HOMEWORK-3

SIDDHANT CHAUDHARY
BMC201953

17. Suppose that R is an integral domain containing a field F such that R is a finite dimensional vector space over F. Show that R itself must be a field. Hint: Imitate the proof of Artin Chapter 11 problem 7.1 that we did in Lecture 2. First show that the appropriate map is linear as a map of F-vector spaces.

Solution. It is enough to show that every non-zero element of R is a unit, since R is already given to be an integral domain. Suppose

$$\dim_F R = n$$

Now suppose $x \in R$ such that $x \neq 0$. First, we claim that x is *not* nilpotent. For the sake of contradiction, suppose x *is* nilpotent. Then, the set

$$\{k > 0 \mid x^k = 0\}$$

is non-empty, and hence contains a least element by the **Well-Ordering Principle**. Since $x \neq 0$, this least element is > 1. If this least element is k, then we have

$$0 = x^k = x \cdot x^{k-1}$$

which contradicts the fact that R is an integral domain. So, x is *not* nilpotent.

Now consider the $n+1$ non-zero elements

$$1, x, x^2, ..., x^n$$

which must be *linearly dependent*. So, there are $a_0, a_1, ..., a_n \in F$ not all zero such that

$$a_0 + a_1 x + ... + a_n x^n = 0$$

Let $0 \leq k < n$ be the smallest index for which $a_k \neq 0$ ($k < n$ because R is an integral domain and $x \neq 0$). Moreover, observe that atleast two of the a_i's must be non-zero because $x \neq 0$ and R is an integral domain. So, the above equation reads

$$a_k x^k + ... + a_n x^n = 0$$

which can be written as

$$x^k(a_k + ... + a_n x^{n-k}) = 0$$

and hence we have

$$a_k + ... + a_n x^{n-k} = 0$$

So, we have

$$a_k = -a_{k+1}x - ... - a_n x^{n-k} = x(-a_{k+1} - ... - a_n x^{n-k-1})$$

and multiplying both sides by a_k^{-1}, we see that x is a unit. This completes our proof and shows that R is indeed a field. ■

Date: November 2020.

18. Chinese Remainder Theorem. Let I and J be ideals of a ring R. Suppose $I + J = R$ (we say in this case that I and J are coprime). Show that $R/? \cong R/I \times R/J$. Identify what $?$ is and identify the idempotents corresponding to the product decomposition (compare Artin Chapter 11 problem 6.8. The ideal ? measures the non-uniqueness of solutions).

Solution. Let I_1, I_2 be ideals of a ring R such that

$$I_1 + I_2 = R$$

Then it is true that

$$I_1 I_2 = I_1 \cap I_2$$

Moreover the homomorphism $R \xrightarrow{\varphi} R/I_1 \times R/I_2$ given by

$$\varphi(s) = (s + I_1, s + I_2)$$

is *surjective*, and hence by the **First Isomorphism Theorem** it follows that

$$R/(I_1 I_2) = R/(I_1 \cap I_2) \cong R/I_1 \times R/I_2$$

So, it follows that

$$? = I_1 \cap I_2 = I_1 I_2$$

The claim about the intersection of the ideals being equal to their product is proven in part **(i)** of problem **19.** below. So I will only prove the *surjectivity* of the map in question here.

As a first observation, the fact that φ is indeed a ring homomorphism is clear because each quotient map is a ring homomorphism. Now, let $(a_1 + I_1, a_2 + I_2) \in R/I_1 \times R/I_2$ be *any* element. We need to show that there is some element $s \in R$ such that

$$(s + I_1, s + I_2) = (a_1 + I_1, a_2 + I_2)$$

which is equivalent to showing that

$$(\dagger) \qquad \begin{aligned} s &\equiv a_1 (\text{mod } I_1) \\ s &\equiv a_2 (\text{mod } I_2) \end{aligned}$$

We will first find elements $s_1, s_2 \in R$ such that

$$\begin{aligned} s_1 &= 1 (\text{mod } I_1) \quad , \quad s_1 = 0 (\text{mod } I_2) \\ s_2 &= 0 (\text{mod } I_1) \quad , \quad s_2 = 1 (\text{mod } I_2) \end{aligned}$$

To do this, observe that we have

$$I_1 + I_2 = R$$

This means that there are $x \in I_1, y \in I_2$ such that $x + y = 1$. I claim that $s_1 = y$ and $s_2 = x$ are the required elements, and this is immediate by the fact that $x + y = 1$.

