MTH 461 **Spring 2020**
Review for Exam 1 **Drew Armstrong**

There are three main topics for the first exam:

(1) The Quadratic and Cubic Formulas

(2) Basic properties of the rings $\mathbb{Z}$ and $\mathbb{F}[x]$

(3) Basic properties of the field $\mathbb{C}$

(1) The Quadratic and Cubic Formulas

- On the exam you may always use modern notation and modern number systems. This means that negative numbers and complex numbers are allowed.
- **Quadratic Formula.** The equation $x^2 + ax + b = 0$ has discriminant $\Delta = a^2 - 4b$. The roots are given by
$$x = (-a \pm \delta)/2,$$
where δ is any number satisfying $\delta^2 = \Delta$.
- If a, b are real then $\Delta > 0$ means two real roots, $\Delta = 0$ means one real root (actually, two equal real roots) and $\Delta < 0$ means two non-real complex roots (which necessarily form a complex conjugate pair).
- If $x^2 + ax + b = (x - r)(x - s)$ then by comparing coefficients we obtain
$$\begin{cases} a & = -(r+s), \\ b & = rs, \end{cases}$$
and from this one can check that $\Delta = a^2 - 4b = (r - s)^2$.
- Any cubic equation $x^3 + ax^2 + bx + c = 0$ with real coefficients $a, b, c \in \mathbb{R}$ satisfying $a \neq 0$ has at least one real root because of the Intermediate Value Theorem.
- **Cubic Formula.** The equation $x^3 + ax^2 + bx + c = 0$ can be reduced to the form $y^3 + py + q = 0$ by setting $x = y - a/3$. Let $\Delta = (q/2)^2 + (p/3)^3$ be the discriminant and let δ be any number satisfying $\delta^2 = \Delta$. Then Cardano's Formula tells us that
$$y = \sqrt[3]{-q/2 + \delta} + \sqrt[3]{-q/2 - \delta}.$$
Most examples are too tricky for the exam. One relatively easy case is $x^3 - 6x - 6 = 0$.

(2) Basic Properties of the Rings $\mathbb{Z}$ and $\mathbb{F}[x]$

- You do not need to memorize the axioms of rings and fields.

- Let $\mathbb{F}$ be a field. A *polynomial* is formal expression $f(x) = \sum_{k\geqslant 0} a_k x^k$, where only finitely many of the coefficients $a_k \in \mathbb{F}$ are nonzero. If a_n is the highest nonzero coefficient then we say $\deg(f) = n$. If there are no nonzero coefficients then we say $\deg(f) = -\infty$. We add and multiply polynomials as follows:

$$\sum_{k\geqslant 0} a_k x^k + \sum_{k\geqslant 0} b_k x^k := \sum_{k\geqslant 0} (a_k + b_k) x^k$$
$$\left(\sum_{i\geqslant 0} a_i x^k\right)\left(\sum_{j\geqslant 0} b_j x^j\right) := \sum_{k\geqslant 0}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

These operations make $\mathbb{F}[x]$ into a ring with "zero element" $0 + 0x + 0x^2 + \cdots$ and "one element" $1 + 0x + 0x^2 + \cdots$. We can view $\mathbb{F} \subseteq \mathbb{F}[x]$ as a subring by writing

$$a = a + 0x + 0x^2 + \cdots \qquad \text{for all } a \in \mathbb{F}.$$

- **The Division Theorem.** For any integers $a, b \in \mathbb{Z}$ with $b \neq 0$ there exist integers $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $|r| < |b|$. For any polynomials $f(x), g(x) \in \mathbb{F}[x]$ with $g(x)$ there exist polynomials $q(x), r(x) \in \mathbb{F}[x]$ such that $f(x) = q(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$.

