Math 351 **Homework 4** **Ian Coley**

This assignment is due **Tuesday, 18 February, 2020** at the beginning of lecture. Please write your name, section number, and the names of any collaborators at the top of your homework. Homework should be written or typed legibly using complete sentences and pages should be paper-clipped or stapled together. Remember to justify all answers fully!

Problem 1. For a polynomial $f(x) = a_0 + a_1x + \cdots + a_mx^m$ in $\mathbb{F}[x]$ with $a_m \neq 0$, what is $\gcd(f(x), 0)$? What does it mean if $\gcd(f(x), 0) = 1$?

Problem 2. Prove one of the theorems not proven in class: for a nonconstant polynomial $p(x)$ in $\mathbb{F}[x]$ (for $\mathbb{F}$ a field), the following are equivalent:

(a) $p(x)$ is irreducible.

(b) If $p(x) = r(x)s(x)$, then one of them is a nonzero constant polynomial.

(c) If $p(x) \mid b(x)c(x)$, then $p(x) \mid b(x)$ or $p(x) \mid c(x)$.

Problem 3. Prove that $x^2 + 1$ is reducible in $\mathbb{Z}/p\mathbb{Z}[x]$ if and only if there exist integers a, b such that $p = a + b$ and $ab \equiv 1 \pmod{p}$. Then find two primes $p, q > 5$ such that $x^2 + 1$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$ and reducible in $\mathbb{Z}/q\mathbb{Z}[x]$. After doing all this, look up *quadratic reciprocity* for the complete answer.

Problem 4. Show that if $f(x)$ and $g(x)$ are associates in $\mathbb{F}[x]$, then they have the same roots in $\mathbb{F}$. Is the converse true for all $\mathbb{F}$?

Problem 5. Prove that a polynomial of degree n is determined by $n + 1$ points. Specifically, suppose that $f(x), g(x) \in \mathbb{F}[x]$ and $c_0, \ldots, c_n$ are $n+1$ distinct elements. Show that if $f(c_i) = g(c_i)$ for all i, then $f(x) = g(x)$ as polynomials.

Problem 6. If $\mathbb{F}$ is a finite field, it follow that there are only finitely many irreducible polynomials of any fixed degree. This is hard to compute in general, but not for degree 2.

(a) Prove that there are exactly $(p^2 + p)/2$ *reducible* monic polynomials of degree 2 in $\mathbb{Z}/p\mathbb{Z}[x]$. Hint: every reducible polynomial has to be a product of polynomials of lower degree.

(b) Show that there are exactly $(p^2-p)/2$ *irreducible* monic polynomials of degree 2 in $\mathbb{Z}/p\mathbb{Z}[x]$.

(c) How many total irreducible polynomials of degree 2 are there?

Problem 7. Suppose that R is an integral domain.

(a) Show that the division algorithm for polynomials in $R[x]$ holds as long as the divisor is a *monic* polynomial. Hint: what is the first step of long polynomial division?

(b) Using (a), prove that the factor theorem still holds in $R[x]$, i.e. $f(a) = 0$ if and only if $(x - a) \mid f(x)$.

(c) Conclude that if $f(x)$ is a nonzero polynomial of degree n, it has at most n roots in R.

This is the first step towards a good theory of polynomials in $\mathbb{Z}[x]$.

Problem 8. Prove the quadratic formula. That is, suppose $f(x) = ax^2 + bx + c$ in $\mathbb{R}[x]$. Then the roots of $f(x)$ in $\mathbb{C}$ are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Conclude that $f(x)$ is irreducible if and only if $b^2 - 4ac < 0$.

Problem 9. Let $\mathbb{F}$ be any field and let $x - a$ be a linear polynomial. Prove that $\mathbb{F}[x]/\langle x - a\rangle$ "is" (the proper phrase is *isomorphic* to) $\mathbb{F}$, i.e. the elements are the same, and the multiplication and addition are the same.

Problem 10. Prove that, if $f(x) \in \mathbb{F}[x]$ is a *reducible* polynomial, $\mathbb{F}[x]/\langle f(x)\rangle$ is not a field. Then choose a reducible polynomial $f(x) \in \mathbb{Q}[x]$ and find two zero divisors in $\mathbb{Q}[x]/\langle f(x)\rangle$.

Problem 11. Let d be a squarefree number, i.e. $d \in \mathbb{Z}$ such that no prime p satisfies $p^2 \mid d$. Consider the ring

$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \subset \mathbb{C}$$

(a) Prove that $\mathbb{Q}(\sqrt{d})$ is a subfield of $\mathbb{C}$.

(b) Prove that $x^2 - d$ is irreducible in $\mathbb{Q}[x]$. Hint: it has roots in $\mathbb{C}$ – are they in $\mathbb{Q}$?

(c) Compare $\mathbb{Q}[x]/\langle x^2 - d\rangle$ to $\mathbb{Q}(\sqrt{d})$.

Problem 12. Show that if $p(x)$ is an irreducible quadratic polynomial (for any $\mathbb{F}[x]$), then $\mathbb{F}[x]/\langle p(x)\rangle$ automatically contains two roots of $p(x)$, not just the one guaranteed by the theorem.

Problem 13. Show that the above phenomenon is not true in general:

(a) What are the three roots of $x^3 - 2$ in $\mathbb{C}$?

(b) As this is irreducible over $\mathbb{Q}$, we know that $\mathbb{Q}[x]/\langle x^3 - 2\rangle$ is a field. Prove that it only contains the real root of $x^3 - 2$.

Problem 14. As a first exploration of something we'll make clearer next week, consider $\mathbb{Z}/2\mathbb{Z}[x]/\langle x^2 + x + 1\rangle = K$.

(a) Prove that $x^2 + x + 1$ is the only irreducible quadratic polynomial in $\mathbb{Z}/2\mathbb{Z}[x]$, which is why we keep using it.

(b) Prove that K has characteristic 2, in the sense of Homework 3, Problem 5. Conclude that K cannot be $\mathbb{Z}/4\mathbb{Z}$ (which has characteristic 4).

(c) Why can't K be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?

Again, the appropriate notion above is not "is" or "be" but *isomorphic*.