Solutions to Exercises for TATA55, batch 3, 2021

December 10, 2021

1. (3p) Let R be a commutative, unitary ring. Let

$$\mathrm{Nil}(R) = \{r \in R | \exists n \geq 1,\ r^n = 0\}.$$

   (a) Show that $\mathrm{Nil}(R)$ is an ideal of R.

   (b) Show that $\mathrm{Nil}(R)$ is not necessarily an ideal of a non-commutative ring R.

   (c) Show that if $r \in \mathrm{Nil}(R)$ then $1 - r$ is invertible in R.

Solution: Let $r, s \in \mathrm{Nil}(R)$, $t \in R$. We can assume that $r^N = s^N = 0$. Then

$$(r+s)^{2N} = \sum_{k=0}^{2N} \binom{2N}{k} r^k s^{2N-k} = 0$$

We also have that $(tr)^N = t^N r^N = 0$.

If $g \in R$ and R is non-commutative, and furthermore $g^n = 0$, it does not follow that for any $t \in R$m $(tg)^n = 0$, since

$$(tg)^n = tgtg \dots tg$$

Let R be finitely presented $\mathbb{Q}$-algebra with generators x, y and relation $x^n = 0$. Then $xyxy \dots xy$ does not reduce to zero.

Another example:

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

in the ring of 2x2-matrices. Then A, B are nilpotent, but $A + B$ is not.

Now R is commutative once again, and $r \in R$ is nilpotent, with $r^n = 0$.

Then

$$(1-r)(1 + r + \dots + r^{n-1}) = 1 - r^n = 1.$$

Some of you expressed this as

$$(1-r)(1+r)(1+r^2)(1+r^4)\cdots = 1,$$

which is actually equivalent.

2. (3p) Find the characteristic of the following commutative rings:

   (a) $\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{9\mathbb{Z}} \times \frac{\mathbb{Z}}{15\mathbb{Z}}$

   (b) $\mathbb{Z}[i]$, where $i \in \mathbb{C}$, $i^2 = -1$

   (c) $\frac{\mathbb{Z}[j]}{(2-5j)}$ where j is a primitive 3rd root of unity, $j^3 = 1$ but, $j^2 \neq 1$, you can explicitly take $j = \exp(\frac{2}{3}\pi i) \in \mathbb{C}$.

   Solution: $1 = ([1]_3, [1]_9, [1]_{15})$, so $n[1] = 0 = ([0]_3, [0]_9, [0]_{10})$ iff n is a common multiple of $3, 9, 15$, so the characteristic is 45.

   In $(\mathbb{Z}[i], +, 0)$, $\langle 1 \rangle$ is infinite, so the characteristic of the ring is zero.

   Call the last ring $R = \mathbb{Z}[j]/I$. In $\mathbb{Z}[j]$ it holds that $j^2 + j + 1 = 0$, so

$$(2-5j)(2-5j^2) = 4 - 10(j + j^2) + 25j^3 = 4 + 10 + 25 = 39,$$

   hence this is zero in R. The characteristic c is hence a divisor of 39. We have expressed $c * 1 \in \mathbb{Z}[j]$ as an element of the ideal $(2-5j)$, so

$$c = (2-5j)(a+bj), \qquad a, b \in \mathbb{Z}.$$

   We can embed $\mathbb{Z}[j]$ inside $\mathbb{C}$, and use complex absolute values: then $|c|^2 = |2-5j|^2|a+bj|^2$. Since $\bar{j} = j^2$ we have that $|a+bj|^2 = (a+bj)(a+bj^2) = a^2 + b^2 + ab(j + j^2 == a^2 + b^2 - ab$ and $|2-5j|^2 = 39$, so we get that

$$c^2 = 39(a^2 + b^2 - ab).$$

   So $39 \,\big|\, c^2$, and hence $c = 39$.

3. (2p) Provide explicit ring isomorphisms between

   (a) $\frac{\mathbb{Z}[x]}{(n,x)}$ and $\frac{\mathbb{Z}}{n\mathbb{Z}}$,

   (b) $\frac{\mathbb{Z}[x]}{(n)}$ and $(\frac{\mathbb{Z}}{n\mathbb{Z}})[x]$.

