HOMEWORK-2

SIDDHANT CHAUDHARY
BMC201953

Norm in Gaussian Integers. For any $a + ib \in \mathbb{Z}[i]$, define

$$N(a + ib) := (a + ib)(a - ib) = a^2 + b^2$$

Then, we see that $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$. Moreover, observe the following chain of equalities.

$$\begin{aligned} N[(a + ib)(c + id)] &= N[ac - bd + i(ad + bc)] \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= N(a + ib)N(c + id) \end{aligned}$$

and hence N is a multiplicative function. We can easily extend this norm to $\mathbb{Q}[i]$ by defining

$$N(p + iq) = p^2 + q^2$$

where $p, q \in \mathbb{Q}$. By the same proof, this norm will also be multiplicative.

Theorem 0.1. *$\mathbb{Z}[i]$ is a Euclidean Domain with respect to the above norm. More specifically, let $a, b \in \mathbb{Z}[i]$ with $a \neq 0$. Then, there are $q, r \in \mathbb{Z}[i]$ such that*

$$b = aq + r$$

and

$$0 \leq N(r) \leq \frac{N(a)}{2}$$

Proof. The idea is simple. Suppose $b = c + id$ and $a = e + if$. Then, using multiplication by conjugates, write the fraction

$$\frac{b}{a} = \frac{b\overline{a}}{N(a)} = g + ih$$

where $g, h \in \mathbb{Q}$ are *rational*. Now, let p be the closest integer to g and let q be the closest integer to h. Then, we know that

$$|g - p|, |h - q| \leq \frac{1}{2}$$

So, our candidate is $q = p + iq$. Now, put

$$r = b - aq$$

Date: November 2020.

and we see that $b = aq + r$. Now, we have the following.

$$\begin{aligned} r &= b - aq \\ &= a(g + ih) - a(p + iq) \\ &= a[(g - p) + i(h - q)] \end{aligned}$$

and by the multiplicativity of the norm in $\mathbb{Q}[i]$, this implies

$$\begin{aligned} N(r) &= N(a)N[(g - p) + i(h - q)] \\ &= N(a)[(g - p)^2 + (h - q)^2] \\ &\leq \frac{N(a)}{2} \end{aligned}$$

and this completes the proof. ∎

Remark 0.1.1. In the following problems, I will heavily use the fact that

$$\frac{R/(a)}{(\bar{b})} \cong \frac{R}{(a, b)} \cong \frac{R/(b)}{(\bar{a})}$$

which was proven in Lecture 4 as a consequence of the **Third Isomorphism Theorem**. So instead of mentioning this every time, I will just say: *by the* **Third Isomorphism Theorem**.

11. Artin Chapter 11: 4.3 b and e (Here take *identify* to mean *find cardinality and whether the ring is a field/integral domain*. You can say more if you like.)

Solution. **(b)** $\mathbb{Z}[i]/(2 + i)$. By **Theorem** 0.1, we know that $\mathbb{Z}[i]$ is a PID as it is a Euclidean Domain. We first show that $(2 + i)$ is a *maximal ideal* in $\mathbb{Z}[i]$. To see this, suppose $z \in \mathbb{Z}[i]$ is any factor of $2 + i$. By the multiplicativity of the norm, it follows that

$$N(z) | N(2 + i) = 1^2 + 2^2 = 5$$

Since 5 is a prime in $\mathbb{Z}$, it follows that $N(z) = 1$ or $N(z) = 5$. Now again by the multiplicativity of the norm, it is easy to see that an element $z \in \mathbb{Z}[i]$ is a unit iff. $N(z) = 1$. So, the above shows that any factor of $2 + i$ is either a unit or an associate of $2 + i$, implying that $2 + i$ is an irreducible element. So, $(2 + i)$ is a maximal ideal, and hence $\mathbb{Z}[i]/(2 + i)$ is a *field*.

