Math 412 Homework 5

Paul Hacking

March 5, 2013

Reading: Saracino, Chapter 20.
Show your work and justify your answers carefully.

(1) Factor the following polynomials into irreducible polynomials.

   (a) $x^2 + 4x + 13$ in $\mathbb{C}[x]$.
   (b) $x^2 + 3$ in $(\mathbb{Z}/7\mathbb{Z})[x]$
   (c) $x^4 + 1$ in $\mathbb{C}[x]$.
   (d) $x^4 + 1$ in $\mathbb{R}[x]$.

(2) (a) Find all solutions of the equation $x^2 - 1 = 0$ in $\mathbb{Z}/8\mathbb{Z}$.
   (b) Use part (a) to give two different factorizations of the polynomial $x^2 - 1 \in (\mathbb{Z}/8\mathbb{Z})[x]$ into monic linear factors.

   [Remark: In class we showed that if K is a field then a nonzero polynomial $f(x) \in K[x]$ has at most $\deg(f)$ roots in K, and f has a unique factorization of the form $f(x) = cp_1 \ldots p_r$ where $c \in K$, $c \neq 0$ and $p_1, \ldots, p_r$ are irreducible monic polynomials. This question shows that the analogous properties do not hold in general for polynomials $f(x) \in (\mathbb{Z}/8\mathbb{Z})[x]$. (Note that $\mathbb{Z}/8\mathbb{Z}$ is not an integral domain and so in particular not a field.)]

(3) Prove that the following polynomials are irreducible.

   (a) $x^2 + 5$ in $(\mathbb{Z}/11\mathbb{Z})[x]$.
   (b) $x^3 + x + 1$ in $(\mathbb{Z}/5\mathbb{Z})[x]$.
   (c) $x^3 + 2x^2 + 5x + 2$ in $\mathbb{Q}[x]$.

(4) Let K be a field and $f(x) \in K[x]$ a polynomial in the variable x with coefficients in K. Show that $f(x)$ is a unit in $K[x]$ iff $f(x)$ is a nonzero constant polynomial.

(5) Let K be a field and $f(x) \in K[x]$ a non-constant polynomial in the variable x with coefficients in K. Consider the quotient ring $R = K[x]/(f(x))$.

  (a) Show that the coset $g(x) + (f(x))$ is a unit of the ring R iff $\gcd(f(x), g(x)) = 1$.

  (b) Compute the inverse of the element $x^2+1+(x^3+1)$ of the quotient ring $R = \mathbb{Q}[x]/(x^3+1)$.

[Hint: The coset $g(x) + (f(x))$ is a unit in $K[x]/(f(x))$ iff there exist $h(x), q(x) \in K[x]$ such that $g(x)h(x) = 1 + q(x)f(x)$ (why?). Given f and g such that $\gcd(f, g) = 1$ we can find h and q using the Euclidean algorithm. (The same procedure for integers was described in Math 300.)]

(6) Let $f(x) \in \mathbb{Q}[x]$. Show that $\gcd(f(x), f'(x)) \neq 1$ iff there exists an irreducible polynomial g such that g^2 divides f.

[Hint: $f'(x)$ denotes the derivative of the polynomial $f(x)$. Use the product rule to show that if g is irreducible, g divides f, and g divides f', then g^2 divides f. Note that $\gcd(g, g') = 1$ for g irreducible (why?)]

(7) (a) Explain why there are only finitely many polynomials of fixed degree n in $(\mathbb{Z}/p\mathbb{Z})[x]$. [How many are there exactly?]

  (b) Show carefully that there are infinitely many irreducible polynomials in $(\mathbb{Z}/p\mathbb{Z})[x]$. [Hint: Adapt Euclid's proof that there are infinitely many primes in $\mathbb{Z}$.]

  (c) Deduce that there are irreducible polynomials in $(\mathbb{Z}/p\mathbb{Z})[x]$ of arbitrarily large degree.

(8) Let $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ be a polynomial in the variable x with coefficients in the finite field $\mathbb{Z}/p\mathbb{Z}$. Show that $f(a) = 0$ for all $a \in \mathbb{Z}/p\mathbb{Z}$ iff $f(x)$ is divisible by $x^p - x$.