   Solution: The surjective ring homomorphism

$$\mathbb{Z}[x] \ni f(x) \mapsto [f(0)]_n \in \mathbb{Z}_n$$

   sends both (x) and (n) to zero, hence its kernel N contains $(x, n) = (x) + (n)$. Conversely, any $f(x)$ can be written as

$$f(x) = xg(x) + c,$$

   which gets sent to $[c]_n$, which is zero iff $c \in (n)$, so the kernel N is precisely (x, n). The explicit isomorphism provided by the first isomorphism theorem is

$$(xg(x) + c) + N \mapsto [c]_n$$

Next, define

$$\phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_n[x]$$
$$\phi\left(\sum_{j=0}^{m} a_j x^j\right) = \sum_{j=0}^{m} [a_j]_n x^j$$

This is again a surjective ring homomorphism, and has kernel (n). So the first isomorphism theorem gives the isomorphism

$$\hat{\phi} : \frac{\mathbb{Z}[x]}{(n)} \longrightarrow \mathbb{Z}_n[x]$$
$$\hat{\phi}\left(\sum_{j=0}^{m} a_j x^j + (n)\right) = \sum_{j=0}^{m} [a_j]_n x^j$$

4. (3p) Which of the following ideals in $\mathbb{Z}[x]$ are prime? Which are maximal?
   (a) $(x, x+1)$,
   (b) $(5, x^2+4)$,
   (c) $(x^2+1, x+2)$.

Solution:

(a) $1 = -1 * x + 1 * (x+1)$ so the ideal is the whole ring.

(b) $\frac{\mathbb{Z}[x]}{(5,x^2+4)} \simeq \frac{\mathbb{Z}_5[x]}{(x^2+4)}$. Since $x^2+4 \equiv x^2-1 \equiv (x+1)(x-1)$ the quotient has zero-divisors, and the original ideal is not prime.

(c) From $x \equiv -2$, $x^2 \equiv -1$ we conclude that $5 \equiv 0$ and $x \equiv 3$, so the quotient is $\mathbb{Z}/(5\mathbb{Z})$, a field, hence the ideal is maximal.

5. (4p) Let $g(x) = x^6 - x^3 - 2 \in \mathbb{Q}[x]$. Put $R = \mathbb{Q}[x]/(g(x))$.
   (a) Is R an integral domain?
   (b) Find all proper, non-trivial ideals of R.
   (c) Let a denote the coset $x + (g(x)) \in R$. Find, if possible, the inverse of a.
   (d) Find a general expression for a^k, $k \geq 0$, as a linear combination of a^0, a^1, a^2, a^3, a^4, a^5.

Solution:

(a) First, we factor $g(x)$ into irreducible factors:

$$g(x) = (x^3-2) * (x^2-x+1) * (x+1).$$

In the quotient, the factors become zero-divisors, so R is no domain.

(b) By the correspondence theorem, proper and non-trivial ideals in the quotient correspond to proper ideals in the polynomial ring which properly contains $(g(x))$, hence, since $\mathbb{Q}[x]$ is a PID, to the ideals $(x+1)$, (x^2-x+1), (x^3-2), $((x^2-x+1)(x+1))$, $((x^3-2)(x+1))$, $((x^3-2)(x+1))$.

(c) Since $a^6 - a^3 - 2 = 0$, we have that $a^6 = a^3 + 2$, and we see that

$$a(a^5 - a^2) = a^6 - a^3 = a^3 + 2 - a^3 = 2,$$

so $a^{-1} = \frac{1}{2}a^5 - \frac{1}{2}a^2$.

(d) We tabulate the first 24 powers of a:

$$\begin{aligned}
(0, 1)\\
(1, a)\\
(2, a^2)\\
(3, a^3)\\
(4, a^4)\\
(5, a^5)\\
(6, a^3 + 2)\\
(7, a^4 + 2 * a)\\
(8, a^5 + 2 * a^2)\\
(9, 3 * a^3 + 2)\\
(10, 3 * a^4 + 2 * a)\\
(11, 3 * a^5 + 2 * a^2)\\
(12, 5 * a^3 + 6)\\
(13, 5 * a^4 + 6 * a)\\
(14, 5 * a^5 + 6 * a^2)\\
(15, 11 * a^3 + 10)\\
(16, 11 * a^4 + 10 * a)\\
(17, 11 * a^5 + 10 * a^2)\\
(18, 21 * a^3 + 22)\\
(19, 21 * a^4 + 22 * a)\\
(20, 21 * a^5 + 22 * a^2)\\
(21, 43 * a^3 + 42)\\
(22, 43 * a^4 + 42 * a)\\
(23, 43 * a^5 + 42 * a^2)
\end{aligned}$$

Then, we ask the Online Encyclopedia of Integer Sequences about

$$1, 3, 5, 11, 21, 43$$

and get the answer: *A001045* Jacobsthal sequence (or Jacobsthal numbers):

$$a(n) = a(n-1) + 2 * a(n-2), \text{ with } a(0) = 0, a(1) = 1;$$

We are already using a, so let us call them $J(n)$ instead. Then, a reasonable hypothesis is that

$$a^{6n+k} = \begin{cases} J(2n)a^3 + J(2n) + 1 & k = 0 \\ J(2n)a^4 + (J(2n)+1)a & k = 1 \\ J(2n)a^5 + (J(2n)+1)a^2 & k = 2 \\ J(2n)a^3 + J(2n) - 1 & k = 3 \\ J(2n)a^4 + (J(2n)-1)a & k = 4 \\ J(2n)a^5 + (J(2n)-1)a^2 & k = 5 \end{cases}$$

This is straightforward, if tedious, to prove by induction, using the relation

$$J(m) = J(m-1) + 2J(m-2).$$

One could also use the CRT and look at the image of x^k in

$$\frac{\mathbb{Q}[x]}{(x^3-2)}, \frac{\mathbb{Q}[x]}{(x^2-x+1)}, \frac{\mathbb{Q}[x]}{(x+1)},$$

to see the patterns there, then lift back to R.

