PMTH332 Assignment 6

Jayden Turner (SN 220188234)

5 October 2018

Question 1

Take $n \in \mathbb{Z}$. If $3 \mid n$, then $n^{33} \equiv n \mod 3 \implies 3|n^{33} - n$. If $3 \nmid n$, then

$$\begin{aligned} n^{33} - n = n(n^{32} - 1) = n((n^2)^{16} - n) = n((n^{\phi(3)})^{16} - n) &\equiv n(1-1) \mod 3 \\ &\equiv 0 \mod 3 \end{aligned} \tag{1}$$

where $\phi(n)$ is the Euler phi function, and (1) holds by Euler's theorem. Thus $3|n^{33} - n$ for all integer n. Similiarly, if $5 \mid n$, then $n^{33} \equiv n \mod 5 \implies 5|n^{33} - n$. Otherwise,

$$\begin{aligned} n^{33} - n = n(n^{32} - 1) = n((n^4)^8 - 1) = n((n^{\phi(n)})^8 - 1) &\equiv n(1-1) \mod 5 \\ &\equiv 0 \mod 5 \end{aligned} \tag{2}$$

where (2) holds by Euler's theorem, and hence $5|n^{33} - n$ for all integer n. Therefore, as both 3 and 5 divide $n^{33} - n$, and $\gcd(3,5) = 1$, it must hold that $3 \cdot 5 = 15|n^{33} - n$ as required.

Question 2

Given a field F, the ring of polynomials over F, $F[x]$ is an integral domain. define $d : F[x] \to \mathbb{N}$ as

$$d(\alpha) := \begin{cases} 0, & \alpha = 0 \\ 2^{\deg(\alpha)}, & \alpha \neq 0 \end{cases} \tag{3}$$

By definition, $d(\alpha) = 0$ if and only if $\alpha = 0$. Further, $d(1) = 2^0 = 1$, and as $\deg(\alpha) \geq 0$, $d(\alpha\beta) = 2^{\deg(\alpha)}2^{\deg(\beta)} \geq 2^{\deg(\alpha)} = d(\alpha)$, given $\beta \neq 0$. Thus d satisfies the first two axioms of a Euclidean function. To see that it satisfies the third, take $\alpha, \beta \in F[x]$ such that $n = \deg(\alpha) \geq \deg(\beta) = m$. Then define $q, r \in F[x]$ as

$$q := \frac{a_n}{b_m} x^{n-m}$$

and

$$r := \alpha - q\beta$$

Clearly $\alpha = q\beta + r$. Expanding r we see that

$$\begin{aligned} r &= a_n x^n + a_{n-1}x^{n-1} + ... + a_0 - \frac{a_n}{b_m} b_m x^n - ... - \frac{a_n}{b_m} b_0 x^{n-m} \\ &= \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1}\right) x^{n-1} + ... + \left(a_{n-m} - \frac{a_n}{b_m} b_0\right) x^{n-m} + ... \end{aligned}$$

which shows that $\deg(r) \leq n - 1 < \deg(\beta)$, and hence d is a Euclidean function. Thus $F[x]$ is a Euclidean domain, which is a principal ideal domain, by Theorem 17.3. Therefore, given any ideal I in $F[x]$, $I = (\alpha)$ for some $\alpha in F[x]$. If I is a prime ideal, then α is prime in $F[x]$. But by Theorem 17.14, if α is prime, then $(\alpha) = I$ is maximal. Therefore, all proper prime ideals of $F[x]$ are maximal.

Question 3

Question 4

Question 5