Lecture 10: Some applications of the 1st isomorphism theorem

Monday, April 23, 2018 11:07 AM

<u>Ex.</u> $\mathbb{Q}[x]/\langle x^2+1\rangle \simeq \mathbb{Q}[i]$.

<u>Pf.</u> In this example we will learn an important technique which will be used again and again.

<u>Evaluation map at i.</u> Consider $\phi_i : \mathbb{Q}[x] \to \mathbb{C}$,

$$\phi_i(p(x)) = p(i).$$

Then ϕ_i is a ring homomorphism. (why? try to justify this).

<u>$\operatorname{Im}\phi_i$</u> $= \mathbb{Q}[i]$.

<u>Pf.</u> $\forall p(x) \in \mathbb{Q}[x]$, $p(x) = a_n x^n + \cdots + a_1 x + a_0$ for some $a_j \in \mathbb{Q}$. Hence $\phi_i(p) = a_n (i)^n + \cdots + a_1 (i) + a_0$ (*)

On the other hand, $a_j \in \mathbb{Q}[i]$ and $i \in \mathbb{Q}[i]$. Thus by (*) $\phi_i(p) \in \mathbb{Q}[i]$. Therefore $\operatorname{Im}\phi_i \subseteq \mathbb{Q}[i]$.

- $\forall a, b \in \mathbb{Q}$, $\phi_i(a+bx) = a+bi$; and so $\mathbb{Q}[i] \subseteq \operatorname{Im}\phi_i$.

And claim follows.

- <u>What is kernel of ϕ_i?</u> • <u>$x^2+1 \in \ker\phi_i$</u>. $\phi_i(x^2+1) = i^2+1 = 0$.

And so $\langle x^2+1\rangle \subseteq \ker\phi_i$.

Lecture 10: Some applications of the 1st iso. thm

Monday, April 23, 2018 11:22 AM

Suppose $f(x) \in \ker \phi_i$. By long division, $\exists\, r(x), q(x) \in \mathbb{Q}[x]$,

$f(x) = q(x)(x^2+1) + r(x)$, $\deg r < 2$.

And so $\phi_i(f) = \phi_i(r) = 0$.

Suppose $r(x) = a + bx$ for $a, b \in \mathbb{Q}$. Then $\phi_i(r) = a + bi = 0$

implies $a = b = 0$. And so $r = 0$, and $f(x) \in \langle x^2+1 \rangle$.

Therefore $\ker \phi_i = \langle x^2+1 \rangle$.

Hence by the 1^{st} isomorphism theorem

$$\mathbb{Q}[x]/\langle x^2+1 \rangle \simeq \mathbb{Q}[i]. \quad \blacksquare$$

From the above example we learn a few important techniques:

① When we want to show a factor ring R/I is isomorphic to a ring S, it is a good idea to start with a ring homomor. $\phi: R \to S$ or $\phi: R \to S'$ s.t. S is a subring of S'. Try to show $\operatorname{Im} \phi = S$ and $\ker \phi = I$.

② Having $\phi: R \to S$, often it is not hard to find $\operatorname{Im}(\phi)$. To show $\ker \phi = I$, one has to show $I \subseteq \ker \phi$ and $\ker \phi \subseteq I$.

Lecture 10: Some examples of the 1st iso. thm.

Monday, April 23, 2018 11:41 AM

Often it is easy to show $I \subseteq \ker \phi$. Most of the times I is given by a set of generators $I = \langle r_1, \ldots, r_n \rangle$. Then to show $I \subseteq \ker \phi$, one has to check $\phi(r_1) = \cdots = \phi(r_n) = 0$, which is often straightfoward. To show $\ker \phi \subseteq I$, it is often hard, and usually a (generalized) division algorithm is useful; specially when $I = \langle b \rangle$ is a principal ideal. Then one starts with $a \in \ker \phi$ then "divides a by b" (if possible), then $a = bq + r$, and r is "smaller"; and $r = a - bq \in \ker \phi$; In the next step, one has to show $r = 0$. This is what we did when we showed $\mathbb{Z}$ is a PID; and we used the same technique to solve the previous example, and we will see that this idea will help us to show $\mathbb{Q}[x]$ is a PID. In the next example we will use a similar idea for Gaussian integers $\mathbb{Z}[i]$; and later we will prove that $\mathbb{Z}[i]$ is a PID.

Lecture 10: Some examples of the 1st iso thm

Tuesday, April 24, 2018 9:04 AM

__Ex.__ $\mathbb{Z}[i]/\langle 3+2i\rangle \simeq \mathbb{Z}/13\mathbb{Z}$.

__Pf.__ We'd like to define a ring homomorphism

$\phi: \mathbb{Z}[i] \to \mathbb{Z}/13\mathbb{Z}$. Where should we send i assuming

$\phi(1) = 1+13\mathbb{Z}$? $\phi(i)^2 = \phi(i^2) = \phi(-1) = -1+13\mathbb{Z}$.

Notice that $5^2 = 25 \equiv -1 \pmod{13}$. So it makes sense

to send i to 5 and define $\phi(a+bi) = a+5b+13\mathbb{Z}$.

__Claim__ ϕ is a ring homomorphism.

$$\phi((a+bi)(c+di)) = \phi((ac-bd)+(ad+bc)i)$$

$$= (ac-bd)+5(ad+bc)+13\mathbb{Z} \qquad (\mathrm{I})$$

$$\phi(a+bi)\,\phi(c+di) = ((a+5b)+13\mathbb{Z})((c+5d)+13\mathbb{Z})$$

$$= (a+5b)(c+5d)+13\mathbb{Z}$$

$$= ac+25bd+5(ad+bc)+13\mathbb{Z}$$

$$= (ac-bd)+5(ad+bc)+13\mathbb{Z} \qquad (\mathrm{II})$$

(I) and (II) imply ϕ preserves multiplication.

It is easy to check that ϕ preserves addition (do it on your own.)

Lecture 10: Some examples of the 1st iso. thm.

Monday, April 23, 2018 11:31 AM

ϕ is onto. Since $\phi(1) = 1 + 13\mathbb{Z}$, $\forall n \in \mathbb{Z}$,

$\phi(n) = n + 13\mathbb{Z}$. And so ϕ is onto.

What is kernel of ϕ?

$\phi(3+2i) = 3 + 5\times 2 + 13\mathbb{Z} = 0 + 13\mathbb{Z}$.

And so $\langle 3+2i \rangle \subseteq \ker \phi$. (II)

To show $\ker\phi \subseteq \langle 3+2i \rangle$, as we explained earlier, we try to divide $a+bi \in \ker\phi$ by $3+2i$.

Going back to integers, we can view division as follows:

for n, m in $\mathbb{Z}$ and $m \neq 0$, we consider the fraction $\frac{n}{m} \in \mathbb{Q}$, let q be the integer part of $\frac{n}{m}$ and write $\frac{n}{m} = q + e$ where $0 \le e < 1$. Then $n = mq + \underbrace{(em)}_{r}$. So $r \in \mathbb{Z}$ and $0 \le em < m$ implies $0 \le r < m$. We will follow the same path in Gaussian integers and consider $\frac{a+bi}{3+2i} = a' + b'i \in \mathbb{Q}[i]$.

(We will continue in the next lecture.)