_{11}[x]$?

(b) How many monic irreducible polynomials of degree 6 are there in $\mathbb{F}_{13}[x]$?