Seminar on Hilbert's Tenth Problem
Homework, due December 16 - model solution

1a) We write $\overrightarrow{a} = a_1, \ldots, a_k$, $\overrightarrow{x} = x_1, \ldots, x_n$ and $\overrightarrow{y} = y_1, \ldots, y_m$. Here m and n are natural numbers. Let S and T have the Diophantine representations

$$(\overrightarrow{a}) \in S \Leftrightarrow \exists \overrightarrow{x} \in R \ \left(D_1\left(\overrightarrow{a}, \overrightarrow{x}\right) = 0\right);$$
$$(\overrightarrow{a}) \in T \Leftrightarrow \exists \overrightarrow{y} \in R \ \left(D_2\left(\overrightarrow{a}, \overrightarrow{y}\right) = 0\right).$$

Now we can define $S \cup T$ by:

$$(\overrightarrow{a}) \in S \cup T \Leftrightarrow \exists \overrightarrow{x}, \overrightarrow{y} \in R \ \left(D_1\left(\overrightarrow{a}, \overrightarrow{x}\right) \cdot D_2\left(\overrightarrow{a}, \overrightarrow{y}\right) = 0\right).$$

We'll show that this definition works. Suppose that $(\overrightarrow{a}) \in S \cup T$. Then $(\overrightarrow{a}) \in S$ or $(\overrightarrow{a}) \in T$. If $(\overrightarrow{a}) \in S$, then there exist $\overrightarrow{x} \in R$ such that $D_1\left(\overrightarrow{a}, \overrightarrow{x}\right) = 0$. So there also exist $\overrightarrow{x}, \overrightarrow{y} \in R$ such that $D_1\left(\overrightarrow{a}, \overrightarrow{x}\right) \cdot D_2\left(\overrightarrow{a}, \overrightarrow{y}\right) = 0$, for example by taking $y_i = 0$ for $1 \leq i \leq m$. The case where $(\overrightarrow{a}) \in T$ is similar.

Now suppose that there exist $\overrightarrow{x}, \overrightarrow{y} \in R$ such that $D_1\left(\overrightarrow{a}, \overrightarrow{x}\right) \cdot D_2\left(\overrightarrow{a}, \overrightarrow{y}\right) = 0$. Since R is a domain, it has no zero divisors, so $D_1\left(\overrightarrow{a}, \overrightarrow{x}\right) = 0$ or $D_2\left(\overrightarrow{a}, \overrightarrow{y}\right) = 0$. This means that $(\overrightarrow{a}) \in S$ or $(\overrightarrow{a}) \in T$, so $(\overrightarrow{a}) \in S \cup T$. □

1b) *Note: since the exercise refers to the fraction field of R, it is implicitly implied that R is again an integral domain. I should have mentioned it in the exercise, but it apparently I failed to do so.*

We use the same notation as in the previous exercise. Let $P = \sum_{i=0}^{d} a_i x^i$ be a polynomial that has no roots in the fraction field of R. Here d is a positive integer and $a_d \neq 0$. We can define $S \cap T$ by

$$(\overrightarrow{a}) \in S \cap T \Leftrightarrow \exists \overrightarrow{x}, \overrightarrow{y} \in R \ \left(\sum_{i=0}^{d} a_i \cdot D_1^{d-i}\left(\overrightarrow{a}, \overrightarrow{x}\right) \cdot D_2^{i}\left(\overrightarrow{a}, \overrightarrow{y}\right) = 0\right).$$

Again, we show that this definition is adequate. Suppose $(\overrightarrow{a}) \in S \cap T$, then $(\overrightarrow{a}) \in S$ and $(\overrightarrow{a}) \in T$. So there exist $\overrightarrow{x} \in R$ and $\overrightarrow{y} \in R$ such that $D_1\left(\overrightarrow{a}, \overrightarrow{x}\right) = 0$ and $D_2\left(\overrightarrow{a}, \overrightarrow{y}\right) = 0$. So the right-hand side of the definition clearly holds.

Now suppose there exist $\overrightarrow{x}, \overrightarrow{y} \in R$ such that the right-hand side holds. Assume that $D_1\left(\overrightarrow{a}, \overrightarrow{x}\right) \neq 0$. Then we have

$$\begin{aligned} 0 &= \sum_{i=0}^{d} a_i \cdot D_1^{d-i}\left(\overrightarrow{a}, \overrightarrow{x}\right) \cdot D_2^{i}\left(\overrightarrow{a}, \overrightarrow{y}\right) \\ &= D_1^{d}\left(\overrightarrow{a}, \overrightarrow{x}\right) \cdot \sum_{i=0}^{d} a_i \cdot \left(\frac{D_2\left(\overrightarrow{a}, \overrightarrow{y}\right)}{D_1\left(\overrightarrow{a}, \overrightarrow{x}\right)}\right)^i = D_1^{d}\left(\overrightarrow{a}, \overrightarrow{x}\right) \cdot P\left(\frac{D_2\left(\overrightarrow{a}, \overrightarrow{y}\right)}{D_1\left(\overrightarrow{a}, \overrightarrow{x}\right)}\right). \end{aligned}$$

