Lang's Algebra Chapter 4 Solutions

Amanuel Tewodros

November 20, 2025

(1) We will show that a $\implies$ b $\implies$ c $\implies$ a.

a $\implies$ b Suppose there is $g(X)$, $\deg g > 0$, such that $(g(X)) \supsetneq (f(X))$. This implies there is $h(X)$ such that $h(X)g(X) = f(X)$. By primality, $g(X) \notin (f(X))$, implies $h(X) \in (f(X))$. This implies $h(X)$ generates $(f(X))$ which implies $h(X) = cf(X)$ and $g(X) = d$ for some $d \in k$, a contradiction. Hence $(f(X))$ must be maximal.

b $\implies$ c If $f(X) = g(X)h(X)$, where neither $g(X)$ nor $h(X)$ are units, then $(g(X)) \supsetneq (f(X))$, contradicting the maximality of $(f(X))$.

c $\implies$ a Let $h(X) = r(X)s(X) \in (f(X))$. Since $k[X]$ is UFD and $f(X)|h(X)$, the prime factorization at least one of r and s contains $f(X)$ as a factor. WLOG, let $f(X) \mid r(X)$, then $r(X) \in (f(X))$ and thus $(f(X))$ is prime.

(2) (a) The equivalent statement for rational numbers is the following:
For a given rational number a/b and the set of primes P of $\mathbb{Z}$, we have

$$\frac{a}{b} = \sum_{p\in P} \frac{a_p}{p^{j_p}} + N,$$

where $j_p > 0$ if $a_p = 0$, $a_p = 0$ if $j_p = 0$, $a_p \le p^{j_p}$ and N is an integer. This expression is unique.
First, we show that such expression exists. Let b be a product of two coprime numbers c and d. The by Euclid's algorithm, there are numbers x, y such that $cx + dy = a$. Substituing this in a/b, we see that

$$\frac{a}{b} = \frac{x}{d} + \frac{y}{c}.$$

And hence,

$$\frac{a}{b} = \sum_{p\in P} \frac{a_p}{p^{j_p}},$$

Where $a_p = 0$ if $j_p = 0$. If $a_p \ge p^{j_p}$, then we can write a_p/p^{j_p} as $a'_p/p^{j_p} + N_p$ for some $N_p > 0$ and $a_p < p^{j_p}$. Hence, the given expression exists. For uniqueness, let

$$\frac{a}{b} = \sum_{p\in P} \frac{a_p}{p^{j_p}} + N = \sum_{p\in P} \frac{b_p}{p^{i_p}} + M.$$

Fix a prime q and WLOG assume $j_q > i_q$. Then we have the following equation

$$\ell(a_q - p^{j_q - i_q} b_q) = q^{j_q} L,$$

where ℓ is the least common multiple of all $p^{j_p}, p^{i_p}, p \neq q$ and L is some integer. Since q^{j_p} divides the L.H.S but not ℓ and a_q, we have $j_q = i_q$. This implies

$$\frac{a_q - b_q}{q^{j_q}} = \sum_{p\neq q} \frac{b_p - a_p}{p^{j_p}} + M - N$$

Since $q \nmid p^{j_p}$ we have $b_p = a_p$ and since $|a_q - b_q| < p^{j_p}$, $M = N$. Hence, the expression is unique.

(b) The equivalent statement for positive integers is the following:
If $\alpha, \beta \in \mathbb{Z}$, such that $\beta > 1$, then there exisit unique positive integers

$$\alpha_0, \alpha_1, \ldots, \alpha_d \in \mathbb{Z},$$

such that $\alpha_i < \beta$ and

$$\alpha = \alpha_0 + \alpha_1 \beta + \cdots + \alpha_d \beta^d.$$

If $\alpha < \beta$, there is nothing to show. If $\beta \leq \alpha$, then by Euclid's algorithm, there are unique positive integers q and $r < \beta$ such that $\alpha = q\beta + r$ and $q < \alpha$. By induciton, existence (and thust uniqueness) is proven.

(3) $f(X+Y) \mod Y = f(X)$. Collecting similar powers of Y, we have the given expression. Now take the i-th derivative of $f(X+Y)$ with respect to Y

$$D^i f(X+Y) = \sum_{k=i}^{n} k! \phi_k(X) Y^{k-i}.$$

Substituting $Y = 0$, you get $D^i f(X) = i! \phi_i(X)$.

(4) First we introduce the notion of partial derivative similar to that in calcus as follows:

$$\frac{\partial}{\partial X_i} \Big(\sum_{(v)} a_{(v)} X_1^{v_1} \cdots X_n^{v_n} \Big) = \begin{cases} \big(\sum_{(v)} a_{(v)} v_i X_1^{v_1} \cdots X_i^{v_i - 1} \cdots X_n^{v_n} \big) \text{ if } v_i > 0, \\ 0 \text{ if otherwise.} \end{cases}$$

We define the taylor expansion in n variables as a polynomial in $k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ such that

$$f(X_1 + Y_1, \ldots, X_n + Y_n) = f(X_1, \ldots, X_n) + \sum_{(v)} \phi_{(v)}(X_1, \ldots, X_n) Y^{v_1} \cdots Y^{v_n}.$$

The above definition can be shown to be unambiguous using a similar proof as (3). Taking the v_i-th partial derivative of f with respect to X_i followed by substituting $Y_i = 0$ and rearranging terms the following relation is proved.

$$\phi_{(v)}(X_1, \ldots, X_n) = \frac{1}{v_1! \cdots v_n!} \frac{\partial^{v_1 + \cdots + v_n} f}{\partial X_1^{v_1} \cdots \partial X_n^{v_n}}$$

(5) (a) For $f(X) = X^4 + 1$, we notice that $f(X+1) = X^4 + 4X^3 + 6X^2 + 4X + 2$ is irreducible over $\mathbb{Z}$ by Eisenstein's crietrion or irreducibility. For $g(X) = X^6 + X^3 + 1$, reducibity over $\mathbb{Z}$ fails by the integral root test as $g(\pm 1) \neq 0$. Irreducibilty over $\mathbb{Q}$ directly follows from the irreducibility over $\mathbb{Z}$.