Finally having found s_1, s_2, we put

$$s = a_1 s_1 + a_2 s_2$$

It is then easy to see that s satisfies the system of equations ($\dagger$). This completes the proof of *surjectivity* of the given map, and hence the proof of CRT.

Now by the CRT we know that if I, J are coprime ideals then

$$R/(IJ) = R/(I \cap J) \cong R/I \times R/J$$

Let us identify the idempotents corresponding to this product decomposition. From Lecture 5, we know that the idempotents corresponding to the product

$R/I \times R/J$ are $(1_I, 0)$ and $(0, 1_J)$, where $1_I \in R/I$ and $1_J \in R/J$ are the respective identity elements. To find these, let $x \in I, y \in J$ be elements of R with $x + y = 1$. Then observe that $x = 1$(mod J), and hence $x + J$ is the identity element of R/J. Similarly, $y + I$ is the identity element of R/I. So, the idempotents are $(y + I, 0)$ and $(0, x + J)$. ■

19. Suppose I and J are coprime ideals of a ring R.
(i) Show that if $I + J = R$ then $IJ = I \cap J$. You may refer to problem **18.**

Solution. Let I_1, I_2 be coprime ideals of a ring R. Here we will show that

$$I_1 \cdot I_2 = I_1 \cap I_2$$

Because I_1, I_2 are coprime, there are elements $x \in I_1, y \in I_2$ such that $x + y = 1$. First, suppose $a \in I_1 \cap I_2$. Then, we can write

$$ax + ay = a$$

and the LHS is clearly in $I_1 \cdot I_2$, and hence $a \in I_1 \cdot I_2$. This shows $I_1 \cap I_2 \subseteq I_1 \cdot I_2$. Conversely, suppose $a \in I_1 \cdot I_2$, and hence

$$a = \sum_{i=1}^{n} a_i b_i$$

where $a_i \in I_1, b_i \in I_2$ for each i and $n \in \mathbb{N}$. Because $a_i \in I_1$ for each i and because I_1 is an *ideal*, it follows that $a_i b_i \in I_1$ for each i, and hence $a \in I_1$. Similarly, it can be shown that $a \in I_2$, so that $a \in I_1 \cap I_2$, and hence $I_1 \cdot I_2 \subseteq I_1 \cap I_2$. This completes the proof. ■

(ii) For principal ideals in a domain show that a sort of converse holds: if $aR \cap bR = abR$ then gcd(a, b) exists and is 1. Deduce that if R is a PID, then converse to **(i)** is true.

Solution. Let a, b be non-zero elements of R such that $aR \cap bR = abR$. We will show that gcd(a, b) exists and is equal to 1. To show that gcd(a, b) is 1, it is enough to show that any common divisor of a and b must be a unit. For the sake of contradiction, suppose d is a non-unit common divisor of a, b. So, we have that

$$a = k_1 d$$
$$b = k_2 d$$

for some $k_1, k_2 \in R$. Now consider the element $k_1 k_2 d$. Clearly, this is a common multiple of a, b and hence lies in the intersection $aR \cap bR$. So, we see that

$$k_1 k_2 d = mab$$

for some $m \in R$. This is the same as the equation

$$k_2 a = mab$$

Since $a \neq 0$ and R is an integral domain, we can cancel a from either side of the equation to get

$$k_2 = mb$$

Substituting in the original equation, we get

$$b = mbd$$

and again since $b \neq 0$, cancelling it from both sides we get

$$1 = md$$

which contradicts that d is *not* a unit. So, every common factor of a, b must be a unit, and hence gcd(a, b) exists and is equal to 1.

Now suppose R is a PID, and we show that the converse to **(i)** will hold. So let I, J be non-zero ideals of R such that $IJ = I \cap J$. Also, suppose $I = aR, J = bR$, and this equation will mean

$$aR \cap bR = abR$$

Applying the result we just proved, we see that gcd$(a, b) = 1$. However, we know that $(a, b) = (d)$ for some $d \in R$, and hence it follows that d must be a unit. This implies that $aR + bR = I + J = R$, and this proves the converse. ■

(iii) In general converse to **(i)** is not true. Give an example in $\mathbb{Z}[x]$ (which even has unique factorization into primes, as we will see).