Since $D_1(\overrightarrow{a}, \overrightarrow{x})$ is non-zero, we must have $P\left(\frac{D_2(\overrightarrow{a},\overrightarrow{y})}{D_1(\overrightarrow{a},\overrightarrow{x})}\right) = 0$. But then we have found a root of P in the fraction field of R: contradiction. So we must have $D_1(\overrightarrow{a}, \overrightarrow{x}) = 0$. Now we get $a_d \cdot D_2^d(\overrightarrow{a}, \overrightarrow{y}) = 0$. Since $a_d \neq 0$, we get $D_2(\overrightarrow{a}, \overrightarrow{y}) = 0$. Now it follows that $(\overrightarrow{a}) \in S$ and $(\overrightarrow{a}) \in T$, so $(\overrightarrow{a}) \in S \cap T$. $\square$

2a) By the binomial theorem and taking even terms and odd terms together, we get

$$X_a(Z) + Y_a(Z)\sqrt{Z^2-1} = \left(Z + \sqrt{Z^2-1}\right)^a = \sum_{i=0}^{a} \binom{a}{i} Z^{a-i}\left(Z^2-1\right)^{\frac{i}{2}}$$
$$= \sum_{i=0}^{\lfloor \frac{a}{2} \rfloor} \binom{a}{2i} Z^{a-2i}\left(Z^2-1\right)^i + \sqrt{Z^2-1}\sum_{i=0}^{\lfloor \frac{a-1}{2} \rfloor} \binom{a}{2i+1} Z^{a-2i-1}\left(Z^2-1\right)^i.$$

So $X_a(Z) = \sum_{i=0}^{\lfloor \frac{a}{2} \rfloor} \binom{a}{2i} Z^{a-2i}\left(Z^2-1\right)^i$. In the i-th term, the highest exponent of Z is $(a-2i)+2i = a$ and the coefficient of Z^a, that is $\binom{a}{2i}$, is positive, so it follows that $\deg X_a = a$.

For the second part, we use a similar calculation to get

$$X_{-a}(Z) + Y_{-a}(Z)\sqrt{Z^2-1} = \left(Z + \sqrt{Z^2-1}\right)^{-a} = \left(Z - \sqrt{Z^2-1}\right)^a$$
$$= \sum_{i=0}^{\lfloor \frac{a}{2} \rfloor} \binom{a}{2i} Z^{a-2i}\left(Z^2-1\right)^i - \sqrt{Z^2-1}\sum_{i=0}^{\lfloor \frac{a-1}{2} \rfloor} \binom{a}{2i+1} Z^{a-2i-1}\left(Z^2-1\right)^i.$$

Now it immediately follows that $X_a = X_{-a}$. $\square$

2b) Since $\mathbb{F}_q[Z]$ is of characteristic p, we have

$$X_{ap^b}(Z) + Y_{ap^b}(Z)\sqrt{Z^2-1} = \left(Z + \sqrt{Z^2-1}\right)^{ap^b} = \left(\left(Z + \sqrt{Z^2-1}\right)^a\right)^{p^b}$$
$$= \left(X_a(Z) + Y_a(Z)\sqrt{Z^2-1}\right)^{p^b} = X_a^{p^b}(Z) + Y_a^{p^b}(Z)\left(Z^2-1\right)^{\frac{p^b}{2}}$$
$$= X_a^{p^b}(Z) + \left(Y_a^{p^b}(Z)\left(Z^2-1\right)^{\frac{p^b-1}{2}}\right) \cdot \sqrt{Z^2-1}.$$

Since p is odd, $\frac{p^b-1}{2}$ is an integer, so it follows that $X_{ap^b} = (X_a)^{p^b}$. $\square$

2c) Note that $X_1(Z) = Z$. So we have $X_m(B) = X_{p^k}(B) = (X_1(B))^{p^k} = B^{p^k} = A$ and $X_n(B+1) = X_{p^k}(B+1) = (X_1(B+1))^{p^k} = (B+1)^{p^k} = B^{p^k} + 1^{p^k} = A+1$. $\square$

2d) Suppose m is negative. Then we have $X_m = X_{-m}$, so we can replace m by the positive number $-m$. Therefore, we may assume that $m \in \mathbb{N}$. The same holds for n. Now we have $X_n(B+1) = A+1 = X_m(B)+1$. Since $m, n \in \mathbb{N}$, we know that $\deg X_m = m$ and $\deg X_n = n$. Putting $d = \deg B$, comparing degrees gives: $dn = dm$. Since B is non-constant, we have $d > 0$, so it follows that $m = n$. Now we get $X_n(B+1) = X_n(B)+1$. $\square$

