Commutative Algebra in Context — Fall 2020
Homework 1 Solutions — Drew Armstrong

Problem 1. Prove that a polynomial $f(x) \in \mathbb{F}[x]$ of degree d over a field $\mathbb{F}$ has at most d roots[1] in $\mathbb{F}$. [Hint: Given $\alpha \in \mathbb{F}$ and $f(\alpha) = 0$ we can divide $f(x)$ by $x - \alpha$ to get $f(x) = (x - \alpha)g(x)$ with $g(x) \in \mathbb{F}(x)$ of degree $d-1$. By induction on degree we know that $g(x)$ has at most $d-1$ roots in $\mathbb{F}$.]

Proof. For any polynomials $f(x), h(x) \in \mathbb{F}[x]$ where $h(x) \neq 0$, the division algorithm produces polynomials $g(x), r(x) \in \mathbb{D}[x]$ such that $f(x) = g(x)h(x) + r(x)$, where either $r(x) = 0$ or $\deg(r) < \deg(h)$. In the case $h(x) = x - \alpha$ we have $f(x) = (x - \alpha)g(x) + r(x)$, where $r(x) = 0$ or $\deg(r) = 0$, i.e., $r(x) = c$ for some constant $c \in \mathbb{F}$. Then substituting $x = \alpha$ gives

$$0 = f(\alpha) = (\alpha - \alpha)g(\alpha) + c = c.$$

We conclude that $f(x) = (x - \alpha)g(x)$ for some $g(x) \in \mathbb{F}[x]$ of degree $d - 1$. Now let $\beta \in \mathbb{F}$ be any other root of $f(x)$, so that

$$0 = f(\beta) = (\beta - \alpha)g(\beta).$$

If $\beta \neq \alpha$ then since $\mathbb{F}$ is a field this implies that $g(\beta) = 0$, hence β is also a root of $g(x)$. By induction on degree, there can be at most $d - 1$ such roots. Hence $f(x)$ can have at most d roots in $\mathbb{F}$: α together with the roots of $g(x)$ that are not equal to α. $\square$

Problem 2. A commutative ring A is called an *integral domain* (or just *domain*) if $a, b \in A \setminus \{0\}$ implies $ab \in A \setminus \{0\}$.

(a) Prove that A is a domain if and only if it is a *subring of a field*.

(b) If A is a domain, use (a) and Problem 1 to prove that a nonzero polynomial $f(x) \in A[x]$ has only finitely many roots in A.

Proof. (a): Let $A \subseteq \mathbb{F}$ be a subring of a field. If $ab = 0$ for some $a, b \in A$ with $b \neq 0$ then we have $a = 0b^{-1} = 0$, hence A is a domain. Conversely, let A be a domain and let $\text{Frac}(A)$ be the set of formal symbols a/b with $b \neq 0$ (called *fractions*). We define an equivalence relation as follows:

$$a/b = a'/b' \quad \Leftrightarrow \quad ab' = a'b.$$

We define addition and multiplication of fractions as follows:

$$a/b + c/d = (ad + bc)/(bd) \quad \text{and} \quad (a/b)(c/d) = (ad)/(bd).$$

[1] Distinct, or counted with multiplicity.

The fractions on the right are defined because $b, d \neq 0$ implies $bd \neq 0$. We observe that addition and multiplication are well-defined with respect to equivalence. Indeed, suppose that $a/b = a'/b'$ (i.e., $ab' = a'b$) and $c/d = c'/d'$ (i.e., $cd' = c'd$). Then we have

$$(ad+bc)(b'd') = (ab')(dd') + (cd')(bb') = (a'b)(dd') + (c'd)(bb') = (a'd' + b'c')(bd)$$

and

$$(ad)(b'c') = (ab')(c'd) = (a'b)(cd') = (a'd')(bc),$$

as desired. Next one can check that these operations define a **field structure** on $\text{Frac}(A)$. The key point is that a "nonzero fraction" a/b has $a \neq 0$, hence there exists an "inverse fraction" $(a/b)^{-1} = b/a$. Finally, we observe that the the function $\varphi : A \to \text{Frac}(A)$ defined by $a \mapsto a/1$ is an injective ring homomorphism. In this sense we can regard A as a subring of its *field of fractions* $\text{Frac}(A)$.

