Math3303 Assignment 7

Dominic Scocchera

May 2023

Q1

We have $f(x) = 1 + x + ... + x^{p-1} \in \mathbb{Z}[x]$, which we want to show is irreducible. The Eisenstein criterion for irreducibility in $\mathbb{Q}[x]$ is:

1. p divides each coeffecient $a_i, \quad 0 \leq i < p-1$
2. p does not divide a_n
3. p^2 does not divide a_0

Now consider:

$$\begin{aligned} f(x+1) &= 1 + (x+1) + ... + (x+1)^{p-1} \\ &= \sum_{n=0}^{p-1}\sum_{k=0}^{n}\binom{n}{k}x^k \\ &= \binom{p}{1} + \binom{p}{2}x + ... + \binom{p}{p-1}x^{p-2} + x^{p-1} \end{aligned}$$

We now see that p divides each coeffecient $a_i, \quad 0 \leq i < p-1$, p^2 does not divide a_0 and p does not divide $a_n = 1$. As the Eisenstein criterion is satisfied we have that $f(x+1)$ is irreducible in $\mathbb{Q}[x]$. We will now show this also holds for $f(x)$ as we can create an automorphism $\alpha : f(x) \to f(x+1)$. Suppose $f(x), g(x) \in \mathbb{Z}[x]$ such that $h_1(x) = f(x) + g(x)$ and $h_2(x) = f(x)g(x)$, then:

$$\begin{aligned} \alpha(f(x) + g(x)) &= \alpha(h_1(x)) \\ &= h_1(x+1) \\ &= f(x+1) + g(x+1) \\ &= \alpha(f(x)) + \alpha(g(x)) \end{aligned}$$

$$\begin{aligned}\alpha(f(x)g(x)) &= \alpha(h_2(x))\\ &= h_2(x+1)\\ &= f(x+1)g(x+1)\\ &= \alpha(f(x))\alpha(g(x))\end{aligned}$$

So it is a homomorphism. Similarly we can define $\beta : f(x+1) \to f(x)$, letting $f(x+1), g(x+1) \in \mathbb{Z}[x]$ such that $h_1(x+1) = f(x+1)+g(x+1)$ and $h_2(x+1) = f(x+1)g(x+1)$, we then have:

$$\begin{aligned}\beta(f(x+1)+g(x+1)) &= \beta(h_1(x+1))\\ &= h_1(x)\\ &= f(x)+g(x)\\ &= \beta(f(x+1))+\beta(g(x+1))\end{aligned}$$

$$\begin{aligned}\beta(f(x+1)g(x+1)) &= \beta(h_2(x+1))\\ &= h_2(x)\\ &= f(x)g(x)\\ &= \beta(f(x+1))\beta(g(x+1))\end{aligned}$$

So β is a homomorphism. Composing α and β we get the identity mapping and hence it is an automorphism. This means that as $f(x+1)$ is irreducible we have that $f(x)$ is also irreducible. Noting the irriducibility of $f(x)$ in $\mathbb{Q}[x]$ from above and that $f(x)$ is a primitive polynomial as all coeffecients are 1, so the gcd of all coefficients is 1, we get from lemma 11.3 in Gregory Lee's Abstract Algebra that $f(x)$ is irreducible in $\mathbb{Z}[x]$ as required.

Q2

First we show that $x = 1+\sqrt{3}i$ is irreducible in $S := \mathbb{Z}+\sqrt{3}i\mathbb{Z} \subseteq \mathbb{C}$.