(b) If f is a reducible polynomial over k, say $f(X) = g(X)h(X)$, $\deg h, \deg g \geq 1$, then $\deg h + \deg g = 3$. This can only happen if either of h and g has degree 1. $X^3 - 5X^2 + 1$ fails irreducibility test by the integral root test thus not irreducible over $\mathbb{Q}$.

(c) Considering $X^2 + Y^2 - 1$ as an element of $K[Y][X]$, we see that $K[Y]$ is factorial and we can use Eisenstein's irreduciblity test using the irreducible $Y - 1$ as p and we see that $Y - 1 \mid Y^2 - 1, (Y-1)^2 \nmid Y^2 - 1$ and $Y - 1 \nmid 1$. Thus $X^2 + Y^2 - 1$ is irreducible over $\mathbb{Q}$ and $\mathbb{C}$.

(6) Let $f(X) = a_0 + \cdots + a_d X^d$. We can turn f to monic by factoring out a_d as $g(X) = f(X)/a_d = X^d + \frac{a_{d-1}}{a_d} X^{d-1} + \cdots + \frac{a_0}{a_d}$. If $t_1, \ldots, t_m$ are the root of g, then we have $t_1 \cdots t_m = a_0/a_d$. It then must be the case that for a root $t_i = x_i/y_i$, $x_i \mid a_0$ and $y_i \mid a_d$.

(7) (a) Suppose $(0, \ldots, 0)$ is the only root of f. Since $a^{q-1} = 1$ for any finite field with q elements and $a \neq 0$,

$$1 - f(X)^{q-1} = \begin{cases} 1 \text{ if } X = 0, \\ 0 \text{ otherwise.} \end{cases}$$

Let $g(X_n) = 1 - f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_{n-1}][X_n]$. This implies all the units $u_1, \ldots, u_{q-1}$ are zeros of g and $\prod_{k=1}^{q-1}(X_n - u_k)$ divides $g(X_n)$. This product is equal to $X_n^{q-1} - 1$. Doing this for all X_i, we see that

$$h(X)\prod_{s=1}^{n} 1 - X_s^{q-1} = (1 - f(X)^{q-1}).$$

The degree of the polynomial on the RHS $< n(q-1)$ where as that of the LHS is $\deg h + (q-1)n > (q-1)n$, a contradiction. Thus $f(X)$ must have a root other than 0.

(b) If $q = 2$, the sum expression is obviously true. Otherwise note that u is unit iff $-u$ is unit in k and that $u^k = v^k$ iff $v = u$ if u and v are units. Thus the sum expression is true. By definition,

$$N = \sum_{x\in k^n} (1 - f(x)^{q-1}).$$

The second expresion for $\prod_i \psi(i)$ directly follow from taking the sum fixing each x_k one by one and factoring out common units $x_1^{i_1}\cdots x_k^{i_k}$ for all valid k.

For the last part, we have

$$I = \{(i_1,\ldots,i_n) \in \mathbb{Z}^n_{\geq 0} : i_1 + \cdots + i_n \leq d(q-1)\}.$$

$$\begin{aligned} N &= \sum_{x\in k^n} (1 - f(x)^{q-1}) \\ &\equiv -\sum_{i\in I} c(i) \sum_{x\in k^n} x_1^{i_1}\cdots x_n^{i_n} \pmod q \\ &\equiv -\sum_{i\in I} c(i)\prod_{k=1}^{n}\psi(i_k) \pmod q. \end{aligned}$$

In the last term all exponents i_j can not be a multiple of $q-1$ because otherwise $\deg f \geq n$. Thus the product $\mathrm{mod}\ q = 0$ and the statement is proved. dots

(c) By assumption and (b) $f_1\cdots f_r(a) = 0$ for some $a \neq 0$. This implies at least one $f_i(a) = 0$. But then $\sum_{k=1}^{r}\prod_{j\neq k} f_j(a) = \prod_{j=1,j\neq i}^{r} f_j(a)$ which implies we have $f_j \neq f_i$ such that $f_j(a) = 0$. Carrying out this process, we prove that a is shared across all a.

(d) Let f be an arbitrary function from $k^n \to k$. Then we define the polynomial $g \in k[X_1,\ldots,X_n]$ as

$$g(X_1,\ldots,X_n) = \sum_{c\in k^n} f(c)(1 - \prod_{i=1}^{n}(X_i - c_i)^{q-1}).$$

It is clear $g = f$

(8) The induced map is going to be the map $f(X) \mapsto f(aX+b)$ which also fixes the elements of A. The map is injective because if $f(aX+b) = 0$, then $f(X) = 0$ for infinitely many entries thus $f(X) = 0$. We also observe that $f(aX+b) = h(X)$, then $h(a^{-1}X - a^{-1}b) = f(X)$, making the induced map an automorphism with the inverse $f(X) \mapsto f(a^{-1}X - a^{-1}b)$.

(9) Let f be an automorphism on $A[X]$. By bijectivity, for any $p \in A[X]$, we have $\deg f(p) = \deg p$. Thus $\deg f(X) = 1$ or $f(X) = aX + b$ for some $a, b \in A$. Now suppose $X = f(cX+d) = ac(X) + cb + d$. This implies $ac = 1$ and a must be a unit.

(10) Let $X \mapsto p(X)/q(X) \in K(X)$ where p and q are coprime in $K[X]$. By surjectivity, we have $f(X) = \sum_{i=0}^{d'} a_i X^i, g(X) = \sum_{i=0}^{d} b_i X^i, a_{d'}, b_d \neq 0$ such that $f(\frac{p}{q}X)/g(\frac{p}{q}X) = X$. We note that

$$f(\frac{p}{q}X) = \big(\sum_{i=0}^{d'} a_i p^i(X) q^{d'-i}(X)\big)/q^{d'}(X)$$

. Similar thing can be said for $g(\frac{p}{q}X)$. By rearranging terms, we get the equation

$$xq^{d'}(X)\sum_{i=0}^{d} b_i p^i(X) q^{d-i}(X) = q^d(X)\sum_{i=0}^{d'} a_i p^i(X) q^{d'-i}(X). \tag{1}$$

We have three cases:

$d' < d$. Since $q^d(X)$ must divide the L.H.S, $q(X) \mid \sum_{i=0}^{d} b_i p^i(X) q^{d-i}(X)$ or $q(X) \mid x$. The former can only happen if $b_d = 0$ contradicting assumption. This implies $q(X) \mid x$ or in other words $q(X) = cX$ for some $c \in K$.