(b): Let A be a domain and let $f(x) \in A[x]$ be nonzero, of degree d. From part (a) we can regard $f(x)$ as an element of $\text{Frac}(A)[x]$. Then from Problem 1 we know that $f(x)$ has finitely many (at most d) roots in $\text{Frac}(A)$ and it follows that $f(x)$ has finitely many roots in A. □

Problem 3. Let A be an infinite domain and suppose that $f(x), g(x) \in A[x]$ satisfy $f(\alpha) = g(\alpha)$ for infinitely many $\alpha \in A$. In this case prove that $f(x) = g(x)$ as polynomials (i.e., they have the same coefficients).

Proof. Consider the polynomial $f(x) - g(x) \in A[x]$. By assumption this polynomial has infinitely many roots $\alpha \in A$, hence it follows from Problem 2(b) that $f(x) - g(x)$ is the zero polynomial. □

Problem 4. Let $\mathbf{x} = (x_1, \ldots, x_n)$ be vector of independent variables and let A be a domain. Define the degree function $A[\mathbf{x}] \setminus \{0\} \to \mathbb{N}$ and prove that it satisfies $\deg(fg) = \deg(f) + \deg(g)$. In particular, this implies that $A[\mathbf{x}]$ is also a domain.

Proof. Let $I = (i_1, \ldots, i_n) \in \mathbb{N}^n$ be a vector of exponents. By definition, any monomial $a\mathbf{x}^I = ax_1^{i_1} \cdots x_n^{i_n} \in A[\mathbf{x}]$ with $a \neq 0$ has degree $\sum I = i_1 + \cdots + i_n$. For any two vectors $I, J \in \mathbb{N}^n$ the product of monomials $m(\mathbf{x}) = a\mathbf{x}^I$ and $n(\mathbf{x}) = b\mathbf{x}^J$ with $a, b \neq 0$ is $m(\mathbf{x})n(\mathbf{x}) = (ab)\mathbf{x}^{I+J}$. Since A is a domain we have $ab \neq 0$ and hence

$$\deg(mn) = \sum(I+J) = \sum I + \sum J = \deg(m) + \deg(n).$$

Now we define the degree of a polynomial $f(\mathbf{x}) \in A[\mathbf{x}]$ as the highest degree of a monomial that it contains. To complete the proof, consider any two nonzero polynomials $f(\mathbf{x}), g(\mathbf{x}) \in A[\mathbf{x}]$ with (possibly non-unique) leading monomials $m(\mathbf{x})$ and $n(\mathbf{x})$. To complete the proof, I claim that $m(\mathbf{x})n(\mathbf{x})$ is a leading monomial in the product $f(\mathbf{x})g(\mathbf{x})$. To see this, we observe that every monomial in $f(\mathbf{x})g(\mathbf{x})$ has the form $m'(\mathbf{x})n'(\mathbf{x})$ for some monomials $m'(\mathbf{x})$ and $n'(\mathbf{x})$

from $f(\mathbf{x})$ and $g(\mathbf{x})$. Then by assumption we have $\deg(m') \leq \deg(m)$ and $\deg(n') \leq \deg(n)$, hence

$$\deg(m'n') = \deg(m') + \deg(n') \leq \deg(m) + \deg(n) = \deg(mn).$$

Finally, since $m(\mathbf{x})n(\mathbf{x})$ is a leading monomial in $f(\mathbf{x})g(\mathbf{x})$ it follows that $\deg(fg) = \deg(mn) = \deg(m) + \deg(n) = \deg(f) + \deg(g)$, as desired. $\square$

Problem 5. Let A be a commutative ring and let $F(\mathbf{x}) \in A[\mathbf{x}]$ be a polynomial in some finite list of variables $\mathbf{x} = (x_1, \ldots, x_n)$. Consider the following conditions:

(H1) Every term of $F(\mathbf{x})$ has the form $ax_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ where $i_1 + \cdots + i_n = d$ and $0 \neq a \in A$.

(H2) We have $F(\lambda\mathbf{x}) = \lambda^d F(\mathbf{x})$ for all scalars $\lambda \in A$.

Polynomials satisfying (H1) are called *homogeneous of degree d*. Prove we always have (H1)⇒(H2). If A is an infinite domain prove that we also have (H2)⇒(H1). [Hint for (H2)⇒(H1): For any polynomial $F(\mathbf{x}) \in A[\mathbf{x}]$ and variable y note that $F(y\mathbf{x}) = \sum_{k\geq 0} y^k F^{(k)}(\mathbf{x}) \in A[\mathbf{x}][y]$, where the sum has finitely many terms and $F^{(k)}(\mathbf{x})$ is homogeneous of degree k in the sense of (H1). Use Problems 3 and 4 to show that $F(\mathbf{x}) = F^{(d)}(\mathbf{x})$.]

