HOMEWORK #9 – MATH 435

SOLUTIONS

Chapter 4, Section 6: #2 Prove that $f(x) = x^3 + 3x + 2$ is irreducible in $\mathbb{Q}[x]$.

Solution: By Gauss' Lemma, it is sufficient to show that this is irreducible in $\mathbb{Z}[x]$. Now, note that $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible. But $f(x+1) = (x+1)^3 + 3(x+1) + 2 = x^3 + 3x^2 + 6x + 6$. But this is irreducible by Eisenstein's criterion.

Chapter 4, Section 6: #3 Show that there are infinitely many integers a such that $x^7 + 15x^2 - 30x + a$ is irreducible.

Solution: Set $a = 5p$ where p is any prime $\neq 5$. There are infinitely many such a, and the polynomial is irreducible for all such a by Eisenstein's criterions.

Chapter 4, Section 6: #11 Let φ be an automorphism of $F[x]$ such that $\varphi(a) = a$ for all $a \in F \subseteq F[x]$. Prove that there exists $0 \neq b, c \in F$ such that $\varphi(f(x)) = f(bx + c)$ for every $f(x) \in F[x]$.

Solution: Let $g(x) = \varphi(x)$. Then it is easy to see that $\varphi(f(x)) = f(g(x))$ for all $f(x) \in F[x]$. Indeed, this follows immediately from the fact that φ is a ring homomorphism.

Suppose now that $\deg g(x) \geq 2$, then $\deg \varphi(f(x)) = \deg(f(g(x))) = (\deg f)(\deg g)$. Thus $\deg(f(g(x))) \neq 1$ no matter what f I pick. It follows that φ is not surjective because there is no $f(x)$ such that $\varphi(f(x)) = x$, since the latter side has degree 1. But then φ is not an isomorphism either.

Finally suppose that $\deg g(x) = 0$. But then $\deg \varphi(f(x)) = \deg(f(g(x))) = 0$ for all $f \in F[x]$. But again, this implies that φ is not surjective and not an automorphism.

Thus $\deg g(x) = 1$ by process of elimination. Therefore $g(x) = bx + c$ where $b \neq 0$ and $b, c \in F$. Thus $\varphi(f(x)) = f(bx + c)$ as desired.

Chapter 5, Section 1: #9(b) Let F be a field of characteristic $p > 0$ and let $\varphi : F \to F$ be defined by $\varphi(a) = a^p$. In part (a), it was shown that φ is an injective ring homomorphism from F to itself. Now we have to give an example of a field F such that φ is not surjective.

Solution: Let $R = \mathbb{Z}_{\text{mod}p}[x]$ and suppose that F is the field of fractions of R as in Chapter 4, Section 7. In other words $F = \{f/g \mid f, g \in R, g \neq 0\}$. We notice that $\varphi(\lambda) = \lambda$ for every $\lambda \in \mathbb{Z}_{\text{mod}p}$ by Fermat's little theorem.

It follows that that $\varphi(f(x)/g(x)) = f(x^p)/g(x^p)$ since φ is a ring homomorphism. In particular, every element has only pth powers of x in it. But then the function $x/1 \in F$ is not of this form, and can't be written in the form $f(x^p)/g(x^p)$. Therefore φ is not surjective.

Chapter 5, Section 1: #10 If F is a finite field, show that φ from 9. is surjective.

Solution: $\varphi : F \to F$ is an injective map between two sets of the same size (actually, the sets are the same, but this doesn't matter). Therefore φ is bijective and so surjective as well.

Chapter 5, Section 2: #3 If V is a vector space of dimension n over $\mathbb{Z}_{\text{mod}p}$, then show that $|V| = p^n$.

Solution: Fix a basis $v_1, \ldots, v_n$ for V over $\mathbb{Z}_{\text{mod}p}$. Every element w in V can be written uniquely as a linear combination:

$$w = a_1 v_1 + \cdots + a_n v_n$$

for some $a_i \in V$. In particular, there are p choices for a_1, p choices for a_2, etc. There are thus p^n choices in all. This completes the proof.

Chapter 5, Section 2: #6(a) Suppose that $W \subseteq V$ are vector spaces over F with V finite dimensional. Prove that $\dim_F(W) \leq \dim_F(V)$.

Solution: Suppose not, then there exists a linearly independent set $w_1, \ldots, w_k$ in W with $k > \dim_F(V)$. But $w_i \in W \subseteq V$, and so the w_i are in V as well, where they are also linearly independent. This is a contradiction to Theorem 5.2.6 from the text.

Chapter 5, Section 3: #1(a) Show that $\sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

Solution: Set $a = \sqrt{2} + \sqrt{3}$. Then

$$a^4 = \sqrt{2}^4 + 4\sqrt{2}^3\sqrt{3} + 6\sqrt{2}^2\sqrt{3}^2 + 4\sqrt{2}\sqrt{3}^3 + \sqrt{3}^4 = 4 + 8\sqrt{6} + 36 + 12\sqrt{6} + 9 = 49 + 20\sqrt{6}$$

and

$$a^2 = \sqrt{2}^2 + 2\sqrt{2}\sqrt{3} + \sqrt{3}^2 = 5 + 2\sqrt{6}.$$

It follows that

$$a^4 - 10a^2 = 49 + 20\sqrt{6} - 50 - 20\sqrt{6} = -1$$

and so a is a root of $f(x) = x^4 - 10x^2 + 1$ which proves that a is algebraic over $\mathbb{Q}$.

Chapter 5, Section 3: #7 If $F \subseteq K$ is a field extension and $a \in K$ is such that a^2 is algebraic over F, then a is also algebraic over F.

Solution: Suppose that $f(x)$ is non-zero polynomial in $F[x]$ such that $f(a^2) = 0$, such an f exists because a^2 is algebraic. Set $g(x) = f(x^2)$. Then $g(a) = f(a^2) = 0$ and this completes the proof.