Solutions to Exercises for TATA55, batch 3

January 30, 2017

1. Let R be a commutative, unitary ring, and I an ideal in R. Suppose that all elements outside I are invertible. Show that I is the unique maximal ideal in R. 2 p

   Solution: Any ideal containing a unit is the whole ring, so every proper ideal is contained in I. This shows both that I is a maximal ideal, and that there are no other maximal ideals.

2. Let $R = \mathbb{C}[[t]]$, the ring of formal power series in t with complex coefficients.

   (a) By inductively solving an infinite system of equations, show that $\sum_{\ell \geq 0} a_\ell t^\ell$ is invertible iff $a_0 \neq 0$. Conclude that (t) is the unique maximal ideal in R. 1 p

   (b) Show that any $f \in R$ (should be non-zero f) can be uniquely written as a product $f = ut^m$, where m is a non-negative integer and $u \in R$ is a unit. 1 p

   (c) List all ideals in R. 2 p

   (d) We say that $f_n \to f \in R$ as $n \to \infty$ if, for all m, there is some $N(m)$ so that $n > N(m)$ implies that $f - f_n \in (t)^m = (t^m)$. Take any $f \in R \setminus (t)$ and write it as $c(1-g)$ with $g \in (t)$. Show that $(1-g)(1+g+g^2+\cdots+g^n) \to 1$ as $n \to \infty$. Hence, the inverse of $1-g$ is $\sum_{\ell \geq 0} g^\ell$, and the inverse of f is $c^{-1} \sum_{\ell \geq 0} g^\ell$. 1 p

   Solution: : Make the Ansatz that the putative inverse is $\sum_{\ell \geq 0} b_\ell t^\ell$. Then

   $$1 = \sum_{\ell \geq 0} a_\ell t^\ell \sum_{\ell \geq 0} a_\ell t^\ell$$

   gives, by comparing coefficients for powers of t, that

   $$\begin{aligned}
   1 &= a_0 b_0 \\
   0 &= a_0 b_1 + a_1 b_0 \\
   0 &= a_0 b_2 + a_1 b_1 + a_2 b_0 \\
   &\vdots \\
   0 &= a_0 b_k + a_1 b_{k-1} + \ldots a_{k-1} b_1 + a_k b_0 \\
   &\vdots
   \end{aligned}$$

   The first equation has the unique solution $b_0 = 1/a_0$ (provided that $a_0 \neq 0$). By induction, if $b_0, b_1, \ldots, b_{k-1}$ are determined, then

   $$b_k = -(a_1 b_{k-1} + \cdots + a_k b_0)/a_0.$$

   Now apply the previous exercise.

   For the (non-zero) $f = \sum_{\ell \geq 0} a_\ell t^\ell \in R$, define the order of f as the d such that $a_d \neq 0$ but $a_i = 0$ for $i < d$. Then $f = t^d \sum_{j=d}^{\infty} a_j t^{j-d} = t^d \sum_{\ell=0}^{\infty} a_{\ell+d} t^d$, as required.

   Put $I = (t)$. We have shown that I is the unique maximal ideal in R. In fact, the set of ideals are precisely I^k for $k \geq 0$. To see this, let J be an ideal in R, and let d be the smallest positive order of an element in J, and let $f \in J$ have order d. By the above, we have that $f = t^d g$, where g is invertible (hence has order zero). So $t^d = g^{-1} f \in J$, hence $(t^d) \subseteq J$. However, if $h \in J \setminus \{0\}$, then $h = t^r u$ with $r \geq d$, u invertible, so $h \in (t^d)$.

We have that $(1-g)(1+g+g^2+\cdots+g^n) = g^{n+1} \in (t)^{n+1}$, which tends to zero.

3. Let $R = \mathbb{C}[x,y]$ and let $M = \left\{ (a,b) \in \mathbb{Z}^2 \middle| a,b \geq 0 \right\}$. Then R is a commutative, unitary ring, and M is a monoid under componentwise addition. Put $X = \left\{ x^a y^b \middle| a,b \in \mathbb{Z}, a,b \geq 0 \right\}$. Then X is a $\mathbb{C}$-basis for R. For $f \in R$, we write

$$f = \sum_{(a,b)\in M} c_{a,b} x^a y^b = \sum_{x^a y^b \in X} c_{a,b} x^a y^b,$$

and put $\operatorname{Supp}(f) = \{ (a,b) \in M | c_{a,b} \neq 0 \}$. Note that this set is finite.