$d' > d$. This is similar to the previous case except there are no enough factors in R.H.S to accomodate the extra multipicity of $q(X)$ and thus impossible to have such (d', d) pair.

$d' = d$. In this case, we can simiplify and rearrange terms to get

$$(b_d X - a_d) p^d(X) = \sum_{i=0}^{d-1} (a_i - x b_i) p^i(X) q^{d-i}(X).$$

Since $q(X)$ divides the R.H.S and p and q are coprime, $q(X) \mid b_d X - a_d \notin K$. Thus $\deg q \leq 1$.

Thus $q(X) = aX + b$ for some $a, b \in K$. To show that $\deg p \leq 1$, we suppose NOT, and compare the degrees of two sides of equation 1. The LHS has a degree of $1 + d' \deg q + d \deg p$. The RHS has a degree of $d \deg q + d' \deg p$. This is clearly a contradiction, thus $\deg p \leq 1$.

(11) (a) Given the extension homomorphism D in K, $D(1) = D(1/1) = 0$ and $D(1/y) = -Dy/y^2$. Then, for $x, y \in A$,

$$\begin{aligned} D(xy) &= D(x/y^{-1}) \\ &= \frac{y^{-1}Dx - xD(1/y)}{y^{-2}}. \\ &= xDy + yDx \end{aligned}$$

Next, we show that D is well-defined in K.

$$\begin{aligned} D(cx/xy) &= \frac{cyD(cx) - cxD(cy)}{c^2y^2} \\ &= \frac{cy(cDx + xDc) - cx(cDy + yDc)}{c^2y^2} \\ &= D(x/y). \end{aligned}$$

(b)

$$\begin{aligned} L(xy) &= D(xy)/xy \\ &= xDy/xy + yDx/xy \\ &= Dy/y + Dx/x \\ &= L(x) + L(y) \end{aligned}$$

(c) Applying product rule directly,

$$\begin{aligned} R'(X) &= D\big(c \prod_i (X - \alpha_i)^{m_i}\big) \\ &= c \sum_i m_i (X - \alpha_i)^{m_i - 1} \prod_{j \neq i} (X - \alpha_j)^{m_j} \end{aligned}$$

Dividing this sum by $R(X)$, we get the desired sum.

(12) (a) Let $f(X) = (a_1 X - b_1)(a_2 X - b_2) = a_1 a_2 (X - \frac{b_1}{a_1})(X - \frac{b_2}{a_2})$. The discriminant is then

$$\begin{aligned} D(f) &= (a_1 a_2)^2 \left(\frac{b_1}{a_1} - \frac{b_2}{a_2} \right)^2 \\ &= (a_2 b_1 - a_1 b_2)^2 \\ &= (a_2 b_1 + a_1 b_2)^2 - 4 a_1 a_2 b_2 b_2 \\ &= b^2 - 4ac \end{aligned}$$

(b) We first prove the expression is true for $a_0 = 1$ and $f(X) = (X - t_1)(X - t_2)(X - t_3)$.

$$\begin{aligned}
s_1^2 s_2^2 &= ((t_1 + t_2 + t_3)(t_1 t_2 + t_2 t_3 + t_3 t_1))^2 \\
&= \left(\sum x_1^2 x_2 + 3 s_3\right)^2 \\
&= \sum x_1^4 x_2^2 + 9 s_3^2 \\
&\quad + 2\left(\sum x_1^3 x_2^3 + \sum x_1^4 x_2 x_3 + \sum x_1^3 x_2^2 x_3 + \sum x_1^2 x_2^2 x_3^2\right) \\
&\quad + 6 \sum x_1^3 x_2^2 x_3 \\
&= \sum x_1^4 x_2^2 + 2 \sum x_1^4 x_2 x_3 + 2 \sum x_1^3 x_2^3 + 8 \sum x_1^3 x_2^2 x_3 + 15 x_1^2 x_2^2 x_3^2 \\
s_1^3 s_3 &= (t_1 + t_2 + t_3)^3 s_3 \\
&= s_3\left(\sum x_1^3 + 3 \sum x_1^2 x_2 + 6 \sum x_1 x_2 x_3\right) \\
&= \sum x_1^4 x_2 x_3 + 3 \sum x_1^3 x_2^2 x_3 + 6 \sum x_1^2 x_2^2 x_3^2 \\
s_2^3 &= (t_1 t_2 + t_2 t_3 + t_3 t_1)^3 \\
&= \sum x_1^3 x_2^3 + 3 \sum x_1^3 x_2^2 x_3 + 6 \sum x_1^2 x_2^2 x_3^2 \\
s_1 s_2 s_3 &= s_3 (t_1 + t_2 + t_3)(t_1 t_2 + t_2 t_3 + t_3 t_1) \\
&= s_3\left(\sum x_1^2 x_2 + 3 x_1 x_2 x_3\right) \\
&= \sum x_1^3 x_2^2 x_1 + 3 x_1^2 x_2^2 x_3^2
\end{aligned}$$

where the sums are taken over all order pairs $(x_1, x_2, x_3) \in \{t_1, t_2, t_3\}^3, x_i \neq x_j$. By the definition of the discriminant, we have

$$\begin{aligned}
D_f &= (t_1 - t_2)^2 (t_2 - t_3)^2 (t_1 - t_3)^2 \\
&= \sum x_1^4 x_2^2 - 2 \sum x_1^4 x_2 x_3 - 2 \sum x_1^3 x_2^3 + 2 \sum x_1^3 x_2^2 x_3 - 6 x_1^2 x_2^2 x_3^2
\end{aligned}$$

From the above one obtains

$$D_f = s_1^2 s_2^2 - 4 s_1^3 s_3 - 4 s_2^3 + 18 s_1 s_2 s_3 - 27 s_3^2.$$

Since the above polynomial is homogenous of degree 6 and $D_{cf} = c^4 D_f$, the statement follows.