Proof. (H1)⇒(H2): The monomial $m(\mathbf{x}) = ax_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ satisfies

$$\begin{aligned} m(\lambda\mathbf{x}) &= a(\lambda x_1)^{i_1}(\lambda x_2)^{i_2}\cdots(\lambda x_n)^{i_n} \\ &= \lambda^{i_1+i_2+\cdots+i_n} a x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} = \lambda^d m(\mathbf{x}). \end{aligned}$$

The same holds for any A-linear combination of monomials, i.e., for any polynomial.

(H2)⇒(H1): Let $F(\mathbf{x}) \in A[\mathbf{x}]$ be any polynomial satisfying $F(\lambda\mathbf{x}) = \lambda^d F(\mathbf{x})$ for all $\lambda \in A$. Note that any monomial $m(\mathbf{x}) = a\mathbf{x}^I$ in $F(\mathbf{x})$ satisfies $m(y\mathbf{x}) = y^{\sum I} m(\mathbf{x})$, where y is another variable. Thus we can write $G(\mathbf{x}, y) := F(y\mathbf{x}) = \sum_{k\geq 0} y^k F^{(k)}(\mathbf{x}) \in A[\mathbf{x}][y]$ as a polynomial in y with coefficients from the ring $A[\mathbf{x}]$. On the other hand, let $H(\mathbf{x}, y) := y^d F(\mathbf{x}) \in A[\mathbf{x}][y]$. By assumption we know that $G(\mathbf{x}, \lambda) = H(\mathbf{x}, \lambda) = 0 \in A[\mathbf{x}]$ for all $\lambda \in A \subseteq A[\mathbf{x}]$. If A is an infinite domain then this holds for infinitely many λ in the domain $A[\mathbf{x}]$, hence it follows from Problem 3 that $G(\mathbf{x}, y) = H(\mathbf{x}, y)$ as elements of $A[\mathbf{x}][y]$. By comparing coefficients this means that $F^{(k)}(\mathbf{x}) = 0$ for all $k \neq d$ and $F^{(d)}(\mathbf{x}) = F(\mathbf{x})$, as desired. $\square$

6. Let A be an infinite domain and consider an invertible matrix $\Phi \in \mathrm{GL}_n(A)$. Let $F(\mathbf{x}) \in A[\mathbf{x}]$ be homogeneous of degree d. In this case prove that $G(\mathbf{x}) := F(\Phi\mathbf{x}) \in A[\mathbf{x}]$ is also homogeneous of degree d. [Hint: Use Problem 5.]

Proof. We will verify condition (2) of Problem 5, which will imply condition (1) because A is an infinite domain. Consider the vector of polynomials $\mathbf{u} = \Phi\mathbf{x} \in A[\mathbf{x}]^n$. By evaluating the equation $F(\lambda\mathbf{x}) = \lambda^d F(\mathbf{x})$ at $\mathbf{x} = \mathbf{u}$ we obtain the equation $F(\lambda\mathbf{u}) = \lambda^d F(\mathbf{u})$ in the ring $A[\mathbf{x}]$. Then since $\mathbf{x} \mapsto \Phi\mathbf{x}$ is a linear function we have

$$G(\lambda\mathbf{x}) = F(\Phi\lambda\mathbf{x}) = F(\lambda\Phi\mathbf{x}) = \lambda^d F(\Phi\mathbf{x}) = \lambda^d G(\mathbf{x})$$

for all $\lambda \in A$, as desired. $\square$

7. For any ring A, the A-linear function $D_x : A[x] \to A[x]$ is defined by

$$D_x(x^k) := \begin{cases} kx^{k-1} & k > 0, \\ 0 & k = 0. \end{cases}$$

Prove that the following properties are satisfied for all $f(x), g(x) \in A[x]$:

(a) $D_x(fg) = D_x(f)g + fD_x(g)$,

(b) $D_x(g^k) = kg^{k-1}D_x(g)$,

(c) $D_x(f \circ g) = (D_x(f) \circ g)D_x(g)$.

Proof. (a): The left and right sides of the equation are A-bilinear functions of f and g. Thus it suffices to prove the statement when $f(x) = x^m$ and $g(x) = x^n$. In this case we have

$$D_x(f)g + fD_x(g) = mx^{m-1}x^n + x^m nx^{n-1} = (m+n)x^{m+n-1} = D_x(fg).$$

(b): We observe that the statement is true for $k = 0$. Now assume that $D_x(g^k) = kg^{k-1}D_x(g)$ for some $k \geq 0$. Then from part (a) we have

$$D_x(g^{k+1}) = D_x(gg^k) = D_x(g)g^k + gkg^{k-1}D_x(g) = (k+1)g^k D_x(g)$$

as desired.