We now find the cardinality of this field, and we again use **Theorem** 0.1. Observe that $N(2+i) = 5$, and hence any *remainder* modulo $2+i$ has norm atmost 2 (here we use the inequality $N(r) \leq 5/2$). Now the only elements of $\mathbb{Z}[i]$ with norm atmost 2 are

$$0, 1, -1, i, -i, 1 + i, 1 - i, -1 + i, -1 - i$$

It can be easily seen that this list modulo $(2 + i)$ can further be reduced to the list

$$0, 1, -1, i, -i$$

because each of the elements $1 + i, 1 - i, -1 + i$ and $-1 - i$ are equal to of the elements in the above list modulo $(2 + i)$. Finally, note that none of the elements in the list

$$0, 1, -1, i, -i$$

are equal modulo $(2 + i)$ which is easy to see by the multiplicativity of the norm, and hence it follows that

$$\mathbb{Z}[i]/(2 + i) = \{\overline{0}, \overline{1}, \overline{-1}, \overline{i}, \overline{-i}\}$$

so that $|\mathbb{Z}[i]/(2+i)| = 5$.
(e) $\mathbb{Z}[x]/(x^2+3,5)$. As covered in lecture 4, we can use the **Third Isomorphism Theorem** here. Observe that $(x^2+3,5)$ is an ideal containing (5). So, we see that

$$\frac{\mathbb{Z}[x]}{(x^2+3,5)} \cong \frac{\mathbb{Z}[x]/(5)}{(x^2+3,5)/(5)}$$

Observe that $\mathbb{Z}[x]/(5) \cong \mathbb{F}_5[x]$, as we proved in class. Moreover, the quotient $(x^2+3,5)/(5)$ will just be generated by the element $\overline{x^2+3}$ (where the bar represents passing to the quotient). So, we see that

$$\frac{\mathbb{Z}[x]}{(x^2+3,5)} \cong \frac{\mathbb{Z}[x]/(5)}{(x^2+3,5)/(5)} \cong \frac{\mathbb{F}_5[x]}{(x^2+3)}$$

Because $\mathbb{F}_5$ is a *field*, $\mathbb{F}_5[x]$ is a PID. Now consider the ideal (x^2+3). Note that any non-trivial factor of x^2+3 in $\mathbb{F}_5[x]$ must be a linear polynomial, which is equivalent to saying that x^2+3 has a root in $\mathbb{F}_5$. But this is clearly not the case. So, it follows that x^2+3 is an *irreducible* in $\mathbb{F}_5[x]$, and hence this implies that (x^2+3) is a *maximal ideal* in this ring (and this is where $\mathbb{F}_5[x]$ being a PID helps). Now, $\mathbb{F}_5[x]/(x^2+3)$ is a *field*. Finding the cardinality of this field is not hard. By **Euclidean Division**, *any* polynomial in $\mathbb{F}_5[x]$ is equal to some polynomial of degree *atmost* 1 modulo (x^2+3). So, this means

$$\mathbb{F}_5[x]/(x^2+3) = \{\overline{ax+b} \mid a,b \in \mathbb{F}_5\}$$

where again the bar represents the image under the quotient. It is also clear that $\overline{a_1x+b_1} \neq \overline{a_2x+b_2}$ if $(a_1,b_1) \neq (a_2,b_2)$, because x^2+3 is a polynomial of degree 2, and hence cannot divide any polynomial of lesser degree. So, there are $5 \times 5 = 25$ choices for a, b above, showing that

$$|\mathbb{F}_5[x]/(x^2+3)| = 25$$

$\blacksquare$

12. Artin Chapter 11: 5.3.

Solution. We will describe the ring obtained by adjoining an inverse of 2 to $\mathbb{Z}/12\mathbb{Z}$. This is equivalent to describing the ring

$$\frac{\mathbb{Z}/12\mathbb{Z}[x]}{(2x-1)}$$

where the inverse of 2 will be the element $\overline{x}$, where as usual the bar represents passing to the quotient.

Now by the **Third Isomorphism Theorem**, we see that

$$\frac{\mathbb{Z}[x]}{(12,2x-1)} \cong \frac{\mathbb{Z}/12\mathbb{Z}[x]}{(2x-1)}$$

where on the right hand side, $2x-1 \in \mathbb{Z}/12\mathbb{Z}[x]$ and on the left hand side, $2x-1 \in \mathbb{Z}[x]$. This is just a reiteration of the fact that we can introduce new relations in any order, which we covered in Lecture 4. So, it is enough to describe the ring $\mathbb{Z}[x]/(12,2x-1)$.

