Homework #3

Due **Wednesday, February 11** in Gradescope by **11:59 pm ET**

READ Sections A.4, 2.4, 3.1, 3.2, 4.1 in Cox

WATCH 1. Video 4: Group Actions (15:28)
2. Video 5: Adjoining Roots via Quotient Rings (16:53)
3. Video 6: On Complex Roots (8:12)

WRITE AND SUBMIT solutions to the following problems.

Problem 1. (10 points) Cox, Appendix A.4, Exercise 5:
Let G be a group acting on a nonempty set X. Prove that the following are equivalent:
(i) G acts transitively on X. (I.e., for all $x, y \in X$, there exists $g \in G$ such that $gx = y$.)
(ii) For all $x \in X$, we have $G \cdot x = X$.
(iii) There exists $x \in X$ such that $G \cdot x = X$.

Problem 2. (10 points) Cox, Section 2.4, Exercise 6(a,b): Let F be a field of characteristic 2.
(a) Let $b \in F$, and let $L \supseteq F$ be a (larger) field such that $b = \beta^2$ for some $\beta \in L$. Prove that β is unique. [In particular, β is the unique (double) root of $x^2 + b$, and we may write $\beta = \sqrt{b}$ with no ambiguity.]
(b) Let $f = x^2 + ax + b \in F[x]$ with $a \neq 0$, and suppose that f is irreducible over F. (So in particular, f has no roots in F.) Let α be a root of f in some larger field $L \supseteq F$. Prove that α **cannot** be written as $\alpha = u + v\sqrt{w}$ for any $u, v, w \in F$.

Problem 3. (12 points) Cox, Section 2.4, Exercise 6(c,d): Let F be a field of characteristic 2.
(c) For $b \in F$, define $R(b)$ to be a root of the polynomial $x^2 + x + b$ (possibly in some larger field). Let's call $R(b)$ and $R(b) + 1$ the **2-roots** of b. Prove that $R(b)$ and $R(b) + 1$ are the two roots of $x^2 + x + b$, and (briefly) explain why adding 1 to $R(b) + 1$ yields $R(b)$.
(d) For $a, b \in F$ with $a \neq 0$, prove that the two roots of $f = x^2 + ax + b$ are $aR(b/a^2)$ and $a(R(b/a^2) + 1)$.

Note: Putting all four parts of the preceding two problems above together (i.e., all of Section 2.4, Exercise 6) shows that when $\mathrm{char}(F) = 2$, the roots of $x^2 + ax + b \in F[x]$ are

$$x = \begin{cases} \sqrt{b} \quad \text{(double root)} & \text{if } a = 0, \\ aR(b/a^2) \text{ and } a(R(b/a^2) + 1) & \text{if } a \neq 0, \end{cases}$$

which can be thought of as the quadratic formula in characteristic 2.

Problem 4. (10 points) Cox, Section 3.1, Exercise 1:
Let F be a field, let $f, g, h \in F[x]$ with $f = gh \neq 0$. Let $I = \langle g \rangle$.
(a) Prove that g is constant if and only if $I = F[x]$.
(b) Prove that h is constant if and only if $I = \langle f \rangle$.

(continued next page)

Note for the next problem: Let F be a field, and let $f, g \in F[x]$. We say f and g are **relatively prime** if the only polynomials $h \in F[x]$ that divide both f and g are constants. It is a fact, which you may assume without proof in the next problem, that f and g are relatively prime if and only if there exist $A, B \in F[x]$ such that $Af + Bg = 1$.

Problem 5. (10 points) Cox, Section 3.1, Exercise 5:
Let F be a field, let $f \in F[x]$ be irreducible, and let $g + \langle f \rangle$ a a nonzero coset in $L = F[x]/\langle f \rangle$.

(a) Prove that f and g are relatively prime. (As defined in the note above.)

(b) By the note above, there exist $A, B \in F[x]$ such that $Af + Bg = 1$. Prove that $B + \langle f \rangle$ is the multiplicative inverse of $g + \langle f \rangle$ in L.

Problem 6. (6 points) Cox, Section 3.1, Exercise 6:
Apply the method of the previous problem to find the multiplicative inverse of the coset $1 + x + \langle x^2 + x + 1 \rangle$ in the field $\mathbb{Q}[x]/\langle x^2 + x + 1 \rangle$.

Problem 7. (10 points) Cox, Section 3.2, Exercise 1:
For $f = \sum_{j \geq 0} a_j x^j \in \mathbb{C}[x]$, define $\bar{f} = \sum_{j \geq 0} \bar{a}_j x^j \in \mathbb{C}[x]$.

(a) Prove that for any $f, g \in \mathbb{C}[x]$, prove that $\overline{fg} = \bar{f}\bar{g}$.

(b) Let $\alpha \in \mathbb{C}$. Prove that if $\bar{f}(\alpha) = 0$, then $f(\bar{\alpha}) = 0$.

[**Note**: Here, if $a = b + ic$ with $b, c \in \mathbb{R}$, then define $\bar{a} = b - ic$, called the *complex conjugate* of $a \in \mathbb{C}$. But don't bother breaking complex numbers down that way here. Instead, you may assume without proof the following facts, which all have short proofs: for any complex numbers $\alpha, \beta \in \mathbb{C}$, we have $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$ and $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$, and also $\overline{\bar{\alpha}} = \alpha$.]

Problem 8. (12 points) Cox, Section 3.2, Exercise 7:
Let F be a field. Prove that F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ has a root in F.

Problem 9. (8 points) Cox, Section 4.1, Exercise 2:
Let F be a field, and let $f, g \in F[x]$ be monic polynomials. Suppose that f and g both divide each other. Prove that $f = g$.

[Note: This fact was needed to prove the uniqueness portion of Lemma 4.1.3.]

Optional Challenges (do NOT hand in): Cox Problems 2.4 #2, 9

Questions? You can ask in:

Class: MWF 9:00am – 9:50am, SCCE C101

My office hours: in my office (SMUD 406):

Mon 2:00–3:30pm
Tue 1:30–3:15pm
Fri 1:00–2:00pm

Also, you may email me any time at `rlbenedetto@amherst.edu`