2e) We have

$$\begin{aligned}(X_c(B+1))^{p^k} &= X_{cp^k}(B+1) = X_n(B+1) = X_n(B)+1 = X_{cp^k}(B)+1 \\ &= (X_c(B))^{p^k} + 1^{p^k} = (X_c(B)+1)^{p^k}.\end{aligned}$$

Since $\mathbb{F}_q[Z]$ is an integral domain of characteristic p, the map $x \mapsto x^p$ is injective. So its k-th iteration, i.e. the map $x \mapsto x^{p^k}$, must also be injective. Hence it follows that $X_c(B+1) = X_c(B)+1$. $\square$

2f) We write $X_c(Z) = \alpha Z^c + \beta Z^{c-1} + \ldots$ with $\alpha, \beta \in \mathbb{F}_q$. Here the dots are the terms of smaller degree in Z. We know that $\deg X_c = c$, so α must be non-zero. We will now expand the expressions $X_c(B+1)$ and $X_c(B)+1$. In what follows, dots are terms of smaller degree in B (that is, smaller than $c-1$).

We have $\alpha(B+1)^c = \alpha B^c + \alpha c B^{c-1} + \ldots$ and $\beta(B+1)^{c-1} = \beta B^{c-1} + \ldots$, so

$$X_c(B+1) = \alpha B^c + (\alpha c + \beta) B^{c-1} + \ldots \tag{1}$$

Since $c \geq 2$, we have $c-1 > 0$, so the degree of 1 as an exponent of B is smaller than $c-1$. We get

$$X_c(B)+1 = \alpha B^c + \beta B^{c-1} + \ldots \tag{2}$$

Expanding the terms on the dots will give us an expression with degree in Z at most $(c-2)d$. Since $d > 0$, we have $(c-1)d > (c-2)d$. So the coefficients of $Z^{(c-1)d}$ in (1) and (2) can only be equal if $\alpha c + \beta = \beta$. So we must have $\alpha c = 0$ and since α was non-zero, we get $c = 0$ in $\mathbb{F}_q$. But this means that $p \mid c$: contradiction!

Since $p \nmid c$, it follows that $c = 1$. Now we get $m = n = p^k$, so $A = X_m(B) = X_{p^k}(B) = B^{p^k}$. This completes the proof of the other direction. $\square$

3) We write $Z^n - 1 = \prod_{k=0}^{n-1}\left(X - \zeta_n^k\right)$, where ζ_n is an n-th primitive root of unity. Consider a k with $0 \leq k < n$. We define $c = \gcd(k, n)$ and $d = \frac{n}{c}$. It is well-known that ζ_n^c is a primitive d-th root of unity. Since $c \mid k$, we can write $k = ac$ for some integer a. Then $\zeta_n^k = \zeta_n^{ac} = (\zeta_n^c)^a$, so ζ_n^k is also a d-th root of unity. Moreover, since $c = \gcd(k, m)$, we have

$\gcd\left(\frac{k}{c}, \frac{n}{c}\right) = 1$, that is: $\gcd(a, d) = 1$. So ζ_n^k is even a primitive d-th root of unity. Now it follows that $X - \zeta_n^k \mid \Phi_d(Z)$. Since d clearly divides n, we get $X - \zeta_n^k \mid \prod_{d|n} \Phi_d(Z)$.

Since all the factors $X - \zeta_n^k$, with $0 \leq k < n$ are pairwise coprime, we obtain

$$\prod_{k=0}^{n-1} \left(X - \zeta_n^k\right) \mid \prod_{d|n} \Phi_d(Z),$$

that is:

$$Z^n - 1 \mid \prod_{d|n} \Phi_d(Z).$$

By the well-known identity $n = \sum_{d|n} \phi(d)$, the degrees of both polynomials are equal. Moreover, both polynomials are clearly monic, so the equality follows. □

Marking scheme

1a) 2 pt: 1 pt for the right definition, 1 pt for proving that it works.
1b) 3 pt: 2 pt for the right definition, 1 pt for proving that it works.
2a) 2 pt: 1 pt for each result.
2b) 1 pt.
2c) 1 pt.
2d) 1 pt.
2e) 2 pt.
2f) 3 pt: 2 pt for obtaining the contradiction, 1 pt. for completing the proof.
3) 5 pt: 1 pt. for introducing a primitive n-th root of unity, 2 pt. for proving that $X - \zeta_n^k \mid \prod_{d|n} \Phi_d(Z)$, 2 pt for completing the proof. Of course, there are different ways of solving this exercise.

Grade = (number of points)/2.