Now, observe that

$$12x - 6(2x-1) = 6$$

This means that $(12,2x-1) = (6,2x-1)$, because $6|12$. Again, note that

$$6x - 3(2x-1) = 3$$

and hence $(6, 2x-1) = (3, 2x-1)$ because $3|6$. So, we have

$$\frac{\mathbb{Z}[x]}{(12, 2x-1)} = \frac{\mathbb{Z}[x]}{(3, 2x-1)}$$

The good thing now is that 3 is a prime in $\mathbb{Z}$. Again by the **Third Isomorphism Theorem**, we see that

$$\frac{\mathbb{Z}[x]}{(12, 2x-1)} = \frac{\mathbb{Z}[x]}{(3, 2x-1)} \cong \frac{\mathbb{F}_3[x]}{(2x-1)}$$

where in the extreme right hand side, $2x-1 \in \mathbb{F}_3[x]$. Now, consider the evaluation map $\mathbb{F}_3[x] \xrightarrow{\text{eval}_{2^{-1}}} \mathbb{F}_3$. This map is clearly surjective, and the kernel of this map is $(2x-1)$. So, it follows that

$$\frac{\mathbb{F}_3[x]}{(2x-1)} \cong \mathbb{F}_3$$

So, it follows that adjoining an inverse of 2 to $\mathbb{Z}/12\mathbb{Z}$ gives us $\mathbb{F}_3$. ■

13. Artin Chapter 11: 5.4 a and b

Solution. Consider the ring $\mathbb{Z}$. We will describe the ring obtained by adjoining an element α to $\mathbb{Z}$ with the given relations.
(a) $2\alpha = 6, 6\alpha = 15$. This is equivalent to describing the ring

$$\frac{\mathbb{Z}[x]}{(2x-6, 6x-15)}$$

First observe that

$$6x - 15 - 3(2x-6) = 3$$

and because $3|6x-15$, it follows that $(2x-6, 6x-15) = (2x-6, 3)$. As usual, by the **Third Isomorphism Theorem**, we see that

$$\frac{\mathbb{Z}[x]}{(2x-6, 6x-15)} = \frac{\mathbb{Z}[x]}{(2x-6, 3)} \cong \frac{\mathbb{F}_3[x]}{2x}$$

and this is because when we quotient $\mathbb{Z}[x]$ by the ideal (3), the image of $2x-6$ is $2x \in \mathbb{F}_3[x]$. Again, consider the evaluation map $\mathbb{F}_3[x] \xrightarrow{\text{eval}_0} \mathbb{F}_3$, which is a surjective map and its kernel is $(x) = (2x)$. So we see that

$$\frac{\mathbb{F}_3[x]}{2x} \cong \mathbb{F}_3$$

and this is the ring we obtain.
(b) $2\alpha - 6 = 0, \alpha - 10 = 0$. This is equivalent to describing the ring

$$\frac{\mathbb{Z}[x]}{(2x-6, x-10)}$$

Consider the evaluation map $\mathbb{Z}[x] \xrightarrow{\text{eval}_{10}} \mathbb{Z}$ which is clearly surjective and its kernel is $x - 10$. So, we see that

$$\frac{\mathbb{Z}[x]}{(x-10)} \cong \mathbb{Z}$$

Moreover, under this map, $2x-6$ is mapped to $20-6=14$. So again, by the **Third Isomorphism Theorem**, we see that

$$\frac{\mathbb{Z}[x]}{(2x-6, x-10)} \cong \frac{\mathbb{Z}}{(14)} \cong \mathbb{Z}/14\mathbb{Z}$$

and hence this is the ring obtained. ■

14. Artin Chapter 11: 5.5 (Hint: consider maximal ideals.)

Solution. Yes, there is such a field F, but such a field F must have characteristic 2. First, we prove that any field whose characteristic is *not* 2 cannot satisfy the above isomorphism.

