MODEL ANSWERS TO HWK #11

1. By Gauss' Lemma, it suffices to prove that $x^3 - 3x + 2$ is irreducible over $\mathbb{Z}$. Suppose not. Then it must factor as

$$x^3 + 3x - 2 = (x + a)(x^2 + bx + c),$$

where a, b and c are all integers. It follows that $ac = 2$, so that a divides 2. In this case, either ± 1 or ± 2 would be a root of $x^3 - 3x + 2$. We compute

$$1^3+3-2 = 2, \quad (-1)^3-3-2 = -6, \quad 2^3+6-2 = 12, \quad (-2)^3-6-2 = -16.$$

So ± 1, ± 2 are not roots of $x^3 - 3x + 2$. Hence this polynomial is irreducible over $\mathbb{Q}$.

2. By Gauss' Lemma it suffices to prove that $f(x)$ is irreducible over the integers for infinitely many a. Let a be any integer which is divisible either by 3 and not by 9, or divisible by 5 and not divisible by 25. By Eisenstein's criterion, applied to $f(x)$ with $p = 3$ or $p = 5$ as appropriate, it follows that $f(x)$ is irreducible. On the other hand there are clearly infinitely many such choices of a.

3. By Gauss' Lemma it suffices to prove that $f(x)$ is irreducible over $\mathbb{Z}$. Suppose not, suppose that $f = gh$. Reducing modulo p we have

$$\bar{a}_0 = \bar{f} = \bar{g}\bar{h}.$$

Thus $\bar{g}$ and $\bar{h}$ are constant polynomials. It follows that the leading coeffcients b_d and c_e must be divisible by p. But then $a_n = b_d c_e$ is divisible by p^2, a contradiction.

4. See the lecture notes.

5. (i) Let $\phi\colon R \longrightarrow S$ be an isomorphism of rings. It is clear that $r \in R$ is irreducible if and only if $\phi(r) inS$ is irreducible.

(ii) Clear.

6. By the universal property of a polynomial ring, there is a unique ring homomorphism

$$\phi\colon F[x] \longrightarrow F[x]$$

which sends x to $bx + c$ and which fixes F. Thus it suffices to find the inverse map. Let

$$\psi\colon F[x] \longrightarrow F[x]$$

by the unique ring homomorphism which sends x to $(x-c)/b$ (and fixes F). The composition sends x to x and by uniqueness the composition is therefore the identity. Thus ϕ is an automorphism.

7. By the uniqueness part of the universal property, it suffices to prove that the image of x has degree one, since if x is sent to $g(x)$, then $f(x)$ is sent to $f(g(x))$, which has degree the product of the degrees of f and g.
Suppose that ϕ is an automorphism of $F[x]$. Note that $F \cup \{x\}$ generates $F[x]$ as a ring. Thus $\phi(x)$ must have the same property. But if $g(x)$ is any element of $F[x]$ the ring generated by $g(x)$ and F is equal to the set of all polynomials of the form $f(g(x))$. Any such polynomial has degree the product of the degrees. Thus to get degree one polynomials, the degree of $g(x)$ must be one. Thus $\phi(x)$ must have degree one, so that $\phi(x) = bx + c$, $b \neq 0$, $c \in F$.
8. (i) Let $b = -1$ and $c = 0$. Then $\phi(x) = -x$ is an automorphism of order two.
(ii) Let ζ be a primitive nth root of unity. That is to say, pick $\zeta \in \mathbb{C}$ such that

$$\zeta^n = 1,$$

whilst no smaller power is equal to one. For example

$$\zeta = e^{\frac{2\pi i}{n}}$$

will do. Let $\phi(x) = \zeta x$. Then $\phi(x)$ is an automorphism by 6. Clearly ϕ^n is the identity, but if $m < n$, then ϕ^m is not, as $\phi^m(1) = \zeta^m \neq 1$. Thus ϕ is an automorphism of order n.
9. (i) By the binomial theorem

$$(a+b)^p = \sum_i \binom{p}{i} a^i b^{n-i},$$

in any commutative ring. It suffices to observe that the natural number

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

is divisibe by p if $0 < i < p$.
(ii) We have

$$\phi(a+b) = (a+b)^q = a^q + b^q,$$

by (i) and an obvious induction. As

$$\phi(1) = 1 \qquad \text{and} \qquad \phi(ab) = a^p b^p,$$

ϕ is a ring homomorphism.
(iii) $a^q = 0$ if and only if $a = 0$ so that the kernel of ϕ is $\{0\}$.
(iv) Since every injective map between two finite sets of the same cardinality is always a bijection, this is clear.

10. Let $F = \mathbb{F}_p(t)$ the field of rational functions with coeffcients in $\mathbb{F}_p$. Suppose that

$$(f(t))^p = \phi(f) = t.$$

If

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0$$

then

$$f(t)^p = a_n^p t^{np} + a_{n-1}^p t^{p(n-1)} + \cdots + a_0^p,$$

has degree np, a contradiction. Thus t is not in the image of ϕ.