David Owen Horace Cutler

Math 146: Homework 3

February 23, 2024

Exercise 1. Let F be a field and let $f \in F[x]$ have degree 1. Prove that the principal ideal generated by f is maximal.

Proof. Assume for the sake of contradiction that (f) is not maximal, i.e. there is some ideal I such that:

$$(f) \subsetneq I \subsetneq F[x]$$

Obviously then, $I \setminus (f)$ is nonempty then. We can consider some polynomial g in $I \setminus (f)$ then.

By definition, $f \nmid g$, as this would have $g \in (f)$. Appealing to the division algorithm for polynomials then, we have a unique decomposition of g given by the following:

$$\begin{gathered} g = fq + r \\ q, r \in F[x],\ \deg(r) < \deg(f) \end{gathered} \tag{1}$$

We note it cannot be $r = 0$, as this would have $g = fq$, i.e. $f \mid g$. As $\deg(r) < \deg(f) = 1$ then, the only possibility is that $\deg(r) = 0$, i.e. r is a constant polynomial.

As $f \nmid g$ then, it must be $r \neq 0$. Reorganizing, we get

$$r = g - fq,$$

where $r \in I$ as $g \in I$ and $-fq = f(-q) \in (f) \subsetneq I$, appealing to fact that I as an ideal is additive subgroup.

Thus I contains a constant polynomial $r = a \neq 0 \in F$. As a is a unit in F then, it follows r is a unit in $F[x]$, i.e. it admits an inverse $r^{-1} \in F[x]$.

As $r \in I$ then, $rr^{-1} = 1 \in I$. But this yields a contradiction as it follows then trivially that I must be the whole ring $F[x]$, as $1 \in I$ has that $1 \cdot h = h \in I$ for all $h \in F[x]$.

Thus it must be the principal ideal (f) is maximal. □

Exercise 2. Let R be a commutative ring. Prove that every maximal ideal is a prime ideal.

Proof. Using the theorems we proved in class, we know for a commutative ring R that given an ideal I, R/I is an integral domain if and only if I is prime, and R/I is a field if and only if I is maximal.

Let I be a maximal ideal in R then. Recalling then that all fields are integral domains (as they admit cancellation), we get the following:

$$\begin{aligned} I \text{ is maximal} &\to R/I \text{ is a field} \\ \to R/I \text{ is an integral domain} &\to I \text{ is prime} \end{aligned} \tag{2}$$

Which shows exactly what is desired. □

Exercise 3. Let $R = \mathbb{Z}[i]$. For a prime number p, let (p) be the principal ideal generated by p in R.

(a) Prove that the ideal (5) is not a prime ideal.

Proof. To show (5) is not prime, we will demonstrate that there are some $x, y \in \mathbb{Z}[i]$ such that $xy \in (5)$ but $x \notin (5)$ and $y \notin (5)$.

For this note we have the following product:

$$(2+i)(2-i) = 5 \tag{3}$$

So it follows $(2+i)(2-i) = 5$. However, we establish neither $2+i$ nor $2+i$ in (5) as we have the following:

$$\begin{aligned} 2+i = 5x &\Leftrightarrow \frac{2}{5} + \frac{i}{5} = x \\ 2-i = 5x &\Leftrightarrow \frac{2}{5} - \frac{i}{5} = x \end{aligned} \tag{4}$$

But neither $\frac{2}{5} + \frac{i}{5}$ nor $\frac{2}{5} - \frac{i}{5}$ lies in $\mathbb{Z}[i]$. In particular, we note we can formalize this notion by viewing these elements as laying in the field $\mathbb{Q}[i]$.

Specifically, we can appeal to the underlying multiplicative group structure of $\mathbb{Q}[i]$ (sans zero), which has that there are unique x that satisfy:

$$\begin{aligned} 2+i &= 5x \\ 2-i &= 5x \end{aligned} \tag{5}$$

Specifically, we note the unique solutions are $\frac{2}{5} + \frac{i}{5}$ and $\frac{2}{5} - \frac{i}{5}$ respectively.

Consequently there can be no solution to either laying in $\mathbb{Z}[i]$, as such a solution would also be a solution in $\mathbb{Q}[i]$, in which the unique solutions are explicitly not Gaussian integers.

Thus neither $2+i$ nor $2-i$ can be written as a multiple of 5, and so neither $2+i$ nor $2+i$ are in (5). It follows (5) is not prime. □

(b) Find an ideal I other than R and (5) such that $(5) \subseteq I$.

Proof. We claim $I = (2+i)$ suffices. Obviously, by the previous part we have $5 \in (2+i)$, which suffices to show that $(5) \subseteq (2+i)$.

Moreover, it is clear that $(2+i) \neq (5)$, as $2+i \in (2+i)$ but $2+i \notin (5)$, again by the previous part.

