Math 412. Polynomial rings

DEFINITION: A polynomial is **monic** if its leading term (i.e., the term of highest degree) has coefficient 1.

THE DIVISION ALGORITHM FOR POLYNOMIALS. Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x) \text{ and either } r(x) = 0 \text{ or } \deg r(x) < \deg g(x).$$

THEOREM 4.8: Let F be a field and $a(x), b(x) \in F[x]$, not both zero. Then there is a unique monic polynomial that is the *greatest common divisor* $d(x)$ of $a(x)$ and $b(x)$. There exist (not necessarily unique) $u(x), v(x) \in F[x]$ such that $u(x)a(x) + v(x)b(x) = d(x)$.

THEOREM 4.14: Let F be a field. Every nonconstant polynomial in $F[x]$ can be factored into *irreducible polynomials.* This factorization is essentially unique in the sense that if we have two factorizations into irreducibles

$$f_1 \cdots f_r = g_1 \cdots g_s,$$

then $r = s$, and after reordering, each f_i is a unit multiple of g_i for all i.

Part 1: Computation.

A. PRACTICE WITH THE DIVISION ALGORITHM FOR POLYNOMIALS. You may have learned to divide polynomials to find a quotient and remainder in high school. The goal in every step is to find some ax^n (that will go into the "quotient") that makes the leading term of the divisor cancel the leading term of the dividend.

(1) Let $f = x^3 + 4x^2 + x + 1$ in $\mathbb{R}[x]$. Find q and r so that $f = qx^2 + r$, where $\deg r < 2$.[1]

(2) In the ring $\mathbb{Z}_2[x]$, divide the polynomial $x^5 + 3x^3 + x^2 + 1$ by $x^2 + 1$. What are the quotient and remainder?

(3) Consider the polynomials $f(x) = x^2 - 3$ and $g(x) = 2x - 1$ in $R = \mathbb{Z}[x]$. What happens if you try to divide $f(x)$ by $g(x)$ *in* $\mathbb{Z}[x]$*?* Is the division algorithm theorem for polynomials true if we only assume that "F" is a *domain*?

Solution.

(1) $q = x + 4, r = x + 1$.

(2) $q = x^3 + 1$, $r = 0$. Remember, in $\mathbb{Z}_2[x]$, the coefficients are really congruence classes living in $\mathbb{Z}_2$ and not integers living in $\mathbb{Z}$. This means we can replace these coefficients by anything else in their congruence class modulo 2. For instance, $x^5 + 3x^3 + x^2 + 1 = x^5 + x^3 + x^1 + 1$ in $\mathbb{Z}_2[x]$.

(3) It doesn't work when we try to do it becuase we end up dividing by 2. The division algorithm is FALSE in this setting. We can show that this f, g are a counterexample to the analgous statement over $\mathbb{Z}[x]$. We will prove that no such q, r as in the statement exist by contradiction. If there were $q, r \in \mathbb{Z}[x]$ with $\deg r < \deg g = 1$ such that $f = qg + r$, these would also live in $\mathbb{R}[x]$, and satisfy the hypotheses of the division algorithm there. Such a solution is unique, and we can find that it is

[1] Hint: If this is unfamiliar to you, the first term we want in q is some ax^n such that $(ax^n)(x^2) = (x^3)$. Now subtract off $(ax^n)(x^2)$ from f and continue...

$q(x) = \frac{1}{2}x + \frac{1}{4}$ and $r(x) = \frac{-11}{4}$. But, these are not elements of $\mathbb{Z}[x]$, so this is a contradiction.

B. FINDING GCDS. Use Theorem 4.14 to find the greatest common divisor of the given polynomials.

(1) Compute the **greatest common divisor** of $2x^2 - 10x + 12$ and $x^7 - 3x^6$ in $\mathbb{Q}[x]$.
(2) Compute the **greatest common divisor** of $(x^2+1)(x^3+x^2)$ and $x^5(x+1)^2$ in $\mathbb{Z}_2[x]$.
(3) Discuss Theorem 4.8 above with your team. Write out what the theorem says about the gcds you found (1) and (2). (Your statement should use the words ”there exist”.) In what sense is the gcd of two polynomials the “greatest”?

Solution.

