Solutions to Exercises for TATA55, batch 5, 2023

December 27, 2023

1. (3p) Provide an explicit ring isomorphism $\frac{\mathbb{Z}[x]}{(4,6,3x,5x)} \simeq \mathbb{Z}_2$.

   Solution: The defining ideal of the qutient ring is $I = (2, x)$. The surjective ring homomorphism

   $$\begin{aligned} \phi : \mathbb{Z}[x] &\to \mathbb{Z}_2 \\ \phi(f(x)) &= [f(0)]_2 \end{aligned}$$

   has kernel I, so the first isomorphism theorem shows that

   $$\frac{\mathbb{Z}[x]}{I} \ni f(x) + I \mapsto [f(0)]_2$$

   is well-defined, and a ring isomorphism.

2. (3p) Solve the equation (in $\mathbb{Q}[x]$)

   $$f(x)(2x^3 + 3x^2 + 7x + 1) + g(x)(5x^4 + x + 1) = x + 3$$

   Solution: Put $a(x) = 2x^3+3x^2+7x+1$, $b(x) = 5x^4+x+1$, $c(x) = x+3$. Let $d(x) = \gcd(a(x), b(x)$. Then Euclides extended algorithm gives that

   $$d(x) = 1 = u(x)a(x) + v(x)b(x)$$

   with

   $$\begin{aligned} u(x) &= -\frac{8088}{8539}x^3 + \frac{1453}{8539}x^2 - \frac{393}{8539}x - \frac{10348}{42695} \\ v(x) &= \frac{16176}{42695}x^2 + \frac{21358}{42695}x + \frac{53043}{42695} \end{aligned}$$

   So

   $$c(x) = c(x)u(x)a(x) + c(x)v(x)b(x).$$

Since $a(x)$ and $b(x)$ are relatively prime, the solutions to the homogeneous equation

$$f_h(x)a(x) + g_h(x)b(x) = 0$$

are given by

$$(f_h(x), g_h(x)) = n(x)(-b(x), a(x)),$$

where $n(x)$ is an arbitrary polynomial. All solutions to the original equation are therefore

$$(f(x), g(x)) = c(x) * (u(x), v(x)) + n(x) * (-b(x), a(x)).$$

Remark: similar to linear Diophantine equations over $\mathbb{Z}$, we should scale u, v by c, but we should not scale the homogeneous solutions $(-b(x), a(x))$ by $n(x)c(x)$ but rather by the general $n(x)$, lest we lose solutions.

3. (4p) List all ideals in $S = \mathbb{Z}_7[x]/(h(x))$ where $h(x) = x^4 + 2x^2 + 2$. Is S an integral domain?

   Solution: Since $h(x) = f(x)g(x)$ with $f(x) = x^2 + 5x + 3$, $g(x) = x^2 + 2x + 3$, both irreducible, $I = (h)$ is not a prime ideal, and $S = \mathbb{Z}_7[x]/I$ is not a domain. By the correspondence theorem the ideals in S correspond to those in $\mathbb{Z}_7[x]$ that contain I, and those are precisely the principal ideals on factors of h. So the ideals in S are

   $$(0), (f) + I, (g) + I, S.$$

4. (3p) Factor $11y^5 - 55y^4 + 85y^3 - 30y^2 - 35y + 39 \in \mathbb{Z}[x]$. (Hint: try a linear substitution)

   Solution: Call the polynomial $f(y)$, then

   $$f(y + 1) = 11y^5 - 25y^3 + 5y^2 - 5y + 15,$$

   which is irreducible by Eisensteins criteria. Hence, $f(y)$ is irreducible, as well.

5. (4p) Let $R = \mathbb{Q}[u, v, w]/(u^2v^2 - w^3)$. Find a finitely many monomials $x^{a_j}y^{b_j}$ in $S = \mathbb{Q}[x, y]$ such that $R \simeq \mathbb{Q}[x^{a_1}y^{b_1}, \ldots, x^{a_r}y^{b_r}]$.