Suppose there is a field F such that

$$F[x]/(x^2) \cong F[x]/(x^2-1)$$

So, the *total number* of ideals in both the rings given above must be the same. By the **Correspondence Theorem**, there is an inclusion preserving bijection between ideals of $F[x]/(x^2)$ and ideals of $F[x]$ containing (x^2), and a similar statement holds for $F[x]/(x^2-1)$. Also, we know that $F[x]$ is a PID (infact a Euclidean Domain) and hence every ideal of $F[x]$ is principal.
Now, suppose $(d(x))$ is an ideal of $F[x]$ containing (x^2) for some $d(x) \in F[x]$. We immediately see that $\deg d(x) \leq 2$. Now, if $d(x)$ has degree 2, i.e

$$d(x) = ax^2 + bx + c$$

then there is some $s \neq 0$ in F such that

$$x^2 = s \cdot (ax^2 + bx + c) = sax^2 + sbx + sc$$

implying that $b = c = 0$ and $s = a^{-1}$. So, we see that $d(x) = ax^2$, and because a is a unit, we have $(d(x)) = (x^2)$. Next, suppose $d(x)$ has degree 1, i.e

$$d(x) = ax + b$$

Then, there are $p, q \in F$ with $p \neq 0$ such that

$$x^2 = (px+q)(ax+b)$$

and this immediately implies that $ap = 1$, $b + q = 0$ and $bq = 0$, which in turn implies that $b = q = 0$. In that case, we have $d(x) = ax$, and hence $(d(x)) = (x)$. Finally, if $d(x)$ has degree 0, then $d(x)$ must be a unit in $F[x]$, and in that case $(d(x)) = F[x]$. So, this shows that the only ideals of $F[x]$ containing (x^2) are $F[x]$, (x) and (x^2), and hence the ring $F[x]/(x^2)$ has exactly *three* ideals.

However, observe that the ideals $F[x]$, $(x-1)$, $(x+1)$ and (x^2-1) are all *distinct* ideals containing (x^2-1) (because F does not have characteristic 2, the ideals $(x-1)$ and $(x+1)$ are distinct because $x-1, x+1$ are not associates). So, $F[x]/(x^2-1)$ has atleast four ideals. But, this contradicts the fact that $F[x]/(x^2) \cong F[x]/(x^2-1)$, and hence there is no such field F.

Now, consider $F = \mathbb{Z}/2\mathbb{Z}$, which has characteristic 2. In this case, observe that

$$x^2 - 1 = (x-1)(x+1) = (x+1)^2$$

and hence we want to show that

$$F[x]/(x^2) \cong F[x]/((x+1)^2)$$

First, consider the unique homomorphism $F[x] \xrightarrow{\varphi} F[x]$ such that $x \xrightarrow{\varphi} x+1$. φ is clearly an isomorphism, because it has an inverse map, namely the unique homomorphism $F[x] \xrightarrow{\Phi} F[x]$ with $x \xrightarrow{\Phi} x-1$ (this is very similar to what we did in HW-1). Now, consider the natural projection map

$$F[x] \xrightarrow{\pi} F[x]/((x+1)^2)$$

which is a surjective homomorphism, and Ker $\pi = (x+1)^2$. Composing this with the map φ, we get the map $\pi \circ \varphi$ which can be represented as

$$F[x] \xrightarrow{\varphi} F[x] \xrightarrow{\pi} F[x]/((x+1)^2)$$

Because both φ and π are surjective, we see that $\pi \circ \varphi$ is also surjective. So, by the **First Isomorphism Theorem**, we see that

$$F[x]/\text{Ker } (\pi \circ \varphi) \cong F[x]/((x+1)^2)$$

Now, we will show that Ker $(\pi \circ \varphi) = (x^2)$, and that will finish our proof.

It is easy to see that Ker $\pi \circ \varphi = \varphi^{-1}[((x+1)^2)]$. So, it is enough to show that $\varphi^{-1}[((x+1)^2)] = (x^2)$. First, suppose $p(x) \in (x^2)$, so that $p(x) = x^2 d(x)$ for some $d(x) \in F[x]$. In that case, we have

$$\varphi(p(x)) = (x+1)^2 d(x+1) \in ((x+1)^2)$$

and hence $(x^2) \subseteq \varphi^{-1}[((x+1)^2)]$. Conversely, suppose $p(x) \in F[x]$ is such that $\varphi(p(x)) \in ((x+1)^2)$, i.e $p(x+1) = (x+1)^2 d(x)$ for some $d(x) \in F[x]$. Applying the map Φ (the inverse of φ) to both sides, we see that

