HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 13

4.5, Q10. (a) It is tempting here to start discussing roots of polynomials, but this idea is currently beyond the scope of the course. However, if x^2+7 were not irreducible over $\mathbb{R}$, then we would have $x^2+7=(x+a)(x+b)$ for some $a,b\in\mathbb{R}$. Thus $x^2+(a+b)x+ab=x^2+7$, which shows that $a+b=0$ and $ab=7$, whence $a^2=b^2=-7$. However, for all $a\in\mathbb{R}$, we have $a^2\geq 0$, so this leads to a contradiction. Hence x^2+7 is irreducible over $\mathbb{R}$.
(b) The polynomial $x^3-3x+3\in\mathbb{Z}[x]$ has lead coefficient not divisible by 3, all remaining coefficients divisible by 3, and constant coefficient not divisible by 3^2. Since 3 is prime, it therefore follows from Eisenstein's criterion that x^3-3x+3 is irreducible over $\mathbb{Z}$, and then Gauss' Lemma shows that this polynomial remains irreducible over $\mathbb{Q}$.
(c) If x^2+x+1 were not irreducible over $\mathbb{Z}_2$, then we would have $x^2+x+1\in(x-a)$ for some $a\in\mathbb{Z}_2$, whence $a^2+a+1=0$. But $a^2+a=0$, and so there is no such value of a, leading to a contradiction. Hence x^2+x+1 is irreducible over $\mathbb{Z}_2$.
(d) If x^2+1 were not reducible over $\mathbb{Z}_{19}$, then we would have $x^2+1\in(x-a)$ for some $a\in\mathbb{Z}_{19}$, whence $a^2+1=0$. But then $a\neq 0$, and it follows from Fermat's Little Theorem that one then has $1=a^{18}=(-1)^9=-1$, which is impossible. We therefore conclude that there is no such value of a, and hence x^2+1 is irreducible over $\mathbb{Z}_{19}$.
(e) If x^3-9 were not reducible over $\mathbb{Z}_{13}$, then we would have $x^3-9\in(x-a)$ for some $a\in\mathbb{Z}_{13}$, whence $a^3-9=0$. But then $a\neq 0$, and it follows from Fermat's Little Theorem that $1=a^{12}=9^4=4^4=256=-4$, which is impossible. We therefore conclude that there is no such value of a, and hence x^3-9 is irreducible over $\mathbb{Z}_{13}$.
(f) The polynomial $x^4+2x^2+2\in\mathbb{Z}[x]$ has lead coefficient not divisible by 2, all remaining coefficients divisible by 2, and constant coefficient not divisible by 2^2. Since 2 is prime, it therefore follows from Eisenstein's criterion that x^4+2x^2+2 is irreducible over $\mathbb{Z}$, and then Gauss' Lemma shows that this polynomial remains irreducible over $\mathbb{Q}$.

4.6, Q2. By Gauss' Lemma, the polynomial x^3+3x+2 is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$. The latter holds if and only if $(x+1)^3+3(x+1)+2=x^3+3x^2+6x+3$ is irreducible over $\mathbb{Z}[x]$. The latter polynomial has lead coefficient not divisible by 3, all remaining coefficients divisible by 3, and constant coefficient not divisible by 3^2. Since 3 is prime, it therefore follows from Eisenstein's criterion that x^3+3x^2+6x+3, and hence also x^3+3x+2, is irreducible in $\mathbb{Z}[x]$, and also in $\mathbb{Q}[x]$.

4.6, Q3. Take $a=3k$, where k is any integer with $(k,3)=1$. Then the polynomial $x^7+15x^2-30x+a$ has lead coefficient not divisible by 3, all remaining coefficients divisible by 3, and constant coefficient not divisible by 3^2. Since 3 is prime, it follows from Eisenstein's criterion that $x^7+15x^2-30x+a$ is irreducible in $\mathbb{Z}[x]$, and by Gauss' Lemma this polynomial is therefore also irreducible in $\mathbb{Q}[x]$. There are infinitely many such values of a, and this is what we were asked to establish.

4.6, Q6. Suppose that $f(x)$ is not irreducible in $F[x]$, but factors as $f(x)=u(x)v(x)$ with $u,v\in F[x]$ and $\deg(u)\geq\deg(v)\geq 1$, as we may suppose. Then since φ is a homomorphism, we have $g(x)=\varphi(f(x))=\varphi(u(x))\varphi(v(x))$. Notice that $\deg(\varphi(u(x)))\geq 1$, for otherwise we have $\varphi(u(x))\in F$, say $\varphi(u(x))=a\in F$, and then the bijective property of the automorphism φ ensures that $u(x)=\varphi^{-1}(a)=a\in F$, contradicting the hypothesis that $\deg(u(x))\geq 1$. Similarly, we have $\deg(\varphi(v(x)))\geq 1$, and thus $g(x)=\varphi(f(x))$ is not irreducible. On the other hand, if $g(x)$ is not irreducible in $F[x]$, then we may argue similarly using φ^{-1} in place of φ, deducing that $f(x) = \varphi^{-1}(g(x))$ is not irreducible. Then $f(x)$ is irreducible if and only if $g(x)$ is irreducible, as required.

