MATH 371 – Midterm II – November 14, 2013

1. (a) Calculate the irreducible factorization of the polynomial $x^7 - 1 \in \mathbb{F}_2[x]$.

(b) Is the ring $\mathbb{F}_2[x]/\langle x^7 - 1\rangle$ a field? Is it an integral domain?

(c) What about the ring $\mathbb{F}_2[x]/\langle p(x)\rangle$ where $p(x) = (x^7-1)/(x-1) = x^6+x^5+x^4+x^3+x^2+x+1$?

(a) Let $f(x) = x^7 - 1$. Since $xf(x) = x^8 - x = x^{2^3} - x$, we have that $xf(x)$ is the product of all the monic irreducible polynomials of degrees 1 and 3. In $\mathbb{F}_2[x]$ the monic irreducible polynomials of degree 1 are x and $x + 1$, and the monic irreducible polynomials of degree 3 (which are the ones for which neither 0 nor 1 is a root) are $x^3 + x^2 + 1$ and $x^3 + x + 1$. Therefore

$$x^7 - 1 = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$$

is the irreducible factorization.

(b) The ring $R = \mathbb{F}_2[x]/\langle p(x)\rangle$ has basis $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ as a vector space over $\mathbb{F}_2$, where $\alpha = [x] \in R$. But from the factorization in part (a), we have that in R, $(\alpha + 1)(\alpha^3 + \alpha^2 + 1)(\alpha^3 + \alpha + 1) = 0$, so that R is neither a field nor an integral domain.

(c) Since $p(x) = (x^3 + x^2 + 1)(x^3 + x + 1)$ is not irreducible, the ring $\mathbb{F}_2[x]/\langle p(x)\rangle$ is neither a field nor an integral domain for the same reason as (b).

---

2. For any prime $p > 5$, calculate the Legendre symbol $\left(\frac{5}{p}\right)$. (Quadratic reciprocity might come in handy.) Is 5 a square mod 157?

Since $5 \equiv 1 \pmod 4$, we have $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, and in this symbol we can replace p by its (necessarily nonzero) remainder (since p is prime) mod 5. Thus:

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if} \quad p \equiv \pm 1 \pmod 5 \\ -1 & \text{if} \quad p \equiv \pm 2 \pmod 5 \end{cases}$$

because only 0 and ± 1 are squares mod 5. Since $157 \equiv 2 \pmod 5$, we have that 5 is *not* a square mod 157.

---

3. If we use the graded lexicographic order with $x > y > z$, is $\{x^4y^2 - z^5\,,\ x^3y^3 - 1\,,\ x^2y^4 - 2z\}$ a Gröbner basis for the ideal generated by these polynomials? Why or why not?

Let $f(x, y, z) = x^4y^2-z^5$, $g(x, y, z) = x^3y^3-1$ and $h(x, y, z) = x^2y^4-2z$. Since $yf-xg = -yz^5+x$ and since the leading term of this with respect to grlex order, namely yz^5, is not in the ideal $\langle x^4y^2\,,\ x^3y^3\,,\ x^2y^4\rangle$ generated by the leading terms of f, g and h (since every polynomial in that ideal is divisible by x^2), the given polynomials do not comprise a Gröbner basis for the ideal they generate.

---

4. Let $f_1, f_2, f_3, \ldots \in k[x_1, \ldots, x_n]$ be an infinite collection of polynomials, and let $I = \langle f_1, f_2, f_3, \ldots\rangle$ be the ideal they generate. Prove that there is an integer N such that $I = \langle f_1, f_2, \ldots, f_N\rangle$.

We know that I is finitely generated, so there is a finite set of polynomials $g_1, g_2, \dots, g_r$ so that for any $p \in I$ we have a set of polynomials $b_i \in k[x_1, \dots, x_n]$ for $i = 1, \dots, r$ such that $p = \sum_{i=1}^{r} b_i g_i$. Now for each $i = 1, \dots, r$ there is a finite set of polynomials $a_{ij} \in k[x_1, \dots, x_n]$ for $j = 1, \dots, N_i$ such that $g_i = \sum_{j=1}^{N_i} a_{ij} f_j$. So we can take $N = \max_i(N_i)$ and by substituting this last sum for g_i in the previous one, we can express any polynomial $p \in I$ in terms of $f_1, \dots, f_N$, so $I = \langle f_1, \dots, f_N \rangle$.

---

5. Factor completely the cyclotomic polynomial $\Phi_p(x) \in \mathbb{F}_p[x]$. (Surprise!)

We know that $\Phi_p(x) = (x^p - 1)/(x - 1)$. But $x^p - 1 = x^p - 1^p = (x - 1)^p$ by the "freshman dream". so we have $\Phi_p(x) = (x - 1)^{p-1}$. That's it.

---

6. Let F be a field and K an extension field of F. An element $\alpha \in K$ is called *algebraic over F* if α is a root of some polynomial $f(x) \in F[x]$.

(a) If $\alpha \in K$ is algebraic over F, show that there is a *monic, irreducible* polynomial $m(x) \in F[x]$ of which α is a root. (Consider the polynomial of smallest degree for which α is a root.)

(b) Show that if $f(x) \in F[x]$ is *any* polynomial such that $f(\alpha) = 0$, then $m(x)$ divides $f(x)$ in $F[x]$. (Use the division algorithm.)

(c) Show that, given α there is only one monic, irreducible polynomial $m(x) \in F[x]$ such that $m(\alpha) = 0$.

(a) By definition, the set of polynomials $S = \{p(x) \in F[x] \mid p \neq 0 \text{ and } p(\alpha) = 0\}$ is non-empty. So the set of degrees of such polynomials is a non-empty set of non-negative numbers, which has a smallest element d. Let $p(x)$ be an element of S of this smallest degree d. By dividing p by its leading coefficient c we can arrange for $m(x) = p(x)/c$ to be monic. Now we have to show that $m(x)$ is irreducible. But if $m(x)$ were reducible, it would be the product of two polynomials $q(x), r(x) \in F[x]$ both of degree strictly less than d. Moreover, we'll have $q(\alpha)r(\alpha) = m(\alpha) = 0$, so one of $q(\alpha)$ or $r(\alpha)$ is zero, which would contradict the minimality of the degree d. Thus m is a monic, irreducible polynomial of which α is a root.

(b) Let $f(x)$ be a polynomial having α as a root. Using the division algorithm, write $f(x) = q(x)m(x) + r(x)$, where either r is the zero polynomial or else the degree of r is less than the degree of $m(x)$. Evaluating both sides at $x = \alpha$ gives the equation $f(\alpha) = q(\alpha)m(\alpha) + r(\alpha)$ or $0 = 0 + r(\alpha)$, so $r(\alpha) = 0$. If r were not the zero polynomial we would contradict the minimality of the degree of m. So $r = 0$ and so m divides f.

(c) If there were another such polynomial, say $m'(x)$, then by part (b) we would have $m \mid m'$ and $m' \mid m$, which would imply m' is a constant multiple of m. But since both are monic, they must be equal.