(c) $f'(X) = \sum_{i=1}^n \prod_{j \neq i} (X - t_i)$. Hence $f'(t_i) = \prod_{i \neq j} (t_i - t_j)$ where i is fixed. By definition

$$D_f = (-1)^{n(n-1)/2} \prod_{i \neq j} (t_i - t_j).$$

where the product is taken over all pairs $(i, j) i \neq j$ which is equivalent to

$$D_f = (-1)^{n(n-1)/2} \prod_{i=1}^n f'(t_i).$$

(13) (a) First suppose, f and g are coprime. By Mason-Stothers we have

$$\begin{aligned}
3 \deg f &\leq \deg f + \deg g + \deg(f^3 - g^2) - 1 \\
2 \deg g &\leq \deg f + \deg g + \deg(f^3 - g^2) - 1
\end{aligned}$$

Adding the above inequalities and simplifying, we get

$$\deg f \leq 2 \deg(f^3 - g^2) - 2$$

If f and g have common factor, then $n_0(fg) < n_0(f) + n_0(g) \leq \deg f + \deg g$. Hence the statement is proven.

(b) The proof for case for relativey prime f, g is very similar to (a). So suppose $f = df_1, g = dg_1$ where $d \notin K$ is the greatest common divisor of f and g.
Taking $A = Ad, f = f_1, g = g_1, B = B$ in the relatively prime case, we then have the following

$$\begin{aligned}
\deg f_1 &\leq \deg Ad + \deg B + 2\deg(Adf_1^3 + Bg_1^2) - 2 \\
&\leq \deg A + \deg d + \deg B + 2\big((Af^3 + Bg^2)/d^2\big) - 2 \\
&\leq \deg A + \deg d + \deg B + 2(\deg(Af^3 + Bg^2) - 2\deg d) - 2 \\
&\leq \deg A + \deg B + 2\deg(Af^3 + Bg^2) - 3\deg d - 2 \\
\implies \deg f &\leq \deg A + \deg B + 2\deg(Af^3 + Bg^2) - 2
\end{aligned}$$

Taking $A = d$ and $B = -1$, we get the general case for part (a).

(c) By part (b), we may assume without loss of generality that f and g are coprime. By Mason's Theorem,

$$m\deg(f) \leqslant \deg(f) + \deg(g) + \deg(h) - 1$$

$$n\deg(g) \leqslant \deg(f) + \deg(g) + \deg(h) - 1$$

Then, with the above equations we find:

$$(n-1)(m-1)\deg(f) \leqslant (n-1)\deg(g) + (n-1)\deg(h) - (n-1)$$

$$(n-1)\deg(g) \leqslant \deg(f) + \deg(h) - 1$$

Adding these together, we find the general version:

$$\big((n-1)(m-1) - 1\big)\deg(f) \leqslant n\deg(h) - n$$

(14) Let $\epsilon > 0$ be a positive number and let u, v be relatively prime non-zero integers. Let $w = u + v$. Define a polynomial f as

$$f(X) = X(X - 3u)(X + 3v)$$

Making the translation $\xi = X + v - u$, we get

$$f(\xi) = \xi^3 - \gamma_2\xi - \gamma_3.$$

Since the discriminant is preserved under such translation, we have the following

$$D = 4\gamma_2^3 - 27\gamma_3^2 = 3^6(uvw)^2.$$

But, by the generalized Szpiro conjecture,

$$\begin{aligned}
|\gamma_2| &\ll N_o(D)^{2+\epsilon} \\
&\ll N_o((uvw)^2)^{2+\epsilon} = N_o(uvw)^{2+\epsilon},
\end{aligned}$$

and

$$|\gamma_3| \ll N_o(uvw)^{3+\epsilon}$$

If r_1, r_2, r_3 are the roots of $f(\xi)$, then

$$\begin{aligned}
\gamma_2 &= -(r_1r_2 + r_2r_3 + r_3r_1) \\
&= -((v-u)(v+w) + (v+w)(-u-w) + (-u-w)(v-w)) \\
\gamma_3 &= r_1r_2r_3 \\
&= (v-u)(v+w)(-u-w)
\end{aligned}$$

From above, the abc conjecture follows.

(15) Define two sets:

$$A = \{p \text{ prime} : 2^{p-1} \not\equiv 1 \mod p^2\}$$

$$B = \{p \text{ prime} : 2^n \equiv 1 \mod p \text{ and } 2^n \not\equiv 1 \mod p^2, n \geq 1\}$$

The two sets are equivalent: Let $p \in B$ and let d be the order of 2 modulo p. Since $2^d - 1 \mid 2^n - 1$, we note that $2^d \not\equiv 1 \mod p^2$. At the same time, $2^{p-1} - 1 = (2^d - 1)(p-1)/d$ (since $d \mid (p-1)$), we note that $2^{p-1} - 1 \not\equiv 0 \mod p^2$. Hence, $B \subseteq A$. The reverse inclusion directly follows from Fermat's little theorem. It follows that we can write any number of the form $2^n - 1$ as a product xy such that $x \in A = B$ and $y \in A^c$. If A is finite, then $x \leq \prod_{p \in A} p$. We also note that, by assumption, $N_0(y) \ll \sqrt{y}$. Assuming abc conjecture is true and taking $a = 2^n - 1$ and $b = 1$, we have

$$\begin{aligned} 2^n - 1 &= xy \\ &\ll N_0(xy)^{1+\epsilon} \\ &\ll y^{(1/2)(1+\epsilon)} \end{aligned}$$

which can only be true if y is bounded. This implies the finiteness of A^c, contradicting the infinitude of primes.