4.6, Q10. Suppose that $\varphi : F[x] \to F[x]$ is an automorphism satisfying the property that $\varphi(a) = a$ for all $a \in F$. Then given a polynomial $f(x) = a_n x^n + \ldots + a_1 x + a_0$ with $a_i \in F$ for each i, it follows from the homomorphism properties of φ that we have $\varphi(f) = \varphi(a_n)\varphi(x)^n + \ldots + \varphi(a_1)\varphi(x) + \varphi(a_0) = a_n g(x)^n + \ldots + a_1 g(x) + a_0$, where we write $g(x) = \varphi(x) \in F[x]$. We may suppose without loss of generality that $a_n \neq 0$, and thus we deduce that $\deg(\varphi(f)) = \deg(g(x)) \cdot \deg(f)$. If $\deg(g(x)) \neq 1$, then there are no polynomials of degree 1 in $\varphi(F[x])$, and so φ cannot be an automorphism (it is not surjective). Then we have $\deg(g(x)) = 1$, whence $\deg(\varphi(f)) = \deg(f)$. Since this relation holds for all $f \in F[x]$, we have established the claimed property.

5.1, Q4. Suppose that D is an integral domain. Then D is a commutative ring with the property that, whenever $a, b \in D$ satisfy $ab = 0$, then either $a = 0$ or $b = 0$. It follows that the polynomial ring $E = D[x]$ is also an integral domain when endowed with polynomial addition and multiplication in the canonical manner. The fact that E is a commutative ring is inherited from the analogous property of D. Moroever, if $A, B \in E$ satisfy $AB = 0$, then $A = 0$ or $B = 0$. To see this, write $A(x) = a_n x^n + \ldots + a_0$ and $B(x) = b_m x^m + \ldots + b_0$, with $a_n \neq 0$ and $b_m \neq 0$. If $AB = 0$, then certainly the lead coefficient of AB is 0, so $a_n b_m = 0$. But D is an integral domain, so either $a_n = 0$ or $b_m = 0$, leading to a contradiction. Then, indeed, one finds that $E = D[x]$ is an integral domain. But $D[x, y] = E[y]$, and E is itself an integral domain. Then we have show that $E[y] = D[x, y]$ is also an integral domain.

5.1, Q7. By the binomial theorem, one has $(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \ldots + \binom{p}{p-1} a b^{p-1} + b^p$, in which the general term takes the shape $\binom{p}{r} a^{p-r} b^r$. Notice that when $1 \leq r \leq p - 1$,

$$\binom{p}{r} = \frac{p!}{r!(p-r)!} \equiv 0 \pmod{p},$$

and hence in a field F of characteristic $p \neq 0$, it follows that all of the terms with $1 \leq r \leq p - 1$ in the expansion vanish. Thus $(a + b)^p = a^p + b^p$.

5.1, Q8. When $n = 1$, one has $(a + b)^{p^n} = (a + b)^p = a^p + b^p$, as a consequence of Q7. We proceed by induction, supposing that $(a + b)^{p^r} = a^{p^r} + b^{p^r}$ for all $1 \leq r < n$. Then $(a+b)^{p^n} = ((a + b)^p)^{p^{n-1}} = (a^p + b^p)^{p^{n-1}} = (a^p)^{p^{n-1}} + (b^p)^{p^{n-1}} = a^{p^n} + b^{p^n}$. This confirms the inductive step, and so the desired conclusion follows by induction.

5.1, Q9. (a) Let $\varphi : F \to F$ be defined by $\varphi(a) = a^p$, where $p = \mathrm{char}(F)$. Then for all $a, b \in F$, one has $\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$, and $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$. So φ defines a homomorphism. Moreover, one has $\varphi(a) = \varphi(b)$ if and only if $a^p = b^p$, and this holds if and only if $0 = a^p - b^p = (a - b)^p$, and hence $a = b$. Thus φ is an injective homomorphism, and hence a monomorphism.

(b) Consider the field $F = \mathbb{Z}_p(x)$, the field of fractions of the polynomial ring $\mathbb{Z}_p[x]$ (also called $\mathbb{F}_p(x)$). We claim that there is no element $\alpha \in F$ having the property that $\alpha^p = x$. Suppose to the contrary that there exist $u, v \in \mathbb{Z}_p[x]$ with $v \neq 0$ and $(u/v)^p = x$. Then we have $u(x)^p = xv(x)^p$. But by applying the binomial theorem, we see that if $u(x) = u_0 + u_1 x + \ldots + u_n x^n$, then $u(x)^p = u_0^p + u_1^p x^p + \ldots + u_n^p x^{np} \in \mathbb{Z}_p[x^p]$, and likewise $v(x)^p \in \mathbb{Z}_p[x^p]$. Consequently, in the relation $u(x)^p = xv(x)^p$, all of the terms appearing on the left hand side with non-zero coefficients involve monomials x^m with $p|m$, while on the right hand side these terms involve monomials x^n with $n \equiv 1 \pmod{p}$. This yields a contradiction, and so there exists no $\alpha \in F$ with $\varphi(\alpha) = \alpha^p = x$, whence φ cannot be surjective from F into F, since $x \notin \varphi(F)$.

5.1, Q10. If F is a finite field, then it has characteristic p for some prime p. Considered as an additive group, it is then evident from Cauchy's theorem that since $pa = 0$ for all $a \in F$, then $|F| = p^n$ for some $n \in \mathbb{N}$. But then the multiplicative group $F^\times$ has order $p^n - 1$, and for each $a \in F^\times$ we have $a^{p^n-1} = 1$, so that $a^{p^n} = a$ for each $a \in F$. If φ were not surjective, then also φ^n cannot be surjective. But for each $a \in F$, one has $\varphi^n(a) = a^{p^n} = a$, so that φ^n is surjective. We conclude that φ must be surjective, and hence from Q9(a) we find that φ is a bijective homomorphism from F into F, so that φ is an automorphism.