Math 412. Adventure sheet on 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.

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 $\mathbb{F}_2[x]$, divide the polynomial $x^5 + 3x^3 + x^2 + 1$ by $x^2 + 1$. What are the quotient and remainder?
(3) In the ring $\mathbb{Q}[x]$, divide $x^4 + 3x^3 - x^2 + 5$ by $x + 1$. What are the quotient and remainder?
(4) 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) $q = x^3 + 1, r = 0$
(3) $q = x^3 + 2x^2 - 3x + 3, r = 2$.
(4) 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 $q(x) = \frac{1}{2}x + \frac{1}{4}$ and $r(x) = \frac{-11}{4}$. But, these are not elements of $\mathbb{Z}[x]$, so this is a contradiction.

[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...

B. THE PROOF OF THE DIVISION ALGORITHM FOR POLYNOMIALS:
The proof uses a similar method as the proof for $\mathbb{Z}$.

(1) Consider the set $\mathcal{S} := \{f(x) - g(x)q(x) \mid q(x) \in F[x]\} \subseteq F[x]$. Explain why the existence part of the Division algorithm is equivalent to the statement that $0 \in \mathcal{S}$ or $\mathcal{S}$ contains an element of degree less than $\deg d$.
(2) Show that if $\mathcal{S}$ contains an element of degree 0, the division algorithm holds for $f(x)$ and $g(x)$.
(3) If $\mathcal{S}$ contains an element h of degree $\delta' \geqslant \delta = \deg(g)$, subtract a suitable multiple of g to find a smaller degree element in $\mathcal{S}$.
(4) Prove the existence part of the statement. Hint: Chose an element of smallest positive degree in $\mathcal{S}$. What axiom guarantees we can do this?
(5) Prove the uniqueness part of the statement.

Solution. See page 92 in the book.

C. 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”.]

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 $x^2(x+1)^2 = f(x^2+1)(x^3+x^2) + gx^5(x+1)^2$.

D. EUCLIDEAN ALGORITHM IN $\mathbb{F}[x]$. Fix a field $\mathbb{F}$.

(1) Suppose that $f, g \in \mathbb{F}[x]$, and we use the division algorithm to write $f = qg + r$ for some appropriate $q, f \in \mathbb{F}[x]$. Prove that gcd (f, g) = gcd (g, r). [Hint: the proof is basically “the same” as for the ring $\mathbb{Z}$.]
(2) Use the Euclidean Algorithm to compute (f, g), where $f = x^3 + 4x^2 + x$ and $g = x^2 + x$ in $\mathbb{C}[x]$.
(3) Express x as a linear combination of f and g from the previous part.
(4) Sketch a proof of THEOREM 4.8.

Solution.

(1) The proof is basically the same as for the ring $\mathbb{Z}$. If d divides both f and g, write $f = ad$ and $g = db$. Then d must divide $r = f - gq = da - dbq = d(a - bq)$. Similarly, if d divides both g and r, it must divide g. So the common factors of f

and g are the same as the common factors of g and r. So the common monic factor with the largest degree is the same too.

(2) To compute (x^3+4x^2+x, x^2+x), we first write $x^3+4x^2+x = q(x^2+x)+r$, where $q = x+3$ and $r = -2x$. We know that

$$(x^3+4x^2+x, x^2+x) = (x^2+x, -2x).$$

Now, by inspection we see that x is the highest degree monic polynomial dividing both.

(3) Backsubstitute to get $x = \frac{-1}{2}(x^3+4x^2+x) + \frac{x-3}{2}(x^2+x)$.

(4) We can run the Euclidean algorithm to get to the GCD. Backsubstituting, we can express each remainder as a linear combination of the dividend and divisor before it, and eventually get the GCD as a linear combination of the things we started with.

E. 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 $\mathbb{Z}_5[x]$.
(5) 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) 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, plus in λ to both sides and observe $r = f(\lambda)$.
(2) Since we know $f = (x-\lambda) + f(\lambda)$, we see that that is $f(\lambda) = 0$, 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.

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

(1) Show that if a polynomial $g \in \mathbb{F}[x]$ has degree three or two, then g is irreducible if and only if g has no roots.
(2) Show that (1) is false for polynomials of degree 4, even in $\mathbb{R}[x]$.

G. POLYNOMIAL RINGS OVER DOMAINS. Let R be a domain (which may or may *not* be a field!).

(1) Let $g(x) \in R[x]$ be a *monic* polynomial, and $f(x) \in R[x]$ be any polynomial. Show that there exist unique polynomials $q(x), r(x) \in R[x]$ such that

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

(2) Show that if $r \in R$, and $f(x) \in R[x]$, then $f(r) = 0$ if and only if $(x - r)$ divides $f(x)$ in $R[x]$.

Solution. Use essentially the same proofs as in the field case!

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 $[g]_f$.

G. 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 $\mathbb{Z}$.

H. 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 degree less than 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, and $f|(f-r)$ by definition of r. So every congruence class contains at least one element of degree less than d.

   Given two polynomials g and h of degree less than d, $f - g$ is a polynomial of degree less than d, and the only polynomial of degree smaller than d that f divides is 0. We conclude that $f|(g-h)$ if and only if $g = h$. So each congruence class contains at most one polynomial of degree less than d.

(2) $2^3 = 8$.

(3) $3^2 = 4$

I. 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

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