(1) Factor: $2x^2 - 10x + 12 = 2(x-3)(x-2)$ and $x^7 - 3x^6 = x^6(x-3)$ so $(x-3)$ is the gcd.
(2) This is tricky because the coefficients are in $\mathbb{Z}_2$. Note that $(x+1)^2 = x^2 + 1$ in $\mathbb{Z}_2[x]$. So $(x^2+1)(x^3+x^2) = (x+1)^3x^2$ and $x^5(x+1)^2$ so the gcd is $x^2(x+1)^2$.
(3) The theorem says that there exists $f, g, \in \mathbb{Q}[x]$ such that $f(2x^2 - 10x + 12) + g(x^7 - 3x^6) = x - 3$. Also that there exists $f, g, \in Z_2[x]$ such that $x^2(x+1)^2 = f(x^2+1)(x^3+x^2) + gx^5(x+1)^2$.

Part 2: Theory.

C. THE REMAINDER THEOREM AND THE FACTOR THEOREM. Fix $f \in \mathbb{F}[x]$.

(1) **Remainder Theorem:** Prove that for any $\lambda \in \mathbb{F}$, the remainder when f is divided by $(x - \lambda)$ is $f(\lambda)$.
(2) **Factor Theorem:** Prove that $(x - \lambda)$ divides f if and only if $f(\lambda) = 0$.
(3) Show that $1, 2, 3$ and 4 are all roots of $x^4 - 1$ in $\mathbb{Z}_5[x]$.
(4) Use the factor theorem to find the factorization of $x^5 - x$ completely into irreducibles as guaranteed by Theorem 4.14 in the ring $\mathbb{Z}_5[x]$.

Solution.

(1) Use the division algorithm to write $f = q(x - \lambda) + r$ where $r = 0$ or $\deg r < \deg(x - \lambda) = 1$. This tells us that r is a constant polynomial. To figure out what constant polynomial, plug in λ to both sides and observe $r = f(\lambda)$.
(2) Since we know $f = (x - \lambda) + f(\lambda)$, we see that that if $f(\lambda) = 0$, then $(x - \lambda)|f$. Conversely, if $(x - \lambda)|f$, then in the unique division statement, the remainder is zero. But also the remainder is $f(\lambda)$.
(3) Plug them in!
(4) We have five roots $0, 1, 2, 3, 4$. Thus, we get five irreducible factors, so $x(x-1)(x-2)(x-3)(x-4)$ divides f. Since the degrees match there must be no other factors and no repeated factors, and since the leading coefficients agree, this must be it.

D. IRREDUCIBILITY. Let $\mathbb{F}$ be any field.

(1) Show that if a polynomial $f \in \mathbb{F}[x]$ has degree three or two, then f is irreducible if and only if f has no roots.
(2) Show that (1) is false for polynomials of degree 4, even in $\mathbb{R}[x]$.
(3) Find the factorization of $x^5 - x$ completely into irreducibles as guaranteed by Theorem 4.14 in the ring $\mathbb{Z}_7[x]$.

Solution.

(1) By problem C2 above, we know that if a polynomial has a root, then it is not irreducible. Converseley, we would like to show that if $f \in \mathbb{F}[x]$ is a degree-2 or degree-3 polynomial and f is *reducible*, then f has a root. So suppose f is reducible. Then we can write $f = gh$ for some non-constant polynomials $g, h \in \mathbb{F}[x]$. As $\mathbb{F}$ is a field, and fields are domains, we know that $\deg f = \deg g + \deg h$ by our last worksheet. We know $\deg g$ and $\deg h$ are positive integers and that $\deg f = 2$ or $\deg f = 3$. In either case, the only way this can be possible is if either $\deg g = 1$ or $\deg h = 1$. Without loss of generality, we may assume $\deg g = 1$. Now, any linear polynomial in $\mathbb{F}[x]$ has a root. Indeed, we can express g as $g = ax + b$ for some $a, b \in \mathbb{F}[x]$, where $a \neq 0$. Then $g(-ba^{-1}) = 0$. Thus $f(-ba^{-1}) = g(-ba^{-1})h(-ba^{-1}) = 0$, as desired.
(2) The polynomial $x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ is reducible, since $x^4 + 2x^2 + 1 = (x^2 + 1)^2$. However, this polynomial has no roots in $\mathbb{R}$.
(3) We can factor out a copy of x to get $x^5 - x = x(x^4 - 1)$ and then use the "difference of squares formula" (does this formula work in any ring?) twice to get $x^5 - x = x(x-1)(x+1)(x^2+1)$. Are we done yet? Linear polynomials are always irreducible,

so we just have to check whether x^2+1 is irreducible. By problem D1, it suffices to check that x^2+1 has no roots in $\mathbb{Z}_7$, which we can check by brute force.