6. (5p) Let $R = \mathbb{Q}[D_4]$, the group algebra on $D_4 = \langle r, s | r^4 = s^2 = rsrs = 1 \rangle$. In other words, R is the $\mathbb{Q}$-vector space with basis elements labeled with the elements of D_4, and with multiplication the $\mathbb{Q}$-linear extension of the multiplication on basis elements given by the multiplication of D_4.

   (a) Put $t = 1 * r + 1 * s \in R$. Calculate $t * t$ and $t * t * t$

   (b) Put $v = 1 * 1 + 1 * s$. Find an explicit expression for v^k for any positive k.

   (c) Show that the map

   $$F : \mathbb{Q}[D_4] \to \mathbb{Q}$$
   $$\sum_{g \in D_5} c(g)g \mapsto \sum_{g \in D_5} c(g)$$

   is $\mathbb{Q}$-linear and calculate its kernel.

   (d) Show that the *left annihilator*

   $$\mathrm{Ann}(t) = \{ f \in R | f * t = 0 \}$$

   is a left ideal of R, and calculate a basis of it as a $\mathbb{Q}$-vector space.

(e) List the conjugacy classes in D_4. Calculate the *center* of R, i.e.,

$$\text{Center}(R) = \{ f \in R | f * h = h * f \text{ for all } h \in R \}$$

Compare.

Solution: : We represent D_4 as a permutation subgroup of S_4 by mapping r to $(1,2,3,4)$ and s to $(2,4)$.

(a) We label the vertices of the square counterclockwise; then $r = (1,2,3,4)$ and $s = (2,4)$, so $t = ((1,2,3,4) + (2,4)$, and

$$t^2 = () + (1,2)(3,4) + (1,3)(2,4) + (1,4)(2,3)$$
$$t^3 = 2 * (2,4) + 2 * (1,2,3,4) + 2 * (1,3) + 2 * (1,4,3,2)$$

(b) Next, we put $v = () + (2,4)$ and calculate

$$v^1 = () + (2,4)$$
$$v^2 = 2 * () + 2 * (2,4)$$
$$v^3 = 4 * () + 4 * (2,4)$$
$$v^4 = 8 * () + 8 * (2,4)$$

It seems reasonable to assume that $v^{n+1} = 2^n * v$, so let us prove this by induction. The base case is clear, so consider

$$\begin{aligned} v^{n+1} &= v * v^n \\ &= (() + (2,4)) * (2^{n-1} * () + 2^{n-1} * (2,4)) \\ &= 2^{n-1} * () + 2^{n-1} * (2,4) + 2^{n-1} * (2,4) + 2^{n-1} * () = 2^n * () + 2^n * (2,4). \end{aligned}$$

(c) The map is the linear map that sends each basis vector to 1, so its matrix with respect to this basis is

$$[1,1,1,1,1,1,1,1]$$

which has nullity 7, with a basis given by $-\mathbf{e}_1 + \mathbf{e}_j$ for $2 \leq j \leq 8$. Translated back to our vector space we have the basis

$$\{ 1 * g - 1 * () | g \neq () \}.$$

(d) We first show that $\text{Ann}(t)$ is a left ideal for any t. Suppose that $f, g \in \text{Ann}(t)$, $u, v \in R$. Then $(f+g)t = ft + gt = 0$, and $(vf)t = v(ft) = v * 0 = 0$, hence the annihilator is a left ideal.

Now let $t = 1 * (1,2,3,4) + 1 * (2,4)$, and let SAGEmath calculate the left annihilator (or solve the linear system of equations in another way). We get a basis

$$(() - (1,4)(2,3), \qquad -(1,2)(3,4) + (1,3)(2,4), \\ -(2,4) + (1,4,3,2), \qquad (1,2,3,4) - (1,3))$$

so the annihilator is a four-dimensional subspace of the eight-dimensional group algebra.

(e) According to SAGEmath, the center has a basis (as a vector subspace) consisting of

$$(), (2,4) + (1,3), (1,2)(3,4) + (1,4)(2,3), (1,2,3,4) + (1,4,3,2), (1,3)(2,4)$$

Each basis element is the sum of all elements in a conjugacy class of D_4.