Homework 12

MATH 115
UC Berkeley
Guilherme Gomes Haetinger

December 9, 2019

Thank you for the semester long grading, Zehao! Happy holidays!

9.1

5)

We can state, for $r \in \mathbb{Q}$, that $f = hg = r * h_1 g_1^*, g, h \in \mathbb{Z}[x]$. By Thm 9.6, we know that $f_1 = h_1 g_1^*$ is primitive. Now we want to prove that $r \in$ Z\$. We first write that $r = \frac{a}{b}, (a, b) = 1$ and try to prove $b = 1$. By this, we know $bf = af_1$ and, thus, that $b|af_1 \to b|f_1$ (b divides all the coefficients in f_1) and, since f_1 is primitive, b must equal *1*. Now we can just simply write $g_1 = r * g_1^*, f = g_1 h_1$.

6)

We know that f and g are primitive, so $f, g \in \mathbb{Z}[x]$. Following this, we have $f(x)|g(x), g(x)|f(x) \to g(x) = q(x)f(x), f(x) = q^*(x)g(x) \to f(x) = q^*(x)q(x)f(x) \to q^*(x)q(x) = \pm 1$ (because they must be integers) $f(x) = \pm g(x)$.

7)

Within our claim, we know, by Thm. 9.1, that $g(m) = q(m)f(m) + r(m)$. We can multiply both sides by an integer k, making $kq(m), kr(m) \in \mathbb{Z}$. Considering that $g(m) > kr(m)$ for a big enough m, we can state that, since $g(m) = kq(m)f(m) + kr(m)$ holds all conditions, then so does $g(m) = q(m)f(m) + r(m)$.

8)

They can be the following: $f(x) = 2x + 4 = 2(x + 2), g(x) = 3x + 3 = 3(x + 1)$. They will always have a GCD of 2 when x is odd, meaning they have a $GCD > 1$ for infinitely many positive integers but their polynomials are coprime.

9)

If we take $x_0 = P^n * f(0)$, as the hint says, with P being the product of all finite primes that divide *f*, we have that, for a large n, the value $f(x_0) = P^n f(0) * q(P^n f(0)) + f(0)$ being the constant value larger than 0 will have the following condition: $f(x_0) > |f(0)|$. This way, we can state $f(x_0) = f(0)(P^n q(P^n f(0))) + 1)$, meaning that f is a polynomial divisible by a number larger than the supposed prime.

9.2

1)

- $7 \rightarrow f(x) = x - 7$
- $\sqrt[3]{7} \rightarrow \frac{x^3}{7} - 1$
- $\frac{1+\sqrt[3]{7}}{2} \rightarrow 4x^3 - 6x^2 + 3x - 4$
- $1 + \sqrt{2} + \sqrt{3} \rightarrow x^4 - 4x^3 - 4x^2 + 16x - 6$

We know that only $(\frac{1+\sqrt[3]{7}}{2})$ is not an Algebraic Integer.

2)

For the first option $-\alpha$, we can just use $alpha$'s polynomial and switch its sign, meaning the degree would be maintained. The second option, α^{-1}, we can still remodel the original polynomial so it takes in consideration the divisor's magnitude, trivially. The third case $\alpha - 1$, we can also remodel the coefficients so it takes into consideration the remainder resulted by the powered polynomial $\alpha - 1$, just canceling each other in every level.

9.3

1) Couldn't understand it properly

2)

We have that the minimal polynomial for the items in $\mathbb{Q}(i)$ is equal $x^2 + 1$, which is the same as the modulo expression in the other field. Now, because, $G(x) = x^2 + 1$ is an irreducible polynomial and the statement in the first sentence is true, we have that they are isomorphic corresponding to Thm 9.16.

9.4

1)

Considering Def. 9.7, we know that the unit of the $\mathbb{Q}$ field it ± 1 because $1 = x\alpha$ with $x, \alpha \in \mathbb{Z}$ only if $x, alpha = \pm 1$. Following this definition, we have that for α, β to be associated need to have their values so that $\frac{\alpha}{\beta} = \pm 1$ (unit), which can only be true if $\alpha = \pm\beta$.

2)

We have that m is the smallest positive rational so that $m\alpha$ is an algebraic integer. We also know that every value in the algebraic integer field can be expressed as a multiplication. Since that's true, we know that b can be expressed as a multiplication of another field member that is considered the smallest, this way $b = x * m \rightarrow m|b$.

3)

- Yes.
- Not necessarily $\rightarrow \alpha = -\frac{1}{2} + \frac{i\sqrt[3]{3}}{2} = e^{\frac{2\pi i}{3}}$. α then satisfies $x^2 + x + 1$, meaning α is an algebraic integer even though $\frac{1}{2}$ isn't.