(16) Let $F(X) = a_0 + a_1 X + \cdots + a_d X^d$ and $G(X) = b_0 + b_1 X + \cdots + b_{d'} X^{d'}$, and assume that

$$|F| = \max_{0 \leq i \leq d} |a_i| \geq 1, \qquad |G| = \max_{0 \leq j \leq d'} |b_j| \geq 1.$$

Let S be the Sylvester matrix of F and G, of size $(d + d') \times (d + d')$. The resultant R of F and G satisfies

$$R = \det(S) = \sum_{\sigma \in \mathfrak{S}_{d+d'}} \operatorname{sgn}(\sigma) \prod_{i=1}^{d+d'} S[i, \sigma(i)].$$

Taking absolute values and using the triangle inequality,

$$|R| \leq \sum_{\sigma \in \mathfrak{S}_{d+d'}} \prod_{i=1}^{d+d'} |S[i, \sigma(i)]|.$$

Each entry of S is a coefficient of F or G, hence has absolute value at most $\max(|F|, |G|)$. More precisely, exactly d' rows contain coefficients of F and d rows contain coefficients of G, so each product contains d' occurrences of coefficients of F and d occurrences of coefficients of G. Therefore,

$$|R| \leq |F|^{d'} |G|^d (d + d')! =: B. \tag{1}$$

WLOG, we can assume $\gcd(F, G) = 1$. There exist polynomials $\phi, \psi \in \mathbb{C}[X]$ such that

$$R = \phi(X) F(X) + \psi(X) G(X),$$

with

$$\deg \phi < d', \qquad \deg \psi < d.$$

Write

$$\phi(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_{d'-1} X^{d'-1}, \qquad \psi(X) = \beta_0 + \beta_1 X + \cdots + \beta_{d-1} X^{d-1}.$$

Equating coefficients of X^k in $R = \phi F + \psi G$, and padding all coefficients outside their natural ranges with 0, we obtain the system

$$a_0 \alpha_0 + b_0 \beta_0 = R, \tag{2}$$

$$\sum_{i=0}^{k} (a_i \alpha_{k-i} + b_i \beta_{k-i}) = 0, \qquad 1 \leq k \leq d + d' - 1. \tag{3}$$

From (1) and (2) we get

$$|a_0 \alpha_0 + b_0 \beta_0| = |R| \leq B.$$

Since $|a_0| \le |F|$ and $|b_0| \le |G|$, it follows that

$$|\alpha_0| + |\beta_0| \le \frac{|R|}{\min(|a_0|, |b_0|)} \le B. \tag{4}$$

We now prove by induction on k that

$$|\alpha_k| + |\beta_k| \le kB \quad \text{for all } 0 \le k \le d + d' - 1. \tag{5}$$

The case $k = 0$ is (4). Assume the claim holds for all $0, 1, \ldots, k-1$. Using (3), we have

$$a_0\alpha_k + b_0\beta_k = -\sum_{i=1}^{k}(a_i\alpha_{k-i} + b_i\beta_{k-i}).$$

Taking absolute values,

$$|a_0||\alpha_k| + |b_0||\beta_k| \le \sum_{i=1}^{k}\big(|a_i||\alpha_{k-i}| + |b_i||\beta_{k-i}|\big).$$

Using $|a_i| \le |F|$, $|b_i| \le |G|$, and the induction hypothesis,

$$|a_0||\alpha_k| + |b_0||\beta_k| \le |F|\sum_{i=1}^{k}|\alpha_{k-i}| + |G|\sum_{i=1}^{k}|\beta_{k-i}| \le (|F| + |G|)\sum_{i=1}^{k}(iB).$$

Since $\sum_{i=1}^{k} i = \frac{k(k+1)}{2} \le k^2$, and $|a_0|, |b_0| \ge 1$, we obtain

$$|\alpha_k| + |\beta_k| \le kB.$$

This completes the induction and proves (5).

Now evaluate the identity $R = \phi(w)F(w) + \psi(w)G(w)$ at $X = w$:

$$|R| = |\phi(w)F(w) + \psi(w)G(w)| \le (|\phi(w)| + |\psi(w)|)(|F(w)| + |G(w)|). \tag{6}$$

Since $|\alpha_k| + |\beta_k| \le kB$ and $c = \max(1, |w|)$, we have

$$|\phi(w)| + |\psi(w)| \le \sum_{k=0}^{d+d'-1}(|\alpha_k| + |\beta_k|)|w|^k \le \sum_{k=0}^{d+d'-1} kB\,c^k \le Bc^{d+d'}(d + d'). \tag{7}$$

Finally, combining (1), (6), and (7), we obtain

$$|R| \le c^{d+d'}|F|^{d'}|G|^d(d + d')^{d+d'}(|F(w)| + |G(w)|).$$

(17) (a) By definition $g(X)$ has $d-2$ integral (and therefore real) roots, $b_1, \ldots, b_{d-2}$ and conjugate pairs of complex roots. Since each b_i is distinct, all the local exterema of the $g(X)$ lays striclty above or below the x-axis. We can find the extremea by taking the derivative and solving $Dg(X) = 0$ for X. Let $x_1, \ldots x_{d-2}$ be the solutions and let $y_i := |g(x_i)|$. Then by the monotonicity of p/p^{dn}, there exists n such that $p/p^{dn} < y_i$ for all y_i. For such n, $g_n(X)$ has exactly $d-2$ real roots.

(b) Let $g(X) = a_0 + \cdots + X^d$. Note that

$$(p^{dn})g_n(X) = p + p^{dn}a_0 + p^{dn-n}a_1(p^nX) + \cdots + p^na_{d-1}(p^nX)^{d-1} + (p^nX)^d$$

By Eisenstein's criterion of irreduciability, the RHS is irreducible in $\mathbb{Z}$. But that means $g_n(X)$ is irreducible in $\mathbb{Q}$.

(18) (a) $P(X) = \frac{1}{2}X^2 + \frac{1}{2}X$.

