MA3202: Algebra II

Satvik Saha, 19MS154 January 24, 2022

Exercise 1 Let R be a commutative ring, and consider the nilradical of R defined by

$$N = \{x \in R : x^n = 0 \text{ for some } n\}.$$

Prove that N is an ideal of R.

Solution It is clear that if $x, y \in N$ with $x^m = y^n = 0$, then

$$(x+y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} = 0.$$

This is because in each term, either the power of x is at least m, or the power of y is at least n. Also,

$$(xy)^{m+n} = x^{m+n} \cdot y^{m+n} = 0,$$

hence $x + y, xy \in N$. Finally, note that for even m,

$$x^m - (-x)^m = (x + (-x)) \cdot (x^{m-1} - x^{m-2} \cdot (-x) + \cdots - (-x)^{m-1}) = 0,$$

and for odd m,

$$x^m + (-x)^m = (x + (-x)) \cdot (x^{m-1} - x^{m-2} \cdot (-x) + \cdots + (-x)^{m-1}) = 0.$$

Hence, $(-x)^m = 0$ giving $-x \in N$. Finally, given $a \in R$, we clearly have

$$(ax)^m = a^m \cdot x^m = 0,$$

giving $ax \in N$.

Exercise 2 Give examples of two rings R, S such that $(R, +)$ and $(S, +)$ are isomorphic, but $(R, +, \cdot)$ and $(S, +, \cdot)$ are not.

Solution It is clear that $\mathbb{Z}$ and $2\mathbb{Z}$ are isomorphic as additive groups. However, they are not isomorphic as rings; if $\varphi\colon \mathbb{Z} \to 2\mathbb{Z}$ were an isomorphism, then we demand $\varphi(1) = \varphi(1^2) = \varphi(1)^2$ which is impossible unless $\varphi(1) = 0$, but this is no longer an isomorphism.

Exercise 3 True or false?

(i) Ring homomorphisms (non-trivial) map zero-divisors to zero-divisors.

(ii) Ring homomorphisms (non-trivial) map nilpotent elements to nilpotent elements.

Solution

(i) False. Consider the homomorphism $\varphi\colon \mathbb{Z}_4 \to \mathbb{Z}_2$, $n \mapsto n \pmod 2$. Then $2 \in \mathbb{Z}_4$ is a zero-divisor since $2 \cdot 2 = 4 \equiv 0$. However, $\mathbb{Z}_2$ has no zero-divisors.

(ii) True. Let $\varphi\colon R \to S$ be a non-trivial ring homomorphism, and let $a \in R$ such that $a^n = 0$. Then, $\varphi(a)^n = \varphi(a^n) = \varphi(0) = 0$.

Exercise 4 Let R be the ring of all 2×2 real matrices of the form

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Prove that R is isomorphic to the ring of complex numbers $\mathbb{C}$.

Solution We define the map

$$\varphi\colon \mathbb{R} \to \mathbb{C}, \qquad \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi.$$

It can be checked that this is indeed an isomorphism.

Exercise 5 How many ring homomorphisms are there from $\mathbb{Z}_3$ to $\mathbb{Z}_7$?

Solution There is only the trivial/zero homomorphism. Any other homomorphism must map $0 \mapsto 0$, $1 \mapsto 1$, hence $2 = 1 + 1 \mapsto 2$. Now, this requires $1 + 1 + 1 \mapsto 3$, but $1 + 1 + 1 \equiv 0$, a contradiction.

Exercise 6 Let R be a commutative ring and $I \subset R$ be an ideal. Consider the radical

$$\sqrt{I} = \{x \in R : x^n \in I \text{ for some } n\}.$$

(i) Prove that $\sqrt{I}$ is an ideal of R.

(ii) Let $f\colon R \to S$ be a surjective ring homomorphism such that $\ker f \subset I$. Prove that $f(\sqrt{I}) = \sqrt{f(I)}$.