Lastly, to show $(2+i) \neq R$, we just note that $1 \notin (2+i)$ as $(2+i)$ is not unit in $\mathbb{Z}[i]$, in particular we can do the same argument in $\mathbb{Q}[i]$:

$$(2+i)^{-1} = \frac{2}{5} - \frac{i}{5} \tag{6}$$

But the latter term is not in $\mathbb{Z}[i]$, so there is no term $x \in \mathbb{Z}[i]$ such that we have $(2+i)x = 1$, as seen by appealing the exact same argument as the previous part.

Thus $(2+i)$ fulfills the desired properties. □

(c) More generally, suppose p is such that there is a solution to the equation $x^2 + 1 = 0$ in $\mathbb{Z}_p$. Prove that the principal ideal (p) is not prime.

Proof. Let $[\alpha]_p$ be a solution to $x^2 + 1$ in $\mathbb{Z}_p$, i.e.

$$[\alpha]_p^2 + [1]_p = [0]_p, \tag{7}$$

it t follows $\alpha^2 + 1 \equiv 0 \pmod{p}$, i.e. $\alpha^2 + 1 = pq$ for some $q \in \mathbb{Z}$. Factoring yields

$$(\alpha + i)(\alpha - i) = pq \tag{8}$$

And so $(\alpha + i)(\alpha - i) \in (p)$. However, we note neither $\alpha + i \in (p)$ nor $\alpha - i \in (p)$ as working over $\mathbb{Q}[i]$ we have

$$\begin{aligned} \alpha + i = px &\Leftrightarrow \frac{\alpha}{p} + \frac{i}{p} = x \\ \alpha - i = px &\Leftrightarrow \frac{\alpha}{p} - \frac{i}{p} = x \end{aligned} \tag{9}$$

and so appealing to the exact same argument as the previous two parts then, in particular as $\frac{1}{p} \notin \mathbb{Z}$, we note there can be no Gaussian integer solutions to x.

Thus neither $\alpha - i \in (p)$ nor $\alpha + i \in (p)$. Thus (p) is not prime. □

(d) On the other hand, prove that (3) *is* maximal.

Proof. I'm not sure there is a more streamlined way to do this then appealing to the argument in (e), so I just verify that there is no solution to $x^2 + 1 = 0$ in $\mathbb{Z}_3$.

In particular, we note:

$$\begin{aligned} 0^2 + 1 &\equiv 1 \pmod{3} \\ 1^2 + 1 &\equiv 2 \pmod{3} \\ 2^2 + 1 &\equiv 2 \pmod{3} \end{aligned} \tag{10}$$

Using (e) then, we note (3) in maximal in $\mathbb{Z}[i]$. □

(e) Suppose that p is any prime such that there is no solution to the equation $x^2+1=0$ in $\mathbb{Z}_p$. Prove that the ideal (3) is maximal.

Proof. Assume for the sake of contradiction (p) is not maximal, i.e.

$$(p) \subsetneq I \subsetneq R \tag{11}$$

For some ideal I. By assumption then, we can consider can consider some $a+bi \in I \backslash (p)$.

As $a+bi \notin (p)$, it must be that $p \nmid a$ or $p \nmid b$. Note then that as x^2+1 has no solutions over $\mathbb{Z}_p$ and is quadratic, it must be irreducible over $\mathbb{Z}_p[x]$.

In particular, if it were not irreducible, it would admit a factorization into linear polynomials which would assuredly admit solutions, contradicting that x^2+1 has no roots.

As $\mathbb{Z}_p$ is a field then, appealing to a result proven in class, we have that ${}^{\mathbb{Z}_p[x]}/_{(x^2+1)}$ is a field, given the irreducibility of x^2-1.

As ${}^{\mathbb{Z}_p[x]}/_{(x^2+1)}$ is "essentially" $\mathbb{Z}_p[x]$ collapsed onto x^2+1, we can view it as $\mathbb{Z}_p[x]$ with the additional rule that $x^2=-1$. Recalling then that $p \nmid a$ or $p \nmid b$, we have

$$[a]_p + [b]_p x \neq 0 \tag{12}$$

As $\mathbb{Z}_p[x]$ with $x^2=-1$ is a field then, $[a]_p+[b]_p x$ is a unit here, i.e. it admits an inverse $[a']_p + [b']_p x$. Thus

$$[a]_p + [b]_p x([a']_p + [b']_p x) = [aa'-bb'] + [ab'+ba']_p x = [1]_p \tag{13}$$

In particular then, it must be $[ab'+ba']_p = [0]_p$ and thus $[aa'-bb']_p = [1]_p$.

This is specifically that $ab'+ba' = mp$ and $aa'-bb' = 1+kp$ for $m,k \in \mathbb{Z}$. Back in $\mathbb{Z}[i]$ now, consider the multiplication

$$(a+bi)(a'+b'i) = (aa'-bb') + (ab'+ba')i \tag{14}$$

, where this product is in I given $a+bi \in I$. It follows

$$(a+bi)(a'+b'i) = (aa'-bb') + (ab'+ba')i = 1+kp+mpi = 1+p(k+mi) \in I \tag{15}$$

But obviously then $kp+mpi = p(k+mi) \in (p) \subsetneq I$, so using the properties of the ideal we have

$$1+p(k+mi) - p(k+mi) = 1 \in I \tag{16}$$

But this is a contradiction as then clearly I becomes the whole ring R, but we assumed $I \subsetneq R$. Thus (p) must be maximal. □

Exercise 4. Let $f \in \mathbb{Q}[x]$ given by $f = x^3 - 2$.