(b) First we show that the set $\{\binom{X}{i}\}$ for $0 \le i \le r$ form a $\mathbb{Q}$-basis for the submodule of $\mathbb{Q}[X]$ of polynomials of degree at most r: We proceed by induction on r. The case $r = 0$ is clear since $\binom{X}{0} = 1$. Assume the claim holds for $r-1$ and let

$$f(X) = a_rX^r + a_{r-1}X^{r-1} + \cdots + a_0 \in \mathbb{Q}[X]$$

have degree r. As $\binom{X}{r} = \dfrac{1}{r!}X^r +$ (lower degree terms), there is a unique rational number $b_r = a_r r!$ for which the polynomial $g(X) := f(X) - b_r\binom{X}{r}$ has degree $< r$; by the induction hypothesis g is a unique $\mathbb{Q}$-linear combination of $\binom{X}{0}, \ldots, \binom{X}{r-1}$, whence $f(X) = \sum_{i=0}^{r} b_i\binom{X}{i}$ with uniquely determined $b_i \in \mathbb{Q}$. This shows the family spans and is linearly independent, so it is a basis.
Hence, given $P \in \mathbb{Q}$ that is integral for at least all $n \geq N, N \in \mathbb{N}$. We can write

$$P(X) = b_r\binom{X}{r} + \cdots + b_0\binom{X}{0}.$$

We note that $\binom{X+1}{i} - \binom{X}{i} = \binom{X}{i-1}$. Hence $P_1(X) = P(X+1) - P(X)$. Defining $P_i(X) = P_{i-1}(X+1) - P_{i-1}(X)$ for $i \geq 2$, we get that

$$P_i(X) = \sum_{k=0}^{r-i} b_{i+k}\binom{X}{k}.$$

Each $P_i(X)$ is integral for at least all sufficiently large n. But $P_r(X)$ is a constant polynomial namely $P_r(X) = b_r$, whence $b_r \in \mathbb{Z}$. This proves $P_r(X)$ is integral for all $\mathbb{N}$. Now assume all $b_{r-k+1} \in \mathbb{Z}$ for all $k \leq i$ and $P_{r-i+1}(X)$ is integral for all $\mathbb{Z}$ for some i. Since $P_{r-i+1}(0) \in \mathbb{Z}$, $P_{r-i}(1) - P_{r-i}(0) = b_{r-i} \in \mathbb{Z}$ and it follows that $P_{r-i}(X)$ is also integral for all $\mathbb{Z}$. Inducting on i, the stament follows.

(c) Since Q is integral, let $Q(X) = \sum_{i=0}^{\deg Q} a_i\binom{X}{i}$. Then by part (b) of this question, there is a polynomial $P(n)$ such that $Q(n) = P(n) - P(n-1)$ if we define $P(X) = \sum_{i=0}^{\deg Q} a_i\binom{X}{i+1} + c$ where c is any constant. Let m be the smallest integer such that $Q(m) = f(m) - f(m-1)$. It follows that $f(n) = \sum_{k=m}^{n} Q(k) + f(m-1)$. Similarly $P(n) = \sum_{k=m}^{n} Q(k) + P(m-1)$. Hence $f(n) - P(n) = f(m-1) - P(m-1)$. Since c can be any constant per our definiton, we can pick c so that $P(m-1) = f(m-1)$, making $P(n) = f(n)$ for all $n \geq m$.

(19) (a) Let I be the ideal generated by $s_1, \ldots, s_n$. Since a monomial is homogeneous and any ideal of $\mathbb{Z}[X]$ is closed under addition, it suffices to prove the statement for a monomial

$$M(X) = X_1^{a_1} \cdots X_n^{a_n},$$

where $a_i \geq 0$ and $\sum a_i > n(n-1)$. Without loss of generality, let $a_1 \geq a_2 \geq \cdots \geq a_n$. Since $\deg M > n(n-1)$, by the pigeonhole principle we have $a_1 \geq n$.
If $a_1 = n$, then each X_i must appear as a factor of M at least once, making

$$M(X) = f(X)s_n \equiv 0 \pmod{I}.$$

If $a_1 > n$, then

$$\begin{aligned}
X_1^{a_1} &\equiv -X_1^{a_1-1}(X_2 + \cdots + X_n) && \pmod{I} \\
&\equiv X_1^{a_1-2} \sum_{1<i<j\leq n} X_i X_j && \pmod{I} \\
&\equiv -X_1^{a_1-3} \sum_{1<i<j<k\leq n} X_i X_j X_k && \pmod{I} \\
&\vdots \\
&\equiv (-1)^n X_1^{a_1-n}(X_2 \cdots X_n) && \pmod{I} \\
&\equiv 0 && \pmod{I}.
\end{aligned}$$

Hence every monomial, and therefore every homogeneous polynomial in $\mathbb{Z}[X]$ of degree $> n(n-1)$, lies in the ideal $I = (s_1, \ldots, s_n)$.

(b) Let $j \geq i \geq 1$ and let $s_i^{(j)}(Y_1, \ldots, Y_j)$ be an i-th elementary symmetric polynomial in j variables $Y_1, \ldots Y_j$, i.e.,

$$s_i^{(j)}(Y_1, \ldots, Y_j) = \sum_{(r)} Y_{r_1} \cdots Y_{r_i}.$$

With this notation, we have $s_i = s_i^{(n)}(X_1, \ldots, X_n)$. Note that $s_i^{t-1}(Y_1, \ldots Y_{t-1}) = s_i^t(Y_1, \ldots, Y_t) - Y_t s_{i-1}^{t-1}(Y_1, \ldots, Y_{t-1})$ if $i \geq 1$ and $s_0^{t-1} = s_0^t - Y_t$. Hence $s_i^{n-1}(X_2, \ldots, X_n) \in \mathbb{Z}[s_1, \ldots, s_n, X_1]$. Similarly, $s_i^{n-j}(X_{j+1}, \ldots, X_n) \in \mathbb{Z}[s_1, \ldots, s_n, X_1, \ldots, X_j]$. Let $a_j(X) = (X - X_j) \cdots (X - X_n)$.

$$\begin{aligned} a_j(X_j) &= (X_j - X_j) \cdots (X_j - X_n) \\ &= X_j^{n-j+1} - s_1^{n-j+1}(X_j, \ldots, X_n) X_j^{n-j} \\ &+ \cdots \pm s_{n-j+1}(X_j, \ldots, X_n) \\ &= 0 \end{aligned}$$