Proof. Letting $x = \alpha\beta$, where $\alpha, \beta \in S$ we require that either α or β is 1. Consider $a, b, c, d \in \mathbb{R}$ we get:

$$\begin{aligned}\alpha\beta &= (a+\sqrt{3}ib)(c+\sqrt{3}id)\\ &= ac+(ad+bc)\sqrt{3}i-3bd\end{aligned}$$

So we get that $ac = 1$, $ad+bc = 1$ and $-3bd = 0 \implies b = 0$ or $d = 0$. If $b = 0$ then $ad = 1 = ac \implies d = c$. Subbing back into $\alpha\beta$ we get

$x = c((a-3b)+(a+b)\sqrt{3}i)$, hence $c = 1$, $a - 3b = 1 \implies a = 1 + 3b$ and $a + b = 1 \implies 3b + 1 + b = 1 \implies b = 0 \implies a = 1$. Subbing back into α we get $\alpha = 1$ as required.

Now if $d = 0$ then $bc = 1 = ac \implies a = b$. Subbing back into $\alpha\beta$ we get $x = b((c-3d)+(d+c)\sqrt{3}i)$, hence $b = 1$, $c - 3d = 1 \implies c = 1 + 3d$ and $c + d = 1 \implies 3d + 1 + d = 1 \implies d = 0 \implies c = 1$. Subbing back into β we get $\beta = 1$ as required. Hence α or β will always be 1 and therefore x is irreducible. □

Now we show that x is not prime.

Proof. x is prime if for $\alpha, \beta \in S$ such that $x|\alpha\beta$ we have $x|\alpha$ or $x|\beta$. We see that $xx^* = (1+\sqrt{3}i)(1-\sqrt{3}i) = 4 = 2^2$. We also see that x divides $1 + \sqrt{3}i$ but it does not divide 2 and hence it is not prime. □

Q3

Let R be a UFD. Suppose $\exists a_1, a_2, ... \in$R such that $(a_1) \subseteq (a_2) \subseteq ...$. Show $\exists i \in \mathbb{Z}_{>0}$ such that $(a_i) = (a_{i+1})$.

Proof. R is a UFD so every non-zero element has a unique factorisation into irreducibles up to multiplication by units. Let $a_1 = b_1^{c_1} b_2^{c_2} ... b_n^{c_n}$, for irreducibles $b_1, ..., b_n \in$R and $c_1, ..., c_n \in \mathbb{Z}_{>0}$. We then have from $(a_1) \subseteq (a_2)$ that a_2 is a product of a subset of $\{b_1, ..., b_n\}$, each raised to their respective powers d_i, where $d_i \leq c_i$. From this we see that the length of the chain is bounded above by $\prod_{j=1}^{n} c_j$. As the length is bounded above we must have that $\exists i \in \mathbb{Z}_{>0}$ such that $(a_i) = (a_{i+1})$. □

Q4

a)

K consists of fractions of the form $f(x)g(x)^{-1}$, with $0 \neq g(x)$ and $f(x), g(x) \in \mathbb{Z}[[x]]$. Now if we write $g(x) = x^k(r - xh(x)) = x^k r(1 - \frac{x}{r}h(x))$ with $k \geq 0$ and $0 \neq r \in$R. Then $\frac{1}{g(x)} = x^{-k} \sum_{n \geq 0} \frac{x^n}{r^n}(h(x))^n$ and we see that $h(x) = \sum_{i \geq m} c_i x_i$ where $m \in \mathbb{Z}$ depends on h and each c_i is of the form $c_i = \frac{a_i}{b_i}$ with $a_i \in$R and $b_i \in \mathbb{Z}_{>0}$. So in K every element is a power series that satisfies that there exists an element $r \in$R such that all $c_i \in$R$\left[\frac{1}{R}\right]$. But it is clear that $\frac{1}{n+1} \notin \mathbb{Z}\left[\frac{1}{n}\right]$, hence $A \notin K$

b)

First we show that F is a field

Proof. We first show closure under addition.