(a) Prove that f is irreducible, i.e. that there no do not exist polynomials $f_1, f_2 \in \mathbb{Q}[x]$ with $\deg f_1 = 1$ and $\deg f_2 = 2$ such that $f = f_1 f_2$.

Proof. Assume for the sake of contradiction f is not irreducible, i.e. it admits a factorization over $\mathbb{Q}[x]$ given by

$$(ax^2 + bx + c)(dx + e) \tag{17}$$

Where $a, b, c, d, e \in \mathbb{Q}$ with at least $a, d \neq 0$. Clearly $dx + e$ admits a root $\frac{-e}{d}$ as

$$d\Big(\frac{-e}{d}\Big) + e = -e + e = 0 \tag{18}$$

So clearly then $\frac{-e}{d}$ is also a root of f, i.e.

$$\Big(\frac{-e}{d}\Big)^3 = 2 \tag{19}$$

Note here it must be $\frac{-e}{d}$ is positive as x^3 preserves sign. Taking the (principal) cube root the has $\frac{-e}{d} = \sqrt[3]{2}$, but this is a contradiction as $\sqrt[3]{2}$ is irrational and $\frac{-e}{d} \in \mathbb{Q}$.

It follows f must be irreducible. □

(b) Conclude that $\mathbb{Q}[x]/(f)$ is a field.

Proof. This follows immediately from a theorem we proved in class. In particular, as $\mathbb{Q}$ is a field and f is non-constant irreducible in $\mathbb{Q}[x]$, it follows this is a field. □

(c) Use the polynomial division algorithm to find polynomials $q, r \in \mathbb{Q}[x]$ such that $x^4 + x + 1 = qf + r$, when $\deg(r) < \deg(f)$. Observe that $r(\sqrt[3]{2}) = \sqrt[3]{2}^4 + \sqrt[3]{2} + 1$.

Proof. We perform the computtion utilizing the division algorithm:

$$\begin{array}{r} x \\ x^3 - 2\overline{\smash{)}\,x^4 + x + 1} \\ -\quad (x^4 - 2x) \\ \hline 3x + 1 \end{array} \tag{20}$$

Thus $x^4 + x + 1 = (x)(x^3 - 2) + (3x + 1)$. Here $q = x$ and $r = 3x + 1$, where we of course have $\deg(r) < \deg(f)$. We note then:

$$r(\sqrt[3]{2}) = 3(\sqrt[3]{2}) + 1 \tag{21}$$

We want to show $r(\sqrt[3]{2}) = \sqrt[3]{2}^4 + \sqrt[3]{2} + 1$, so we would like $\sqrt[3]{2}^4 + \sqrt[3]{2} = 3(\sqrt[3]{2})$. For this, just note

$$2\sqrt[3]{2} = \sqrt[3]{2}^4 \Leftrightarrow 2^1 2^{\frac{1}{3}} = 2^{\frac{4}{3}} \Leftrightarrow 2^{\frac{4}{3}} = 2^{\frac{4}{3}} \tag{22}$$

Which verifies (21). □

(d) Use the polynomial Euclidean algorithm to find explicit polynomials $A, B \in \mathbb{Q}[x]$ such that $A \cdot (3x+1) + B \cdot f = 1$.

Proof. We first apply the division algorithm to $x^3 - 2$ and $3x+1$, which has

$$x^3 - 2 = \Big(\frac{x^2}{3} - \frac{x}{9} + \frac{1}{27}\Big)(3x+1) + \Big(\frac{-55}{27}\Big), \tag{23}$$

and so we can rearrange to get

$$\frac{55}{27} = \Big(\frac{x^2}{3} - \frac{x}{9} + \frac{1}{27}\Big)(3x+1) - (x^3 - 2), \tag{24}$$

which finally has

$$1 = \frac{27}{55}\Big(\frac{x^2}{3} - \frac{x}{9} + \frac{1}{27}\Big)(3x+1) - \frac{27}{55}(x^3 - 2) \tag{25}$$

Expanding then, we can get the desired polynomials are $A = \frac{9x^2}{55} - \frac{3x}{55} + \frac{1}{55}$ and $B = -\frac{27}{55}$. □

(e) Express $\frac{1}{3\sqrt[3]{2}+1}$ in the form $a + b\sqrt[3]{2} + c\sqrt[3]{2}$, for $a, b, c \in \mathbb{Q}$.

Proof. This is just a routine application of the last part, plugging into A.

Doing this yields:

$$\frac{1}{3\sqrt[3]{2}+1} = \frac{9}{55}\sqrt[3]{4} - \frac{3}{55}\sqrt[3]{2} + \frac{1}{55} \tag{26}$$

Which is exactly what is desired. □