MATH 340 Assignment 6 Solutions, Fall 2017

Michael Monagan

Additional questions on extension fields and roots of unity.

1. Is $\mathbb{Q}[z]/(z^3+1)$ a field? Justify your answer briefly.

   Since $z^3+1 = (z+1)(z^2-z+1)$ is not irreducible over $\mathbb{Q}$, $\mathbb{Q}[z]/(z^3+1)$ is not a field, because, for example, $[z+1]$ is a zero divisor as $[z+1][z^2-z+1] = [z^3+1] = [0]$.

2. Consider the field $F = \mathbb{Q}[z]/(z^2-2)$.
   Use the extended Euclidean algorithm to find the inverse of $[z] \in F$.

   Since z^2-2 is irreducible over $\mathbb{Q}$ we have $\gcd(z, z^2-2) = 1$. If we use the extended Euclidean algorithm to solve $\lambda z + \mu(z^2-2) = \gcd(z, z^2-2) = 1$ for $\lambda, \mu \in \mathbb{Q}[z]$ then $[\lambda]$ will be the inverse of $[z]$ in F. I get $\lambda = \frac{1}{2}z$ and $\mu = -\frac{1}{2}$ so $[z]^{-1} = [\frac{1}{2}z]$ in F.

3. Consider the field $F = \mathbb{R}[z]/(z^2+1)$. Let $\phi : F \to \mathbb{C}$ be the mapping given by $\phi([a+bz]) = a+bi$. Show that ϕ is isomorphism.

   Since ϕ is invertible with $\phi^{-1}(a+bi) = [a+bz]$ we have a bijection.
   Let $A = [a+bz]$ and $B = [c+dz]$ be elements of F.
   We must show $\phi(A+B) = \phi(A)+\phi(B)$ and $\phi(AB) = \phi(A)\phi(B)$.

   $\phi([a+bz]+[c+dz]) = \phi([(a+c)+(b+d)z]) = (a+c)+(b+d)i = (a+bi)+(c+di) = \phi([a+bz]) + \phi([c+dz])$.

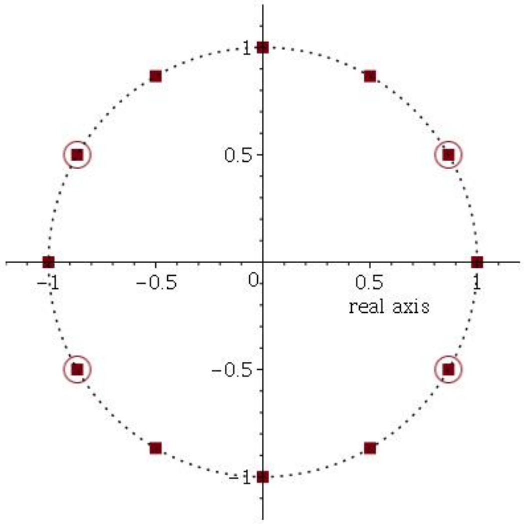
   Now in F we have $[z^2+1] = [z^2]+[1]$ so that $[z^2] = [-1]$.

   $\phi(AB) = \phi([a+bz]\cdot[c+dz]) = \phi([ac+(bc+ad)z+bdz^2]) = \phi([ac+(bc+ad)z-bd]) = (ac-bd)+(bc+ad)i$.

   And $\phi(A)\phi(B) = \phi([a+bz])\cdot\phi([c+dz]) = (a+bi)(c+di) = (ac-bd)+(ad+bc)i$.

4. Sketch the 12'th roots of unity in the complex plane. Circle which ones are primitive.

   See next page



5. Let ω be a primitive n'th root of unity. For n even, prove that $\omega^{n/2} = -1$.

   Since n is even let we have $1 = \omega^n = (\omega^{n/2})^2$ in $\mathbb{C}$. In $\mathbb{C}$ the equation $x^2 = 1$ has two solutions $x = 1$ and $x = -1$. If $\omega^{n/2} = 1$ then this would contradict ω is primitive. Thus the only possibility is $\omega^{n/2} = -1$.

6. What are the primitive 6'th roots of unity?
   Find $\phi_6(x)$ the sixth cyclotomic polynomial. See Theorem 2.8.11.

   We have $\omega = \cos(2\pi/6) + i\sin(2\pi/6) = \cos(\pi/3) + i\sin(\pi/3) = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ is a primitive 6'th root of unity. We also have ω^m is a primitive 6'th root of unity iff $\gcd(m, 6) = 1$ implies $m = 1, 5$ thus $\cos(5\pi/3) + i\sin(5\pi/3)$ is the other primitive 6'th root of unity.

   The divisors of 6 are 1,2,3,6 thus $x^6 - 1 = \phi_1(x)\phi_2(x)\phi_3(x)\phi_6(x)$ by the formula on the top of page 138. Hence

$$\phi_6(x) = \frac{x^6 - 1}{\phi_1(x)\phi_2(x)\phi_3(x)} = \frac{(x^3 - 1)(x^3 + 1)}{(x - 1)(x + 1)(x^2 + x + 1)} = (x^2 - x + 1)$$

Note this polynomial is the minimal polynomial for the primitive 6'th roots of unity.