Solution. The counterexample is easy to give. Let $I = (2)$ and let $J = (3x)$, where $R = \mathbb{Z}[x]$. Observe that I is the set of all polynomials in $\mathbb{Z}[x]$ with even coefficients, and J is the set of all polynomials with zero constant term and such that each coefficient is a multiple of 3. It then immediately follows that

$$I \cap J = (6x) = I \cdot J$$

However, we claim that $I + J \neq R$. For the sake of contradiction, suppose $I + J = R$, which means that $(2, 3x) = R$. This would imply that 1 can be written as a linear combination of 2 and $3x$, i.e

$$1 = 2p(x) + q(x)3x$$

But this is a contraidiction; observe that $2p(x)$ is a polynomial with even coefficients, and $q(x)3x$ has no constant term. So, $I + J \neq R$ and this is the required counterexample. ■

20. Artin Chapter 11: M.4 (Do both parts but submit only part a.)

Solution. In this exercise we will classify rings that satisfy a certain criterion.
(a) Rings that contain $\mathbb{C}$ and have dimension 2 as a vector space over $\mathbb{C}$. Let R be such a ring. Because R contains $\mathbb{C}$, there is an inclusion $\mathbb{C} \hookrightarrow R$, which we will use. First we choose a basis of R. So let $\{1, r\}$ be a basis of R, and clearly $r \in R - \mathbb{C}$, because all elements of $\mathbb{C}$ are $\mathbb{C}$ multiples of 1. Now, consider the unique ring homomorphism $\mathbb{C}[x] \xrightarrow{\varphi} R$ which restricts to the inclusion on $\mathbb{C}$ and maps $x \mapsto r$. Since $\mathbb{C}[x]$ is a PID, Ker $\varphi = (f(x))$ for some polynomial $f(x) \in \mathbb{C}[x]$. By the **First Isomorphism Theorem**, we have

$$R \cong \frac{\mathbb{C}[x]}{(f(x))}$$

Note that the above isomorphism also gives us a *vector space isomorphism*. Now we know that $\mathbb{C}[x]/(f(x))$ is a $\mathbb{C}$-vector space of dimension n, where $n =$ deg$(f(x))$ (this was proven in Lecture 5). Since dim $R = 2$, we must have that deg$(f(x)) = 2$, i.e $f(x)$ is a *quadratic polynomial*.

Now, we know that $\mathbb{C}$ is algebraically closed, and hence every polynomial completely factors into linear factors in $\mathbb{C}[x]$. Now there are two cases to handle.

(1) In the first case, $f(x) = a(x - c)^2$ for some $c \in \mathbb{R}$ and $a \neq 0$, i.e f has a double root in $\mathbb{C}$. So, we see that $(f(x)) = ((x - c)^2)$. Now, it is not hard to see that the quotient $\mathbb{C}[x]/((x - c)^2)$ is isomorphic to the quotient

$\mathbb{C}[x]/(x^2)$; consider the map $\mathbb{C}[x] \xrightarrow{\Psi} \mathbb{C}[x]$ given by $\Psi(x) = x - c$. Compose this with the quotient map: $\mathbb{C}[x] \xrightarrow{\Psi} \mathbb{C}[x] \xrightarrow{\pi} \mathbb{C}[x]/((x-c)^2)$, and from here the argument is very similar to what we did in HW-2 problem **14.** So, in this case we see that $R \cong \mathbb{C}[x]/((x-c)^2) \cong \mathbb{C}[x]/(x^2)$.

(2) In the second case, $f(x) = a(x-c_1)(x-c_2)$ where $c_1 \neq c_2$ and $a \neq 0$, i.e f has two distinct roots in $\mathbb{C}$. So we observe that $(f(x)) = ((x-c_1)(x-c_2))$. Now, consider the two ideals $(x-c_1)$ and $(x-c_2)$. We have

$$(x-c_2) - (x-c_1) = c_1 - c_2 \neq 0$$

and hence multiplying by $(c_1 - c_2)^{-1}$ on both sides, we see that the ideals $(x-c_1), (x-c_2)$ are coprime. Note that $((x-c_1)(x-c_2)) = (x-c_1)\cdot(x-c_2)$ (product of ideals), which is immediate. So by the CRT which is proven in problem **18.**, we see that

$$\frac{\mathbb{C}[x]}{(f(x))} = \frac{\mathbb{C}[x]}{((x-c_1)(x-c_2))} = \frac{\mathbb{C}[x]}{(x-c_1)\cdot(x-c_2)} \cong \frac{\mathbb{C}[x]}{(x-c_1)} \times \frac{\mathbb{C}[x]}{(x-c_2)}$$

Moreover, both of the rings $\mathbb{C}[x]/(x-c_1)$ and $\mathbb{C}[x]/(x-c_2)$ are isomorphic to $\mathbb{C}$ via the evaluation maps at c_1 and c_2 respectively. So in this case, we see that $R \cong \mathbb{C}^2$.