- **Descartes' Factor Theorem.** For any polynomial $f(x) \in \mathbb{F}[x]$ and constant $a \in \mathbb{F}$, the remainder of $f(x)$ when divided by $x - a$ is the constant $f(a) \in \mathbb{F}$ (i.e., the evaluation of $f(x)$ $x = a$). It follows that

$$f(a) = 0 \text{ in the field } \mathbb{F} \quad \Leftrightarrow \quad (x-a)|f(x) \text{ in the ring } \mathbb{F}[x].$$

- As a corollary of Descartes, any polynomial $f(x) \in \mathbb{F}[x]$ of degree $n \geqslant 0$ has at most n roots in $\mathbb{F}$. Proof: If $f(a) = 0$ then $f(x) = (x-a)g(x)$ where $g(x)$ has degree $n - 1$. By induction we can assume that $g(x)$ has at most $n - 1$ roots in $\mathbb{F}$. But if $f(b) = 0$ and $b \neq a$ then substituting $x = b$ gives $0 = (b-a)g(b)$ and hence $g(b) = 0$.

- **Euclid's Lemma.** We say that $p \in \mathbb{Z}$ is *prime* if $|p| \geqslant 2$ and $p = ab$ implies $|a| = 1$ or $|b| = 1$. We say that $p(x) \in \mathbb{F}[x]$ is prime if $\deg(p) \geqslant 1$ and $p(x) = f(x)g(x)$ implies $\deg(f) = 0$ or $\deg(g) = 0$. Then Euclid's Lemma says that

$$p|ab \Rightarrow p|a \text{ or } p|b \qquad \text{in } \mathbb{Z},$$
$$p(x)|f(x)g(x) \Rightarrow p(x)|f(x) \text{ or } p(x)|g(x) \qquad \text{in } \mathbb{F}[x].$$

You do not need to prove this.

- **Unique Prime Factorization.** Example: Let $p_1, p_2, q_1, q_2 \in \mathbb{Z}$ be prime with $p_1p_2 = q_1q_2$. Since $p_1|q_1q_2$ and p_1 is prime we must have $p_1|q_1$ or $p_2|q_2$. Let's say $p_1|q_1$. Then since q_1 is prime we must have $p_1 = \pm q_1$, hence $p_1p_1 = \pm p_1q_2$. Finally, by canceling p_1 from both sides we obtain $p_2 = \pm q_2$.

- **Example of a Prime Polynomial.** Let $d \in \mathbb{Z}$ be a non-square integer. Then I claim that $x^2 - d$ is a prime element of $\mathbb{Q}[x]$. Proof: If $x^2 - d$ is not prime then we have $x^2 - d = f(x)g(x)$ with $\deg(f) = 1$ and $\deg(g) = 1$. But then $f(x)$ has a root in $\mathbb{Q}$, hence $x^2 - d$ has a root in $\mathbb{Q}$. But I claim that $x^2 - d$ has no roots in $\mathbb{Q}$. Indeed, if $(a/b)^2 - d = 0$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Then $a^2 = db^2$. Now use Euclid's Lemma in $\mathbb{Z}$ to get a contradiction.

(3) Basic Properties of the Field $\mathbb{C}$

- A *complex number* if a formal expression $a + bi$ with $a, b \in \mathbb{R}$. We add and multiply complex numbers as follows:

$$(a + bi) + (c + di) := (a + c) + (b + d)i$$
$$(a + bi)(c + di) := (ac - bd) + (ad + bc)i.$$

These operations make $\mathbb{C}$ into a ring with "zero element" $0 + 0i$ and "one element" $1 + 0i$. In fact, $\mathbb{C}$ is a field, since for any $a + bi \neq 0 + 0i$ we have

$$(a + bi)^{-1} = \left(\frac{a}{a^2 + b^2} \right) + \left(\frac{-b}{a^2 + b^2} \right) i.$$

We can view $\mathbb{R} \subseteq \mathbb{C}$ as a subfield by writing

$$a = a + 0i \quad \text{for all } a \in \mathbb{R}.$$

- For all $a + bi \in \mathbb{C}$ we define $(a + bi)^* := a - bi$. One can check that $(\alpha + \beta)^* = \alpha^* + \beta^*$ and $(\alpha\beta)^* = \alpha^*\beta^*$ for all $\alpha, \beta \in \mathbb{C}$ and $a^* = a$ for all $a \in \mathbb{R}$. And by combining the facts we obtain $f(\alpha)^* = f(\alpha^*)$ for all $f(x) \in \mathbb{R}[x]$ and $\alpha \in \mathbb{C}$. It follows that non-real complex roots of real polynomials come in conjugate pairs.

- Application: Every polynomial with real coefficients has an even number of non-real complex roots (possibly zero).