(c): Let $f(x) = \sum a_k x^k$ so that $f \circ g = \sum a_k g^k$. Then it follows from (b) that

$$D_x(f \circ g) = \sum a_k D_x(g^k) = \left(\sum a_k k g^{k-1}\right) D_x(g) = (D_x(f) \circ g)D_x(g).$$

$\square$

8. Euler's Formula. Let $\mathbf{x} = (x_1, \ldots, x_n)$. We define the function $D_{x_i} : A[\mathbf{x}] \to A[\mathbf{x}]$ as in Problem 5 by thinking of $A[\mathbf{x}] = A_i[x_i]$ as the ring of polynomials in x_i with coefficients from $A_i := A[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$. Now fix some $F(\mathbf{x}) \in A[\mathbf{x}]$ and $d \geq 0$ and consider the following condition:

(H3) $\sum_i x_i D_i(F) = dF$

Prove that (H1)$\Rightarrow$(H3) for any ring. If A is a domain of characteristic zero (necessarily infinite), prove that we also have (H3)$\Rightarrow$(H1). [Hint for (H3)$\Rightarrow$(H1): Write $F(\mathbf{x}) = \sum_k F^{(k)}(\mathbf{x})$ where each $F^{(k)}(\mathbf{x})$ is a sum of monomials of degree k. Then since the operator $\sum_i x_i D_{x_i}$ is linear we have $dF = \sum_i x_i D_{x_i}(F) = \sum_k \sum_i x_i D_{x_i}(F^{(k)})$.]

Proof. (H1)$\Rightarrow$(H3): For any monomial $m(\mathbf{x}) = ax_1^{e_1} \cdots x_n^{e_n}$ we have

$$x_i D_{x_i}(m) = x_i a e_i x_1^{e_1} \cdots x_{i_1}^{e_{i-1}} x_i^{e_i - 1} x_{i+1}^{e_{i+1}} \cdots x_n^{e_n} = e_i a x_1^{e_1} \cdots x_n^{e_n} = e_i m(\mathbf{x}),$$

so that

$$\sum x_i D_{x_i}(m) = (e_1 + \cdots + e_n) m(\mathbf{x}) = \deg(m) m(\mathbf{x}).$$

But note that the operator $\sum x_i D_{x_i}$ is A-linear. Thus if every monomial in $F(\mathbf{x})$ has degree d then we conclude that $\sum x_i D_{x_i}(F) = dF$.

(H3)⇒(H1): Let us assume that $\sum x_i D_{x_i}(F) = dF$ for some polynomial $F(\mathbf{x}) \in A[\mathbf{x}]$, and let us write $F(\mathbf{x}) = \sum F^{(k)}(\mathbf{x})$ where each $F^{(k)}(\mathbf{x})$ is a sum of monomials of degree k. Our goal is to show that $F(\mathbf{x}) = F^{(d)}(\mathbf{x})$. Then from the first part of the proof we obtain

$$\begin{aligned} \sum x_i D_{x_i}(F) &= dF \\ \sum_i x_i D_{x_i} \left(\sum_k F^{(k)} \right) &= dF \\ \sum_k \sum_i x_i D_{x_i}(F^{(k)}) &= dF \\ \sum_k k F^{(k)}(\mathbf{x}) &= d \sum_k F^{(k)}(\mathbf{x}). \end{aligned}$$

Now let y be another variable and substitute $\mathbf{x} \mapsto y\mathbf{x}$ to obtain

$$\begin{aligned} \sum_k k F^{(k)}(y\mathbf{x}) &= d \sum_k F^{(k)}(y\mathbf{x}) \\ \sum_k k y^k F^{(k)}(\mathbf{x}) &= d \sum_k y^k F^{(k)}(\mathbf{x}) \\ \sum_k k y^k F^{(k)}(\mathbf{x}) &= \sum_k d y^k F^{(k)}(\mathbf{x}). \end{aligned}$$

We can regard this as an identity of polynomials in the ring $A[\mathbf{x}][y]$, hence the coefficient of y^k is the same on each side:

$$\begin{aligned} k F^{(k)}(\mathbf{x}) &= d F^{(k)}(\mathbf{x}) \\ (k-d) F^{(k)}(\mathbf{x}) &= 0. \end{aligned}$$

Finally, since A is a domain of characteristic zero, we see that $k \neq d$ implies $F^{(k)}(\mathbf{x}) = 0 \in A[\mathbf{x}]$, and hence $F(\mathbf{x}) = F^{(d)}(\mathbf{x})$ as desired. $\square$