So the only rings having this property are $\mathbb{C}^2$ and $\mathbb{C}[x]/(x^2)$. ■

21. Artin Chapter 12: 1.5.

Solution. Suppose $a, b \in \mathbb{Z}$ are coprime integers. We will show that there are integers m, n such that

$$a^m + b^n = 1(\text{mod } ab)$$

Because a, b are coprime, by the CRT we know that

$$\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

Now the image of a in $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ is $(0, a \text{ mod } b)$ and the image of b in $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ is $(b \text{ mod } a, 0)$. So, we just need to show that there are integers m, n such that

$$(b \text{ mod } a, 0)^n + (0, a \text{ mod } b)^m = 1 \text{ in } \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

because the same m, n will work for the images of a, b in $\mathbb{Z}/ab\mathbb{Z}$. This helps because we can now work individually with components in $\mathbb{Z}/a\mathbb{Z}$ and $\mathbb{Z}/b\mathbb{Z}$ respectively.

Because a, b are coprime, b is a unit in $\mathbb{Z}/a\mathbb{Z}$, i.e b is an element of the multiplicative group of units $(\mathbb{Z}/a\mathbb{Z})^\times$. This group has order $\varphi(a)$, and hence by **Lagrange's Theorem** we see that

$$(b(\text{mod } a))^{\varphi(a)} = b^{\varphi(a)}(\text{mod } a) = 1(\text{mod } a)$$

So we can put $n = \varphi(a)$. Similarly, we can put $m = \varphi(b)$. This proves the existence of such integers m, n. ■

22. Artin Chapter 12: 5.6.

Solution. Suppose $R = \mathbb{Z}[\sqrt{-3}]$. We will show that an integer p is prime in R iff. the polynomial $x^2 + 3$ is irreducible in $\mathbb{F}_p[x]$.

Our first observation is that

$$\frac{\mathbb{Z}[x]}{(x^2+3)} \cong \mathbb{Z}[\sqrt{-3}]$$

To prove this, consider the unique homomorphism $\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}[\sqrt{-3}]$ given by $x \mapsto \sqrt{-3}$ and that restricts to the identity on $\mathbb{Z}$. This homomorphism is surjective because given any $a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$, we see that

$$\varphi(a + bx) = a + b\sqrt{-3}$$

As I proved in HW-1, the kernel of this map must be a *principal ideal* in $\mathbb{Z}[x]$, and the kernel is infact (x^2+3). So this proves the required isomorphism.

Now, suppose an integer p is prime in $\mathbb{Z}[\sqrt{-3}]$. This happens if and only if $\mathbb{Z}[\sqrt{-3}]/(p)$ is an *integral domain*. By the above isomorphism, this is true if and only if the ring

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

is an integral domain, where in the extreme right side $x^2 + 3 \in \mathbb{F}_p[x]$ (we used the fact that the order of taking quotients does not matter; this was proved in Lecture 4 and I also mentioned it in HW-2). But again, this is true if and only if the polynomial x^2+3 is prime in $\mathbb{F}_p[x]$. So, it is enough to show that x^2+3 is prime in $\mathbb{F}_p[x]$ if and only if it is irreducible.

One direction is clear: if x^2+3 is irreducible in $\mathbb{F}_p[x]$, then the ideal (x^2+3) is *maximal* (because $\mathbb{F}_p[x]$ is a PID) and hence it is *prime*, because maximal ideals are prime as well. For the converse, suppose x^2+3 is a prime element. For the sake of contradiction, suppose x^2+3 was reducible, i.e it factors into linear factors in $\mathbb{F}_p[x]$. But, this is a contradiction to the fact that x^2+3 is prime, because x^2+3 being a quadratic polynomial cannot divide either of its linear divisors. Hence, x^2+3 must be irreducible. This completes the proof. ■