Hence the ideal $(1, X_j, \ldots, X_j^{n-j})$ spans $\mathbb{Z}[s_1, \ldots, s_n, X_1, \ldots, X_{j-1}][X_j]$ for all $2 \leq j \leq n$ and $(1, X_1, \ldots, X_1^{n-1})$ spans $\mathbb{Z}[s_1, \ldots, s_n][X_1]$. To show the set is linearly independent, it suffices to show that the $n \times n$ Vandermonde matrix

$$V = \begin{bmatrix} 1 & X_1 & X_1^2 & \ldots & X_1^{n-1} \\ 1 & X_2 & X_2^2 & \ldots & X_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & X_n^2 & \ldots & X_n^{n-1} \end{bmatrix}$$

has non-zero determinant because we are looking for solutions $f_1, f_2, \ldots f_n \in \mathbb{Z}[s] = \mathbb{Z}[s_1, \ldots, s_n]$ such that

$$f_n(s) X^{n-1} + f_{n-1}(s) X^{n-2} + \cdots + f_1(s) = 0.$$

By the permutation notation, $\det(V)$ is the symmetric sum

$$\sum_{\sigma \in \mathfrak{S}} \operatorname{sgn}(\sigma) X_{\sigma(1)}^{n-1} \cdots X_{\sigma(n)}^0,$$

which is non-zero. By Cramers's rule, the equation

$$V[f_1(s), \ldots, f_n(s)]^\top = \mathbf{0}$$

has a unique solution which is the trivial solution. Hence $\{1, X_1, \ldots, X_1^{n-1}\}$ form a basis for $\mathbb{Z}[s][X_1]$. By similar argument, $\{1, X_j, \ldots, X_j^{n-j}\}$ form a basis set over $\mathbb{Z}[s^{(n-j)}][X_j] = \mathbb{Z}[s, X_1, \ldots, X_{j-1}][X_j]$.

Taking the cartesian product of the basis sets, we observe that $\prod_{(r)} X_i^{r_i}$ forms a $\mathbb{Z}[s]$-basis for $\mathbb{Z}[X]$.

(c) Using almost the exact same technique as part (b), we can show that $\mathbb{Z}[X][Y]$ is a free $\mathbb{Z}[X, s']$-module with basis $Y^{(q)}$. Similarly, we can show that $\mathbb{Z}[s'][X]$ is a free $\mathbb{Z}[s', s]$-module with basis $X^{(r)}$. Since X and Y are algebraically independent, one can see that the product $X^{(r)} Y^{(q)}$ forms a $\mathbb{Z}[s, s']$-basis for $\mathbb{Z}[X, Y]$.

(d) Since $I \subset \mathbb{Z}[s, s']$ and $\mathbb{Z}[s, s'] \subset \mathbb{Z}[X, Y] \implies I \subset J, I \subset J \cap \mathbb{Z}[s, s']$. Hence, it suffices to prove the reverse inclusion. Let $f(s, s')$ be an element in the intersection. By (c), one sees that $f(s, s') = \sum_{(r),(q)} a_{(r),(q)}(s, s') X^{(r)} Y^{(q)}$. Since $f(s, s') \in J$, it follows that $a_{(r)(q)} \in I$. Since $f(s, s') \in \mathbb{Z}[s, s']$, one shall be able to write f as $\sum_{a \in I} ag(s, s') \subseteq I$.

(20) Let (e_i) and (f_i) be variables such that $a_{m-k} = s_k(e_i)$ and $b_{n-k} = s_k(f_i)$. By definition, $0 = c_{m+n-k} = s_k(e_i, f_i)$ for all $k < n + m$. Let $M(a)$ be a monomial in a_i such that the degree of $M > (n+m)(n+m-1) \geq n(n-1)$. By problem 19(a), $M(a) \in (s_k(e_i)) \subseteq (s_k(e_i, f_i))$. However, only $s_{n+m}(e_i, f_i)$ is non-zero and equal to 1 (because $a_0 = b_0 = 1$) which implies $M(a) \in (s_{n+m}(e_i, f_i)) = \mathbb{Z}$. This can only be true if the product is 0.

(21) Let $x, y \in K$. Then

$$\begin{aligned} x + y \mapsto \lambda_t(x + y) &= \sum_{i=0}^{\infty} \lambda^i(x + y) t^i \\ &= \sum_{i=0}^{\infty} t^i \sum_{k=0}^{i} \lambda^k(x) \lambda^{i-k}(y) \\ &= \lambda_t(x) \lambda_t(y). \end{aligned}$$

Conversely, let $\lambda_t : K \to 1 + tK[[t]]$ be a homomorphism such that

$$\lambda_t(x) := a_0(x) + a_1(x)t + a_2(x)t^2 + \cdots,$$

where $a_0(x) = 1$ and $a_1(x) = x$. For two elements $x, y \in K$, one can see that

$$\begin{aligned}
\lambda_t(x)\lambda_t(y) &= \sum_{i=0}^{\infty} a_i(x)t^i \sum_{i=0}^{\infty} a_i(y)t^i \\
&= \sum_{i=0}^{\infty}\sum_{k=0}^{i} a_k(x)t^k a_{i-k}(y)t^{k-i} \\
&= \sum_{i=0}^{\infty} t^i \sum_{k=0}^{i} a_k(x)a_{i-k}(y),
\end{aligned}$$

From this, one sees that a_i is precisly a λ-operation.

(22) After one notes that $s^i = a^i t^i +$ higher terms, one can iteratively construct b_i by taking the inverse of a^i and multiplying by the appropriate coefficient to cancel out terms. More precisly, if $s = at + a_2t^2 + \ldots$, set $b_0 = 0$, $b_1 = a^{-1}$, $b_2 = -(b_1 a_2 a^{-2})$ and so on. Therefore, we have

$$t^n = \sum_i s^i \sum_{\sum r_k = i} b_{r_1} \cdots b_{r_n}.$$

Hence, every $f(t) \in K[[t]]$ can be written as $h(s) \in K[[s]]$.