$$p(x) = (x-1+1)^2 d(x-1) \in (x^2)$$

This completes the proof. ■

15. Artin Chapter 11: 8.2 b, c and d, also identify which of the given rings are fields.

Solution. First, because $\mathbb{R}$ is a field, we know that $\mathbb{R}[x]$ is a PID.
(b) $\mathbb{R}[x]/(x^2)$. Observe that (x^2) is *not* a maximal ideal in $\mathbb{R}[x]$, since $(x^2) \subset (x)$, hence $\mathbb{R}[x]/(x^2)$ is *not* a field. Now by the **Correspondence Theorem**, there is an inclusion preserving bijection between ideals of $\mathbb{R}[x]/(x^2)$ and ideals of $\mathbb{R}[x]$ containing (x^2). It is easy to see that the only ideals of $\mathbb{R}[x]$ containing (x^2) are $\mathbb{R}[x]$, (x) and (x^2) (the fact that $\mathbb{R}[x]$ is a PID comes in handy here). So, it follows that $(x)/(x^2)$, which is an ideal of $\mathbb{R}[x]/(x^2)$, is the only maximal ideal of $\mathbb{R}[x]/(x^2)$.
(c) $\mathbb{R}[x]/(x^2-3x+2)$. We see that

$$x^2 - 3x + 2 = (x-1)(x-2)$$

and hence (x^2-3x+2) is *not* a maximal ideal in $\mathbb{R}[x]$, and so this ring is *not* a field. We again rely on the **Correspondence Theorem**. Observe that the only ideals of $\mathbb{R}[x]$ which contain (x^2-3x+2) are $\mathbb{R}[x]$, $(x-1)$, $(x-2)$ and (x^2-3x+2). The ideals $(x-1)$ and $(x-2)$ are distinct since these two linear polynomials are *not* associates. So, it follows that $\mathbb{R}[x]/(x^2-3x+2)$ has *two* maximal ideals, namely $(x-1)/(x^2-3x+2)$ and $(x-2)/(x^2-3x+2)$.
(d) $\mathbb{R}[x]/(x^2+x+1)$. We will show that (x^2+x+1) is a *maximal ideal* in $\mathbb{R}[x]$, and hence $\mathbb{R}[x]/(x^2+x+1)$ will be a *field*. Now any non-trivial factor of x^2+x+1 must be a *linear polynomial*, but that would mean that x^2+x+1 has a root in $\mathbb{R}[x]$. But it is easily seen that this is not true by the quadratic formula. So, (x^2+x+1) is a maximal ideal, and hence $R[x]/(x^2+x+1)$ is a field, meaning that the only maximal ideal in this field is the 0 ideal. ■

16. Artin Chapter 11: Suppose you are given a finite field E. Show that $|E| = p^n$ for a prime number p. (Hints: **(i)** First identify p from F using the first isomorphism theorem. Which other ring should you use? **(ii)** If a field F is subfield of a ring E, then note that E is in particular a vector space over F with the given operations. We will use this repeatedly, especially when E is a field as well. In particular we can consider dimension of E over F, which we call the degree of E over F, denoted $[E : F]$.)

Solution. Consider the characteristic map $\mathbb{Z} \xrightarrow{\text{char}} E$, and let Ker char $= p\mathbb{Z}$ for some $p \in \mathbb{Z}$. Because E is a finite field, $p = 0$ is not possible (because $\mathbb{Z}$ is an infinite set). Moreover, we know that p is the characteristic of the field E, and since it is non-zero, it must be a prime (because E is an integral domain). By the **First Isomorphism Theorem**, we see that

$$\mathbb{Z}/(p\mathbb{Z}) \cong \text{char}(\mathbb{Z})$$

and hence E contains $F = \mathbb{Z}/p\mathbb{Z}$ as a *subfield*. Because E is also a field, let us prove that E is a vector space over F, where the action of F on E is simply left-multiplication. We already know that E is an (additive) abelian group, so we only need to check the compatibility of the action of F over E. But this is an immediate consequence of the distributive law in E. So E is indeed a vector space over F.

Now, suppose the dimension of E as a vector space is n. By basic vector space theory we see that

$$E \cong F^n := F \times F \times \ldots \times F$$

where the above isomorphism is a *vector space isomorphism* and since $|F| = p$, we see that $|E| = |p|^n$. This completes the proof. ■