$$\begin{aligned}
\frac{x^{N_1}}{\alpha_1}\sum_{n\geq 0} a_n\left(\frac{x}{\alpha_1}\right)^n + \frac{x^{N_2}}{\alpha_2}\sum_{n\geq 0} b_n\left(\frac{x}{\alpha_2}\right)^n &= \sum_{n\geq 0}\left(\frac{x^{N_1}a_n}{\alpha_1^{n+1}} + \frac{x^{N_2}b_n}{\alpha_2^{n+1}}\right)x^n \\
&= \sum_{n\geq 0}\left(\frac{x^{N_1}a_n\alpha_2^{n+1} + x^{N_2}b_n\alpha_1^{n+1}}{\alpha_1^{n+1}\alpha_2^{n+1}}\right)x^n \\
&= \frac{1}{\alpha_1\alpha_2}\sum_{n\geq 0}\left(x^{N_1}a_n\alpha_2^{n+1} + x^{N_2}b_n\alpha_1^{n+1}\right)\left(\frac{x}{\alpha_1\alpha_2}\right)^n \\
&= \frac{x^j}{\alpha_3}\sum_{n\geq 0} c_n\left(\frac{x}{\alpha_3}\right)^n
\end{aligned}$$

Where $j = \min\{N_1, N_2\}$ and $c_n = \begin{cases} a_n\alpha_2^{n+1} & \text{if } j = N_1 \text{ and } |n - N_1| < N_2 \\ b_n\alpha_1^{n+1} & \text{if } j = N_2 \text{ and } |n - N_2| < N_1 \\ a_n\alpha_2^{n+1} + b_n\alpha_1^{n+1} & \text{else} \end{cases}.$
We also notice that we have $\alpha_1\alpha_2 = \alpha_3 \in \mathbb{Z}$, $j \in \mathbb{Z}$ and $c_n \in \mathbb{Z}$. Hence it is closed under addition. We now show it is closed under multiplication.

$$\begin{aligned}
\left(\frac{x^{N_1}}{\alpha_1}\sum_{n\geq 0} a_n\left(\frac{x}{\alpha_1}\right)^n\right)\left(\frac{x^{N_2}}{\alpha_2}\sum_{n\geq 0} b_n\left(\frac{x}{\alpha_2}\right)^n\right) &= \frac{x^{N_1+N_2}}{\alpha_1\alpha_2}\sum_{n\geq 0}\left(\sum_{k=0}^{n}\frac{a_k b_{n-k}}{\alpha_1^n\alpha_2^n}\right)x^n \\
&= \frac{x^{N_1+N_2}}{\alpha_1\alpha_2}\sum_{n\geq 0}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)\left(\frac{x}{\alpha_1\alpha_2}\right)^n \\
&= \frac{x^{N_3}}{\alpha_3}\sum_{n\geq 0} c_n\left(\frac{x}{\alpha_3}\right)^n
\end{aligned}$$

Where $N_1 + N_2 = N_3 \in \mathbb{Z}$, $\alpha_3 \in \mathbb{Z}$ and $\sum_{k=0}^{n} a_k b_{n-k} = c_n \in \mathbb{Z}$. So it is also closed under multiplication. We also see that 0 $(a_n = 0)$ and 1 $(\alpha = 1, N = 0$ and $a_n = 0$ for all $n > 0)$ are in F. As it is a polynomial and closed under addition and multiplication we see that associativity, commutativity, distributivity and identity hold for both addition and multiplication. We also see that additive inverse is just the series whose coeffecients are the negative of a_n. Now we show that the mulitiplicative inverse exists.

Hence F is a field. □

Now we wish to show that $K \subseteq F$.

Proof. Take $k \in K$, where $k = f(x)g(x)^{-1}$, such that $g(x) \neq 0$ and $f(x), g(x) \in \mathbb{Z}[[x]]$. We see that $f(x)$ and $g(x)^{-1}$ are some power series with integer coeffecients and that as K is a field (inverses exist and closed under multiplication) we get $k = f(x)g(x)^{-1} = h(x)$, where:

$$h(x) = x^N \sum_{n \geq 0} a_n x^n, \quad a_n \in \mathbb{Z}$$

Hence this is also an element of F where $\alpha = 1$. From this we get the result $K \subseteq F$. $\square$