HOMEWORK #8 – MATH 435

SOLUTIONS

Chapter 4, Section 5: #1 If F is a field, show that the only invertible elements in $F[x]$ are the non-zero elements of F.

Solution: Certainly the elements of F are invertible. Conversely, suppose that $g \in F[x]$ is invertible but is not in F. Thus $\deg g \geq 1$. Suppose $gh = 1$, then since $(\deg g)+(\deg h) = \deg 1 = 0$, we have that $\deg h \leq -1$, which is impossible.

Chapter 4, Section 5: #5 In problem # 3, let $I = \{af + bg \mid f, g \in \mathbb{Q}[x]\}$. Find d such that $I = \langle d \rangle$.

Solution: Setting $d = \gcd(a, b)$ will work.

(a) $x^3 - 6x + 7$ and $x + 4$. The only way they have a non-zero gcd is if -4 is a root of both polynomials. But $(-4)^3 - 6(-4) + 7 = -64 + 24 + 7 \neq 0$. Thus we can take $d = 1$.

(b) $x^2 - 1$ and $2x^7 - 4x^5 + 2$. The only way they can have a non-zero gcd is if either of ± 1 is a root of the second polynomial. Now $2(1)^7 - 4(1)^5 + 2 = 0$ but $2(-1)^7 - 4(-1)^5 + 2 = -2 + 4 + 2 \neq 0$. Thus $d = x - (1)$ will work.

(c) $3x^2 + 1$ and $x^6 + x^4 + x + 1$. The polynomial on the left is irreducible since it doesn't have any roots in $\mathbb{Q}$. By reduction mod 3, the polynomial on the right is also irreducible since $1^6 + 1^4 + 1 + 1 = 1 \mod 3$ and $2^6 + 2^4 + 2 + 1 = 64 + 16 + 2 + 1 = 83 = 2 \mod 3$. Thus they have no terms in common.

(d) $x^3 - 1$ and $x^7 - x^4 + x^3 - 1$. The left term factors as $x^3 - 1 = (x - 1)(x^2 + x + 1)$ and the second term is irreducible. We note immediately that 1 is a root of $b = x^7 - x^4 + x^3 - 1$ and so the only question is whether $x^2 + x + 1$ also divides b. By doing polynomial long division we see that this is indeed the case. $x^7 - x^4 + x^3 - 1 = (x^3 - 1)(x^4 + 1)$ and so the gcd is $x^3 - 1$.

Chapter 4, Section 10: #35 Show that the following polynomials are irreducible over the field F indicated.

Solution:

(a) $x^2 + 7$ over $F = \mathbb{R}$. It is degree 2 and has no roots.

(b) $x^3 - 3x + 3$ over $F = \mathbb{Q}$. Use Eisenstein.

(c) $x^2 + x + 1$ over $F = \mathbb{Z}_{\text{mod}2}$. It is degree 2 and has no roots.

(d) $x^2 + 1$ over $F = \mathbb{Z}_{\text{mod}19}$. One can check all potential roots and see that there are none. Or one can use basic facts about when -1 has a square root.

(e) $x^3 - 9$ over $F = \mathbb{Z}_{\text{mod}13}$. Again, brute force will do the trick.

(f) $x^4 + 2x^2 + 2$ over $F = \mathbb{Q}$. Use Eisenstein.

Chapter 4, Section 1: #12 If $F \subseteq K$ are two fields and $f, g \in F[x]$ are relatively prime, show they are relatively prime in $K[x]$.

Solution: There exists $s, t \in F[x] \subseteq K[x]$ such that $sf + tg = 1$ since f, g are relatively prime in F. But s, t also have coefficients in K, so f and g are relatively prime in $K[x]$ as well.

Chapter 4, Section 1: #13

Solution: Show that $\mathbb{R}[x]/\langle x^2+1\rangle \simeq \mathbb{C}$. We have a surjective homomorphism $\phi : \mathbb{R}[x] \to \mathbb{C}$ which sends x to i (and sends $f(x)$ to $f(i)$). Note that x^2+1 is in the kernel $K = \langle d\rangle$, which is principal since $\mathbb{R}[x]$ is a PID. Thus d divides x^2+1 so it is either equal to it, or equal to 1. $d = 1$ would imply that ϕ is the zero map as everything would be in the kernel, but this is not the case. Thus $d = x^2+1$ and the proof is complete.

Chapter 4, Section 1: #15 Let $F = \mathbb{Z}_{\text{mod}p}$ be a field where p is prime. Suppose that $q \in F[x]$ is irreducible of degree n. Prove that $F[x]/\langle q\rangle$ is a field with at most p^n elements.

Solution: Set $J = \langle q\rangle$. Consider $a + J \in F[x]/J$. We can write $a = qd + r$ for some $d \in F[x]$ and r with $0 \leq \deg r < \deg q$. Thus $a + J = qd + r + J = r + J$. In particular, every element of $F[x]/J$ can be expressed as

$$(a_{n-1}x^{n-1} + \cdots + a_1x^1 + a_0) + J$$

for some $a_i \in F$. But there are only q^n possible choices. This completes the proof.

Chapter 4, Section 1: #25 If p is prime, show that $x^{p-1} + \cdots + x + 1$ is irreducible in $\mathbb{Q}[x]$.

Solution: Now, $(x^p - 1)/(x - 1) = x^{p-1} + \cdots + x + 1$. Thus

$$\begin{aligned}
& (x+1)^{p-1} + \cdots + (x+1) + 1 \\
= \; & ((x+1)^p - 1)/(x+1-1) \\
= \; & (x^p + \tbinom{p}{1}x^{p-1} + \cdots + \tbinom{p}{p-1}x^1 + 1 - 1)/x \\
= \; & x^{p-1} + \tbinom{p}{1}x^{p-2} + \cdots + \tbinom{p}{p-2}x^1 + p
\end{aligned}$$

But this is irreducible by Eisenstein's criterion and so the proof is complete.