Solution

(i) Let $x, y \in \sqrt{I}$ such that $x^m, y^n \in I$. Then it is clear from previous arguments that $-x, xy, x+y \in I$. Furthermore, given $a \in R$, we have $(ax)^m = a^m x^m \in I$, hence $ax \in \sqrt{I}$.

(ii) First, pick $x \in f(\sqrt{I})$. Thus, there exists $y \in \sqrt{I}$, $y^n \in I$ for some n, such that $x = f(y)$. Thus, $x^n = f(y^n) \in f(I)$, hence $x \in \sqrt{f(I)}$.

Next, pick $x \in \sqrt{f(I)}$, with $x^m \in f(I)$ for some m. Thus, there exists $w \in I$ such that $x^m = f(w)$. From the surjectivity of f, there exists $y \in R$ such that $x = f(y)$, hence $x^m = f(y^m)$. This gives us $f(w - y^m) = 0$, hence $w - y^n \in \ker f \subset I$. Since $w \in I$, we are forced to have $y^m \in I$, $y \in \sqrt{I}$. Thus, we have $x = f(y) \in f(\sqrt{I})$.

Exercise 7 Show that every field contains a subring isomorphic to $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

Solution Let F be a field, and let $1 \in F$ be its multiplicative identity. Define a homomorphism φ, such that $\varphi(1) = 1$. Then, the image of $\mathbb{Z}$ is a subring of F; if it is finite, then this image is a finite integral domain, hence isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p. Otherwise, we have embedded $\mathbb{Z}$ inside F. Now, extend φ so that $\varphi(1/n) = n^{-1}$ in F, and $\varphi(p/q) = p \cdot q^{-1}$ in F. This gives an embedding of $\mathbb{Q}$ in F.

Exercise 8 Let R and S be commutative rings with identities, and let $T = R \times S$. Show that every ideal I of T is of the form $I = J \times K$, where J and K are ideals of R and S respectively.

Solution Let I be an ideal in $R \times S$. Then given non-zero $(r, s) \in I$, we demand $(r, 0) = (r, s) \cdot (1, 0) \in I$, as well as $(0, s) = (r, s) \cdot (0, 1) \in I$. Now if $(r', s') \in I$, we immediately have $(r', s), (r, s') \in I$. In other words, if we set J to be the set of first coordinates of elements in I, and K to be set of second coordinates of elements in I, then $I = J \times K$.

To show that J is an ideal in R, note that given any $x, y \in J$, we have $(x, 0), (y, 0) \in I$, hence $(-x, 0), (x + y, 0), (xy, 0) \in I$. By definition of J, we have $-x, x + y, xy \in I$. A similar argument shows that K is an ideal in S.

Exercise 9 How many isomorphisms $\varphi\colon \mathbb{C} \to \mathbb{C}$ are there such that $\varphi(\mathbb{R}) \subset \mathbb{R}$?

Solution Two. Note that $\varphi(1) = 1$ forces φ to fix the integers, hence the rationals, hence the reals. Now, $\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -1$, forcing one of $\varphi(i) = \pm i$. It can be checked that both choices determine distinct isomorphisms.

Exercise 10 Let $f\colon R \to S$ be a ring homomorphism and I, J be ideals of R, S respectively. Assume that $f(I) \subset J$. Show that f defined a homomorphism $\tilde{f}\colon R/I \to S/J$. What is the kernel of $\tilde{f}$?

Solution Define the natural homomorphism

$$\tilde{f}\colon R/I \to S/J, \qquad x + J \mapsto f(x) + J.$$

It is easily checked that this is indeed a homomorphism.

Suppose that $x + I \in \ker \tilde{f} = K$. In other words, $x + I \mapsto J$, hence $f(x) + J \sim J$ or $f(x) \in J$. Thus, $x \in f^{-1}(J) \supset I$, so $K = f^{-1}(J)/I$.