Homework 3 (Due Feb 7, 2025)

Jack Hyatt
MATH 547 - Algebraic Structures II - Spring 2025

June 8, 2025

Justify all of your answers completely.

1. Use a substitution and Eisenstein's criterion to prove that each of the polynomials below is irreducible over $\mathbb{Q}$.

   (a) $f(x) = x^6 + x^3 + 1$

   Let us substitute with x+1.

$$\begin{aligned} f(x+1) &= (x+1)^6 + (x+1)^3 + 1 \\ &= x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3 \end{aligned}$$

   Let our prime be $p = 3$. We have that $p \nmid 1$, p divides all other coefficients, and $p^2 \nmid 3$.
   So $f(x)$ must be irreducible over $\mathbb{Q}[x]$.

   (b) $f(x) = x^3 + 3x^2 + 5x + 5$

$$\begin{aligned} f(x+1) &= (x+1)^3 + 3(x+1)^2 + 5(x+1) + 5 \\ &= x^3 + 6x^2 + 14x + 14 \end{aligned}$$

   Let our prime be $p = 2$. We have that $p \nmid 1$, p divides all other coefficients, and $p^2 \nmid 14$.
   So $f(x)$ must be irreducible over $\mathbb{Q}[x]$.

2. Find the factorization of $f(x) = x^8 - 1$ into irreducible factors in $\mathbb{Q}[x]$. Prove that the factors you found are irreducible in $\mathbb{Q}[x]$.

$$f(x) = x^8 - 1 = (x^4 + 1)(x^4 - 1) = (x^4 + 1)(x^2 + 1)(x + 1)(x - 1)$$

   Clearly $(x^2 + 1)$ is irreducible since it is of degree ≤ 3 with no roots in $\mathbb{Q}$, and clearly the linear terms $(x - 1)$ and $(x + 1)$ are irreducible. Now to show irreduciblity for $(x^4 + 1)$.

Consider substitution with $x+1$.

$$f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$$

Clearly, with the prime being 2, Eisenstein's criterion holds. So We have all irreducible factors.

3. Find the factorization of $f(x) = x^{12} - 1$ into irreducible factors in $\mathbb{Q}[x]$. Prove that the factors you found are irreducible in $\mathbb{Q}[x]$.

$$\begin{aligned} f(x) = x^{12} - 1 &= (x^6+1)(x^6-1) \\ &= (x^2+1)(x^4-x^2+1)(x^3+1)(x^3-1) \\ &= (x^2+1)(x^4-x^2+1)(x+1)(x^2-x+1)(x-1)(x^2+x+1) \end{aligned}$$

Clearly (x^2+1),(x^2-x+1), and (x^2+x+1) are irreducible since they are degree ≤ 3 with no roots in $\mathbb{Q}$, and clearly the linear terms $(x-1)$ and $(x+1)$ are irreducible. Now to show irreduciblity for (x^4-x^2+1).

Let us first show it cannot factor into two quadratic factors. Let $y = x^2$. Then x^4-x^2+1 becomes y^2-y+1, which has no real solutions. So no quadratic factors.
Now to show it cannot factor with a linear factor. By rational root theorem, the only possible factors could be $x \pm 1$. But $(\pm1)^4 - (\pm1)^2 + 1 = 1 \neq 0$. So no linear factors.
So all the factors found are irreducible.

4. Let m and n be positive integers. Prove that $(x^m - 1) \mid (x^n - 1)$ in $\mathbb{Q}[x]$ if and only if $m \mid n$. Hint: It might be useful to look at the complex roots of these polynomials.

Proof. ($\implies$)
Since $(x^m-1) \mid (x^n-1)$, then every root, r, of x^m-1 is also a root of x^n-1. Since r is a m'th root of unity, we shall represent the root as

$$r = \cos(\frac{2\pi}{m}k) + i\sin(\frac{2\pi}{m}k)$$

for some k. Since r is also an n'th root of unity, we have

$$1 = r^n = \cos(2\pi k\frac{n}{m}) + i\sin(2\pi k\frac{n}{m}).$$

So then n/m is an integer, meaning $m \mid n$.

($\impliedby$)
Let $n = km$ for some integer k. Then

$$x^n - 1 = x^{km} - 1 = (x^m)^k - 1^k = (x^m-1)(x^{(k-1)m} + x^{(k-2)m} + \ldots + x^m + 1)$$

So $(x^m-1) \mid (x^n-1)$ in $\mathbb{Q}[x]$. ∎