Math250aHw9

Trustin Nguyen

October 24, 2023

Exercise 1: Recall that $R = \mathbb{Z}[i]$ is a UFD. What is the content of the polynomial $(5+5i)X^2 + (-1+3i)X + 2 \in R[X]$?

Proof. We know that $\mathbb{Z}[i]$ is a Euclidean domain with a measure of size as the norm. Then we have:

$$5 + 5i = 5(1 + i)$$

where $1 + i$ is irreducible because

$$\|1 + i\| = 2$$

and then if $1 + i$ is a product of two complex numbers: $z_1 z_2$, then $\|z_1\|\|z_2\| = 2$, so one of them is a unit. Now for 5, we see that:

$$5 = 1^2 + 2^2$$

so we can take:

$$(1 + 2i)(1 - 2i) = 5$$

Now for the second coefficient, we have:

$$\|-1 + 3i\| = 10$$

and if $-1 + 3i = (a + bi)(c + di)$, then

$$(a^2 + b^2)(c^2 + d^2) = 10$$

which means that either factor is either 1 and 10 or 2 and 5. If it is 1, then one factor is a unit and we are done. If

$$a^2 + b^2 = 2 \text{ and } c^2 + d^2 = 5$$

we have

$$\begin{aligned} a &= \pm 1 \\ b &= \pm 1 \\ c &= \pm 1 \text{ or } \pm 2 \\ d &= \pm 1 \text{ or } \pm 2 \end{aligned}$$

We get

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i = -1 + 3i$$

and by trial and error, we find:

$$(1 + i)(1 + 2i) = -1 + 3i$$

and both factors are irreducible. Finally

$$2 = (1 + i)(1 - i)$$

So we have

$$(1 + 2i)(1 - 2i)(1 + i)X^2 + (1 + i)(1 + 2i)X + (1 + i)(1 - i)$$

Then we pull out the largest power of each prime that divides each coefficient. We get that the content is

$$(1 + i)$$

so we are done. □

Exercise 2:

(a) Find an ideal in $\mathbb{Z}[X]$ that cannot be generated by 2-elements.

Proof. Consider the ideal $(4, 2x, x^2)$. This ideal is not generated by one element, otherwise, the 3 polynomials would share a common root or they would all be constants, which is not the case. We can look at the ideals generated by the leading coefficients which gives $(4) \subset (2) \subset (1)$. Now suppose that this was generated by an ideal (f, g) on two elements. We also consider the ideal generated by their leading coefficients which would be $(a) \subset (b)$. Now suppose that the degrees of f and g were less than or equal to 2. Then it follows that assuming $(f, g) \subseteq (4, 2x, x^2)$, we require that $a, b \in \{1, 2, 4\}$. But no matter how we chain the ideals such as:

$$(4) \subseteq (2) \subseteq (2), (4) \subseteq (1) \subseteq (1), (2) \subseteq (1) \subseteq (1)$$

we find that no generators can be found with the corresponding two coefficients that generate $(4, 2x, x^2)$. So $(f, g) \not\supseteq (4, 2x, x^2)$. If either had degree greater than or equal to 2, then we should be able to reduce them so that their degrees were less than or equal to 2, assuming that $(4, 2x, x^2) \subseteq (f, g)$ and show that they are not equal by the same process. □

(b) Give an example of a prime ideal in $\mathbb{Z}[X]$ that is not maximal.

Proof. A prime ideal is (x) because if $f \in (x)$, then $x \mid f$. So if $f = gh$, $h \notin (x)$, then $x \mid gh$ means that $x \mid g$. So (x) is prime. But $(x) \subseteq (x, 2)$ and $(x, 2) \neq \mathbb{Z}[X]$. So (x) is prime but not maximal since $2 \nmid x$. □

(c) Show that every maximal ideal in $\mathbb{Z}[X]$ is generated by 2-elements.

Proof. Let I be an ideal in $\mathbb{Z}[X]$. Consider the set of leading coefficients S_i attached to the term x^i. Then we have:

$$S_0 \subseteq S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n = S_{n+1} \cdots$$

Then it follows that if $P_m = \bigcup_{i=0}^{m} S_i$, then P_m is generated by one element as $\mathbb{Z}$ is a Euclidean domain. So if $P_n = (k)$, then (x, k) contains the ideal I. If $k = 1$, we say $P_{n-1} = (k')$ and (x, k') contains I.

In either case, we have have found an ideal containing I that is not the whole ring. Furthermore, if k, k' are not prime, we can find a prime dividing it called p and $(x, k) \subseteq (x, p) \neq \mathbb{Z}[X]$.

