HW 7 SOLUTIONS

JC

(1) (a) $x^3 + 2x + 1 = (x - 2)(x^2 + 2x + 6) + 13$.
(b) $x^3 + 2x + 1 = (x + 1)(x^2 + 2x) + 1$ (notice $x - 2 = x + 1$ here).

(2) (a) If a polynomial of degree 3 is reducible it must have a linear factor (remember the degree of a product is the sum of the degrees of the factors). The only linear polynomials are x and $x + 1$. Routinely

$$x^3+x+1 = x(x^2+1)+1, x^3+x^2+1 = x(x^2+x)+1, x^3+x+1 = (x+1)(x^2+x)+1, x^3+x^2+1 = (x+1)x^2+1.$$

So the polynomials are both irreducible.
(b) $x^4 + x^2 + 1 = \frac{x^6-1}{x^2-1} = \frac{(x^3-1)(x^3+1)}{(x-1)(x+1)} = (x^2 + x + 1)(x^2 - x + 1)$. It is not irreducible, even though it has no real roots.

(3) (a) The painful way to do this would be to compute $(x + 1)f$ for every f. We do it an easier way by using Euclid's algorithm (which works perfectly well in the ring of polynomials over a field).
Now $x^3 + x + 1 = (x + 1)(x^2 + x) + 1$, and accordingly $x^2 + x$ is the inverse (remember $-1 = +1$ here so $(x + 1)(x^2 + x) = f + 1$.
Let us compute the powers of $x + 1$ mod f. We do this by repeatedly multiplying by $x + 1$ and reducung mod f. We get a sequence

$$1, x + 1, x^2 + 1, x^2, x^2 + x + 1, x, x^2 + x, 1$$

so $n = 7$.
(b) Similarly to the last part: $x^3 + x^2 + 1 = (x + 1)x^2 + 1$, so x^2 is the inverse. The powers are

$$1, x + 1, x^2 + 1, x, x^2 + x, x^2 + x + 1, x^2, 1$$

so again $n = 7$.
(c) Since 7 is prime, a little thought shows that there was nothing special about $x + 1$ in the previous exercises: any element other than 0, 1 will have the property that its powers run through all seven nonzero elements. In particular x has this property. It will be helpful to have listed the zero through six powers of x mod f and mod g: mod f we have

$$1, x, x^2, x + 1, x^2 + x, x^2 + x + 1, x^2 + 1$$

and mod g we have

$$1, x, x^2, x^2 + 1, x^2 + x + 1, x + 1, x^2 + x$$

If we have a map ϕ of the kind required then easily $\phi(a^n) = \phi(a)^n$ for all a and n, so it suffices to give the value of ϕ at x to determine ϕ completely, in fact if $\phi(x) = x^n \mod g$ then ϕ is given by $\phi(x^m \mod f) = x^{mn} \mod g$.

So now we just need to determine an acceptable value for n. Any value of n which we choose will give a map which respects multiplication, the trick is to choose n so that ϕ respects addition as well. Now notice that x satisfies the equation $x^3 + x + 1 = 0$ in F, so $\phi(x)$ must satisfy $\phi(x)^3 + \phi(x) + 1 = 0$ in G. This limits the possibilities to $\phi(x) \in \{x+1, x^2+1, x^2+x\}$. It turns out that all three of them work, we choose $\phi(x) = x^2 + 1 = x^3 \mod g$ so that $\phi(x^n \mod f) = x^{3n} \mod g$.

Explicitly this gives $\phi(1) = 1$, $\phi(x) = x^2+1$, $\phi(x^2) = x^2+x$, $\phi(x+1) = x^2$, $\phi(x^2+x) = x+1$, $\phi(x^2+x+1) = x$, $\phi(x^2+1) = x^2+x+1$. Of course $\phi(0) = 0$. It is now routine if tedious to check that addition is respected: for example $\phi(x+x^2) = x+1 = (x^2+1) + (x^2+x) == \phi(x) + \phi(x^2)$.

(4) By the associative law for $+$, $f(a)+f(b) = f(a+b)$. By the distributive law for $\times$ over $+$ and the equation $1 \times 1 = 1$, $f(a)f(b) = f(ab)$. If n is minimal with $f(n) = 0$ let $n = ab$ with $0 < a < n$. Then $f(n) = f(a)f(b) = 0$ so easily $f(a) = 0$ or $f(b) = 0$, and it follows that $a = 1$ and $b = n$ by minimality of n. So n is prime.