MATH 850 Final Exam 22 May 2017 8:00–10:30 a.m.

Name: _____

Show complete work—that is, all the steps needed to completely justify your answer. Simplify your answers as much as possible. You may refer to theorems in the text book and homework problems (without referring to the exact theorem numbers).

(1) Let F be a field and consider $I = \langle x^2 - y, x^3 - z \rangle \in F[x, y, z]$.

(a) Define what a Gröbner basis for I is.

(b) Compute a Gröbner basis for I using graded lexicographic order with $x \geq y \geq z$.

(c) Is your Gröbner basis reduced?

Solution: (b) We use Buchberger's algorithm and compute

$$S\big(x^2 - y, x^3 - z\big) = x\left(x^2 - y\right) - \left(x^3 - z\right) = -xy + z\,.$$

Thus $x^3 - z \in (x^2 - y, -xy + z)$, and so $I = \langle x^2 - y, -xy + z \rangle$. Now $S(x^2 - y, -xy + z) = xz - y^2$. We compute

$$S\big(x^2 - y, xz - y^2\big) = -yz + xy^2 = -y\,(-xy + z)$$

and

$$S\big(-xy + z, xz - y^2\big) = -y^3 + z^2.$$

Let

$$G = \left\{x^2 - y, -xy + z, xz - y^2, -y^3 + z^2\right\}.$$

So far we computed $S(x^2 - y, -xy + z)$, $S(x^2 - y, xz - y^2)$, and $S(-xy + z, xz - y^2)$, and they all give remainder 0 under the extended Euclidean algorithm. We further compute

$$\begin{aligned} S\big(x^2 - y, -y^3 + z^2\big) &= y^3\left(x^2 - y\right) + x^2\left(-y^3 + z^2\right) = x^2z^2 - y^4 \\ &= z^2\left(x^2 - y\right) + y\left(-y^3 + z^2\right) \end{aligned}$$

which also gives remainder 0,

$$\begin{aligned} S\big(-xy + z, -y^3 + z^2\big) &= y^2\,(-xy + z) - x\left(-y^3 + z^2\right) = -xz^2 + y^2z \\ &= -z\left(xz - y^2\right) \end{aligned}$$

again with remainder 0, and

$$\begin{aligned} S\big(xz - y^2, -y^3 + z^2\big) &= y^3\left(xz - y^2\right) + xz\left(-y^3 + z^2\right) = -y^5 + xz^3 \\ &= y^2\left(-y^3 + z^2\right) + z^2\left(xz - y^2\right) \end{aligned}$$

once more with remainder 0. Hence G is a (in fact, reduced) Gröbner basis for I.

(2) Let $a \in \mathbb{Q} \setminus \{0\}$ and let $\omega = e^{2\pi i/8}$.

(a) Define the Galois group of a field extension K/F.

(b) Determine for which a the field $\mathbb{Q}(\omega\sqrt{a})$ is of degree 4 over $\mathbb{Q}$.

(c) In the case that $[\mathbb{Q}(\omega\sqrt{a}) : \mathbb{Q}] = 4$, prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega\sqrt{a})) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Solution: (b) The minimal polynomial of $\omega\sqrt{a}$ is $x^4 + a^2$. It has no roots in $\mathbb{Q}$ but comes with the quadratic factorization

$$x^4 + a^2 = \left(x^2 + \sqrt{2a}\, x + a\right)\left(x^2 - \sqrt{2a}\, x + a\right).$$

Thus $x^4 + a^2$ is irreducible over $\mathbb{Q}$ if and only if $\sqrt{2a} \neq \frac{p}{q}$ for some integers p and q, and so these are precisely the cases when $[\mathbb{Q}(\omega\sqrt{a}) : \mathbb{Q}] = 4$.

(c) We now assume $x^4 + a^2$ is irreducible over $\mathbb{Q}$. Thus $\mathbb{Q}(\omega\sqrt{a})/\mathbb{Q}$ is Galois, and we have the three intermediate fields

$$\mathbb{Q}(i),\ \mathbb{Q}\left(\sqrt{2a}\right),\ \text{ and }\ \mathbb{Q}\left(i\sqrt{2a}\right).$$

By the fundamental theorem of Galois theory, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega\sqrt{a}))$ has three distinct subgroups of order 2; since $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega\sqrt{a}))$ has order 4, it is therefore isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(3) Let q be a prime power and $n \in \mathbb{Z}_{>0}$.

(a) Prove that if a polynomial $p(x_1, x_2, \ldots, x_n)$ over $\mathbb{F}_q$ of degree $< q$ vanishes at every point in $\mathbb{F}_q^n$, then $p(x_1, x_2, \ldots, x_n)$ has to be the zero polynomial.

(b) Give an example that shows that our assumption about the degree of $p(x_1, x_2, \ldots, x_n)$ is necessary.

Solution: (a) We use induction on n; the base case follows from linear algebra. For the induction step, assume that $p(x_1, x_2, \ldots, x_n)$ vanishes at every point in $\mathbb{F}_q^n$ and write

$$p(x_1, x_2, \ldots, x_n) \;=\; \sum_{j=0}^{q-1} p_j(x_1, x_2, \ldots, x_{n-1})\, x_n^j$$

for some polynomials $p_0, p_1, \ldots, p_{q-1}$ in the first $n-1$ variables; note that they are all of degree $< q$. Viewing the above expression as a polynomial in the single variable x_n, we know again from linear algebra that it has to be the zero polynomial (since it vanishes for all $x_n \in \mathbb{F}_q$), that is, each $p_0, p_1, \ldots, p_{n-1}$ vanishes at $\mathbb{F}_q^{n-1}$. By the induction hypothesis, each $p_0, p_1, \ldots, p_{n-1}$ is the zero polynomial, and thus so is $p(x_1, x_2, \ldots, x_n)$.

(b) For a prime p, the (nonzero) polynomial $x^p - x \in \mathbb{F}_p[x]$ vanishes at $\mathbb{F}_p$.