   Solution: Define a surjective ring homomorphism

   $$\phi : \mathbb{Q}[u, v, w] \to \mathbb{Q}[x, y]$$

by specifying that

$$\begin{aligned}\phi(u) &= x^2y\\ \phi(v) &= xy^2\\ \phi(w) &= x^2y^2\end{aligned}$$

end then extending this in the unique way that satisfies the rules for a ring homomorphism, i.e.,

$$\phi\left(\sum c_{a,b,c}u^a v^b w^c\right) = \sum c_{a,b,c}\phi(u^a v^b w^c) = \sum c_{a,b,c}\phi(u)^a\phi(v)^b\phi(w)^c$$

Then clearly $u^2v^2 - w^3 \in \ker\phi$. Let us introduce the integer matrix

$$A = \begin{pmatrix}2 & 1 & 2\\ 1 & 2 & 2\end{pmatrix}$$

Then a monomial in u, v, w with exponent vector (a, b, c) gets mapped to the monomial in x, y with exponent vector $A * (u, v, w)^t$, so a binomial $u^a v^b w^c - u^d v^e w^f$ gets mapped zero iff $A * (a, b, c)^t = A * (d, e, f)$, i.e. if $(a, b, c) - (d, e, f)$ lies in the (right) nullspace of A. This nullspace is

$$\left\{ n(2, 2, -3)^t \middle| n \in \mathbb{Z} \right\}$$

so since the kernel of the ring homomorphism ϕ is obviously a binomial ideal, it is precisely $(u^2v^2 - w^3)$.

The first isomorphism theorem then gives that R is isomorphic to the image of ϕ, which is the subring (noth the ideal!) generated by x^2y, xy^2, x^2y^2.

6. (6p) Show that

   (a) not every function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ is $\mathbb{Z}_2$-linear,

   (b) but all such functions are polynomial,

   (c) and they correspond bijectively to cosets of the ideal

$$(x_1^2 + x_1, x_2^2 + x_2, \ldots, x_n^2 + x_n) \subset \mathbb{Z}_2[x_1, \ldots, x_n].$$

Solution: A $\mathbb{Z}_2$ linear function must map zero to zero; the constant 1 function does not.

Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. Each $\mathbf{u} \in \mathbb{Z}_2^n$ correspond to a subset $S \subseteq [n] = \{1, 2, \ldots, n\}$, and to a squarefree monomial $m_S = \prod_{i\in S} x_i \in \mathbb{Z}_2[x_1, \ldots, x_n]$.

Let $p = \sum_{\{S \subseteq [n] \mid f(S)=1\}} m_S$. Then evaluating the polynomial p gives the function f.

As an example, if

$$f((x_1, x_2, x_3)) = \begin{cases} 1 & \text{if } x_1 + x_2 + x_3 = 1 \in \mathbb{Z}_2 \\ 0 & \text{otherwise} \end{cases}$$

then the corresponding polynomial is

$$p = x_1 + x_2 + x_3 + x_1x_2x_3.$$

Finally, two polynomials p, q give the same evaluation function iff $p - q$ is constantly zero. Put $I = (x_1^2 + x_1, \ldots, x_n^2 + x_n)$. Then clearly every polynomial in I evaluates to the constant zero function.

Conversely, let $p(x_1, \ldots, x_n) \in \mathbb{Z}_2[x_1, \ldots, x_n]$. Since $x_j^k + x_j$ is constantly zero, any x_j^k-term may be replaced with x_j in p without changing the corresponding evaluation function. Thus p is equivalent in this sense to a polynomial with squarefree monomials. All squarefree monomials correspond to the characteristic function on the corresponding subset of $[n]$, for which a value may be freely prescribed — hence all polynomials with only squarefree monomials in their support yield different evaluations. The conclusion follows.