Finally, maximal ideals cannot be one element ideals because either it is a constant and we can adjoin x, or it is a non constant polynomial, to which we can adjoin the constant to get a two element proper ideal. So this tells us that

So any maximal ideal has at least two elements, and any ideal with more than 2 elements is contained in some proper ideal generated by two elements. So every maximal ideal is generated by 2 elements. □

Exercise 3: Show that the rings $\mathbb{Z}[2i]$ and $\mathbb{Z}[\sqrt{-7}]$ are not integrally closed. Give explicit examples where unique factorization fails.

Proof. $\mathbb{Z}[2i]$ is not integrally closed because $1+i = \frac{2+2i}{2} \in \mathbb{Q}[2i]$ is a root of the polynomial:

$$x^2 - 2i \in \mathbb{Z}[2i][x]$$

$\mathbb{Z}[\sqrt{-7}]$ is not integrally closed because we have that $\frac{1+\sqrt{-7}}{2} \in \mathbb{Q}[\sqrt{-7}]$ but it is the root of the polynomial of

$$x^2 + x + 1 - \sqrt{-7}$$

as

$$\begin{aligned}\left(\frac{1+\sqrt{-7}}{2}\right)^2 + \left(\frac{1+\sqrt{-7}}{2}\right) + 1 - \sqrt{-7} &= \frac{1+2\sqrt{-7}-7}{4} + \frac{1+\sqrt{-7}}{2} + 1 - \sqrt{-7} \\ &= \frac{-6+2\sqrt{-7}}{4} + \frac{2+2\sqrt{-7}}{2} + 1 - \sqrt{-7} \\ &= \frac{-4+4\sqrt{-7}}{4} + 1 - \sqrt{-7} \\ &= -1 + \sqrt{-7} + 1 - \sqrt{-7} \\ &= 0\end{aligned}$$

Now for the example where unique factorization fails, we have that:

$$2i \cdot 2i = -4 = -1 \cdot 2 \cdot 2$$

We know that 2 is prime because if $2 \mid (x+2yi)(w+2zi)$, then $2 \mid xw$. Since 2 is prime in $\mathbb{Z}$, then $2 \mid x$ or $2 \mid w$. So 2 divides either $(x+2yi)$ or $(w+2zi)$. We also know that $2i$ is prime because $\mathbb{Z}[2i]/(2i) = \mathbb{Z}$ which is an integral domain. Since $2i$ and 2 do not differ by a unit, we have that unique factorization fails.

For the other one, we have:

$$(1+\sqrt{-7})(1-\sqrt{-7}) = 8 = 2 \cdot 2 \cdot 2$$

which is a decomposition of unequal numbers of irreducible elements. □

Exercise 4: Let G be the group of complex n-th roots of unity. Let $\zeta \in G$ act on $k[X,Y]$ by $\zeta \cdot X = \zeta X$ and $\zeta \cdot Y = \zeta^{-1} Y$. Show that there is an isomorphism $k[X,Y]^G = k[U,V,W]/(UW - V^n)$.

Proof. Consider the term $X^i Y^j$. Then if $\varphi : G \circlearrowleft k[X,Y]$ as defined above, we have:

$$\varphi(X^i Y^j) = \varphi(X^i)\varphi(Y^j) = \zeta^i \zeta^{-j} X^i Y^j$$

We require $\zeta^i \zeta^{-j} = \zeta^{i-j} = 1$. We have that $\zeta^{zn} = 1$ exactly when $z \in \mathbb{Z}$. So $i - j = zn$. So $i \equiv j \pmod{n}$. So this tells us that:

$$k[X,Y]^G = k[X^n, XY, Y^n] = k[U,V,W]/\sim$$

where $\sim$ is the relation, $UW = V^n$. So we have:

$$k[X,Y]^G = k[U,V,W]/(UW - V^n)$$

which concludes the proof. □

Exercise 5: Write $X_1^3 + X_2^3$ as a polynomial in $e_1 = X_1 + X_2$ and $e_2 = X_1 X_2$.

Proof. We first note that

$$e_1^3 = (X_1 + X_2)^3 = X_1^3 + 3X_1^2X_2 + 3X_1X_2^2 + X_2^3$$

Then

$$e_1e_2 = (X_1 + X_2)X_1X_2 = X_1^2X_2 + X_1X_2^2$$

So

$$3e_1e_2 = 3X_1^2X_2 + 3X_1X_2^2$$

and so

$$e_1^3 - 3e_1e_2 = X_1^3 + X_2^3$$

which is what we wanted. □