Part 3: Going deeper.

Fix a polynomial $f(x) \in \mathbb{F}[x]$. Define two polynomials $g, h \in \mathbb{F}[x]$ to be **congruent modulo** f if $f|(g-h)$. We write $g \equiv h \mod f$. The set of all polynomials congruent to g modulo f is written $[g]_f$.

E. Congruence in $\mathbb{F}[x]$.

(1) Prove that *Congruence is an equivalence relation:*
   (a) reflexive: for all g, we have $g \equiv g \mod f$;
   (b) symmetric: $g \equiv h \mod f$ implies $h \equiv g \mod f$ for all $g, h \in \mathbb{F}[x]$.
   (c) transitive: $g \equiv h \mod f$ and $h \equiv k \mod f$ implies $g \equiv k \mod f$ for all $g, h, k \in \mathbb{F}[x]$.

(2) Prove that $[g]_f = \{g + kf \mid k \in \mathbb{F}[x]\}$.

(3) Prove that if $h \in [g]_f$, then $[g]_f = [h]_f$.

(4) Explain why, for any two polynomials $g, h \in \mathbb{F}[x]$, either $[g]_f = [h]_f$ or $[g]_f \cap [h]_f = \emptyset$.

Solution. Use the same ideas as we did for congruence classes modulo n over $\mathbb{Z}$.

F. Congruence Classes in $\mathbb{F}[x]$. Fix a polynomial $f(x) \in \mathbb{F}[x]$ of degree $d > 0$.

(1) Prove that every congruence class $[g]_f$ contains a *unique* polynomial of the set $S = \{h(x) \in F[x] \ : \ h(x) = 0 \text{ or } \deg h(x) < d\}$.

(2) How many distinct congruence classes are there for $\mathbb{Z}_2[x]$ modulo $x^3 + x$?

(3) How many distinct congruence classes are there for $\mathbb{Z}_3[x]$ modulo $x^2 + x$?

Solution.

(1) For each congruence class modulo f, pick some element g in that congruence class. Let r be the remainder of dividing g by f; then r has degree less than d or $r = 0$, and $f|(g-r)$ by definition of r. So $r \in [g]_f$ and $r \in S$. That is, we have shown that every congruence class contains at least one element of S.

Let g and h be two polynomials in S which are both in the same congruence class modulo f. Since g and h are in the same congruence class, then $f|g-h$. Since g and h are both in S, $g-h$ is either 0 or a polynomial of degree less than d. Since f can't divide a non-zero polynomial of degree smaller than d, we get that $g-h=0$. Hence, each congruence class contains at most one polynomial in S.

(2) $2^3 = 8$.

(3) $3^2 = 9$

G. Ring Structure on the set of Congruence Classes modulo f in $\mathbb{F}[x]$.

(1) Fix a polynomial $f(x) \in \mathbb{F}[x]$ of degree $d > 0$. Let $\mathcal{R}$ be the set of all congruence classes modulo f. Can you define a natural addition and multiplication on $\mathcal{R}$ to make it into a ring? Remember: Each is element of $\mathcal{R}$ is a set, so be careful with your definition!

(2) In the case of $\mathbb{Z}_2[x]$ modulo x^2, the ring $\mathcal{R}$ has only four elements: why? Make a table for your operations on $\mathcal{R}$. To what familiar ring is $\mathcal{R}$ isomorphic?

Solution.

(1) Just as we did with congruences modulo n, we can check that $[g] + [h] = [g + h]$ and $[g] \cdot [h] = [gh]$ are well-defined operations, and they make $\mathcal{R}$ into a ring with zero $[0]$ and one $[1]$.

(2) There are only four polynomials of degree less 2: $0, 1, x$, and $x+1$. Each one of these represents a distinct class. This ring is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, with isomorphism given by

$$\begin{aligned} (0,0) &\longleftrightarrow 0 \\ (1,1) &\longleftrightarrow 1 \\ (1,0) &\longleftrightarrow 1 + x \\ (0,1) &\longleftrightarrow x \end{aligned}$$