(23) (a)

$$\begin{aligned}
\sum \gamma^n(x+y)t^n &= \gamma_t(x+y) \\
&= \lambda_s(x+y) \\
&= \lambda_s(x)\lambda_s(y) \\
&= \gamma_t(x)\gamma_t(y) \\
&= \sum t^n \sum_{k=0}^{n} \gamma^k(x)\gamma^{n-k}(y)
\end{aligned}$$

(b)

$$\begin{aligned}
\gamma_t(1) &= \lambda_s(1) \\
&= 1 + s \\
&= 1/(1-t)
\end{aligned}$$

(c)

$$\begin{aligned}
\gamma_t(-1) &= \gamma_t(1 + (-1))/\gamma_t(1) \\
&= 1/(1/(1-t)) \\
&= 1 - t
\end{aligned}$$

(24) (a)

$$\begin{aligned}
\gamma_t(u-1) &= \gamma_t(u)\gamma_t(-1) \\
&= (1 + us)(1-t) \\
&= 1 + t(u-1)
\end{aligned}$$

(b)

$$\begin{aligned}
\gamma_t(1-u) &= \frac{\gamma_t((1-u) + (u-1))}{1 - t(1-u)} \\
&= \frac{1}{1 - t(1-u)} \\
&= \sum_{i=0}^{\infty} (1-u)^i t^i
\end{aligned}$$

(25) (a)

$$\begin{aligned} t &= (e^t - 1)\sum_{i=0}^{\infty} B_k \frac{t^k}{k!} \\ &= \sum_{k=1}^{\infty} \frac{t^k}{k!} \sum_{k=0}^{\infty} \frac{t^k}{k!} \\ &= \sum_{k=1}^{\infty} t^k \sum_{i=0}^{k-1} \frac{B_i}{i!(k-i)!} \end{aligned}$$

From the above, one gets

$$\begin{aligned} 1 &= B_0 \\ 0 &= 1/2 + B_1 \\ 0 &= 1/6 - 1/4 + B_2/2 \end{aligned}$$

(b)

$$\begin{aligned} F(-t) &= \frac{-t}{e^{-t} - 1} \\ &= \frac{te^t}{e^t - 1} \\ &= t + F(t) \end{aligned}$$

Then we have $t = F(t) - F(-t) = t + 2\sum \frac{B_k t^k}{k!}$ where the sum is over k odd > 1. Hence $B_k = 0$ for all k odd > 1.

(26) (a) Doing similar rearrangement of terms as in part (a) of problem 25, we get the following three equations

$$\begin{aligned} 1 &= \mathbf{B}_0(X) \\ X &= \frac{1}{2} + \mathbf{B}_1(X) \\ \frac{X^2}{2} &= \frac{1}{6} + \frac{X - \frac{1}{2}}{2} + \frac{1}{2}\mathbf{B}_2(X) \end{aligned}$$

(b)

$$\begin{aligned} \frac{Nte^{Xt}}{e^t - 1} &= \frac{(Nt)e^{Nt\frac{X}{N}}}{e^t - 1} \\ &= (Nt)e^{Nt\frac{X}{N}} \frac{\sum_{a=0}^{N-1} e^{at}}{e^{Nt} - 1} \\ &= \frac{(Nt)\sum_{a=0}^{N-1} e^{Nt(\frac{X}{N} + \frac{a}{N})}}{e^{Nt} - 1} \end{aligned}$$

From the above one can directly deduce that $NB_k(x) = N^k \sum_{a=0}^{N-1} B_k\left(\frac{X+a}{N}\right)$.

(c) As in part (a), one can derive the equations

$$\frac{X^k}{k!} = G(X) + \frac{\mathbf{B}_{k-1}}{2!(k-1)!} + \frac{\mathbf{B}_k(X)}{k!},$$

where $\deg G < k - 1$. Multiplying both sides by $k!$ and rearranging terms, one immediatley sees that $\mathbf{B}_k(X) = X^k - \frac{k}{2}\mathbf{B}_{k-1}(X) - G(X)$.

(d)

$$\begin{aligned} F(t, X+1) - F(t, X) &= \frac{te^{tX+t} - te^{tX}}{e^t - 1} \\ &= \frac{te^{tX+t}(e^t - 1)}{e^t - 1} \\ &= te^{tX} \\ &= \sum_{i=1}^{\infty} kX^{k-1} \frac{t^k}{k!} \end{aligned}$$

(e) Immediately follows from last line.

(27) (a)

$$\begin{aligned} F_f(t, X+k) &= \sum_{a=0}^{N-1} f(a) \frac{te^{(a+X+k)t}}{e^{Nt} - 1} \\ &= \sum_{a=0}^{N-1} f(a) \frac{te^{(a+X)t} e^{kt}}{e^{Nt} - 1} \\ &= e^{kt} \sum_{a=0}^{N-1} f(a) \frac{te^{(a+X)t}}{e^{Nt} - 1} \\ &= e^{kt} F_f(t, X+k) \end{aligned}$$

(b) Immediately follows from (a).

(c) By (b), one has

$$F_f(t, X+N) - F_f(t, X) = \sum_{a=0}^{N-1} f(a) te^{(a+X)t}.$$

Hence $\frac{\mathbf{B}_{k,f}(X+N) - \mathbf{B}_{k,f}(X)}{k!} = \sum_{a=0}^{N-1} f(a) \dfrac{(a+X)^{k-1}}{(k-1)!}$.

(d) By part (a), we have

$$F_f(t, X) = e^{tX} F_f(t, 0) = \left(\sum_{k=0}^{\infty} \frac{X^k t^k}{k!} \right) \left(\sum_{k=0}^{\infty} B_{k,f} \frac{t^k}{k!} \right).$$

Multiplying the two series gives

$$F_f(t, X) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} \binom{k}{j} B_{j,f} X^{k-j} \right) \frac{t^k}{k!}.$$

Comparing the coefficients of $t^k/k!$, we obtain

$$\mathbf{B}_{k,f}(X) = \sum_{i=0}^{k} \binom{k}{i} B_{i,f} X^{k-i},$$

as required.