(a) We say that an ideal $I \subseteq R$ is a monomial ideal if

$$f \in I \implies x^a y^b \in I \text{ for all } (a,b) \in \operatorname{Supp}(f).$$

Show that an ideal is a monomial ideal if and only if it is generated by monomials. 2 p

(b) A subset $J \subset M$ is called a monoid ideal if $(a,b) \in J \implies (a,b)+(c,d) \in J$ for all $(c,d) \in M$. Show that the exponential mapping

$$M \ni (a,b) \mapsto x^a y^b \in X \subset R$$

induces a bijection between the set of monomial ideals in R and the set of monoid ideals in M. 1 p

(c) Show that, under this bijection, union of monoid ideals (which is again a monoid ideal) correspond to sums of monomial ideals. Show furthermore that intersections correspond to intersections. 1 p

(d) Draw a figure (by shading lattice points in the positive quadrant) of $I = (x^2, y^3)$ and of I^2, and of $J = (x^2, xy)$. Calculate (i.e. give generators for) $I^2 + J$, $I^2 \cap J$ and $I^2 J$. 2 p

(e) For all the above ideals, the quotient ring is a vector space over $\mathbb{C}$. Give vector space bases for these spaces! 2 p

Solution: An ideal generated by monomials is clearly a monomial ideal, and a monomial ideal is generated by all monomials that occur in the support of elements in the ideal.

The bijection mentioned in (b) maps induces the following bijection between monomail ideals iand monoid ideals:

map a monomial ideal I to the set of $\operatorname{Supp}(I)$ of exponents occuring in the union of the supports of elements in I. This is a monoid ideal. The inverse maps a monoid ideal to the monomial ideal generated by all $x^a y^b$ for which (a,b) belongs to the monoid ideal.

Next, we will show that the above bijection maps sums to sums and intersections to intersections. Let I, J be monomial ideals, then any $f \in I \cap J$ has the property that any monomial in its support belongs to $I \cap J$. So $I \cap J$ is a monomial ideal, and $\operatorname{Supp}(I \cap J) = \operatorname{Supp}(I) \cap \operatorname{Supp}(J)$. If $f \in I + J$ then $f = g + h$ with $g \in I$, $h \in J$. We have that

$$\operatorname{Supp}(f) \subseteq \operatorname{Supp}(g) \cup \operatorname{Supp}(h) \subseteq \operatorname{Supp}(I) \cup \operatorname{Supp}(J),$$

so $\operatorname{Supp}(I+J) \subseteq \operatorname{Supp}(I) \cup \operatorname{Supp}(J)$. Conversely, since $I \subseteq I + J$ we have that $\operatorname{Supp}(I) \subseteq \operatorname{Supp}(I+J)$, and similarly for J, so $\operatorname{Supp}(I+J) = \operatorname{Supp}(I) \cup \operatorname{Supp}(J)$. It is now clear that any monomial (with exponents) in $\operatorname{Supp}(f)$ belongs to $I + J$, which hence is a monomial ideal.

We have that $I^2 = (x^4, x^2y^3, y^6)$, $I^2 + J = (x^4, x^2y^3, y^6, x^2, xy) = (x^2, xy, y^6)$, $I^2 \cap J = (x^4, x^2y^3, xy^6)$, $I^2 J = (xy^7, x^2y^6, x^3y^4, x^4y^3, x^5y, x^6)$.

4. Consider the complex square matrix

$$C = \begin{bmatrix} 3 & 1 & 1 & 1 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}.$$

Find the characteristic polynomial of C. Calculate C^2, and show that the set $\{I, C, C^2\}$ is linearly dependent. Use this to show that the minimal polynomial has degree 2, and calculate it. 3 p

Let R be the $\mathbb{C}$-algebra generated by C. Show that is isomorphic to $\mathbb{C}[x]/(x^2)$. 2 p

Solution: The characteristic polynomial of C is $(t-3)^4$, since the only non-zero term in the determinant of $C - tI$ is the diagonal. Hence, by the Cayley-Hamilton theorem, the minimal polynomial is some divisor of that. We calculate that $C^2 - 6C + 9I$ is the zero matrix, hence, since I, C are linearly independent, the minial polynomial has degree > 1, so it is $(t-3)^2$.

Let R be the C-algebra generated (inside $\mathrm{Mat}(\mathbb{C}, 4, 4)$) by C. It is the set

$$\{0\} \cup \left\{ a_0 + a_1 C + \ldots a_N C^N \middle| a_i \in \mathbb{C}, N \geq 0 \right\}.$$

Since the different powers of C commute, this is a commutative C-subalgebra of the non-commutative C-algebra $\mathrm{Mat}(\mathbb{C}, 4, 4)$. In fact, since $C^2 = 6C - 9I$, the algebra generated by C is spanned, as a vector space, by I and C. However, the relation

$$(C - 3I)(C - 3I) = \mathbf{0}$$

shows that this algebra has zero-divisors, hence it is not a domain, and certainly **not a field!**

Consider the map

$$\mathbb{C}[t] \ni f(t) \mapsto f(C) \in \mathrm{Mat}(\mathbb{C}, 4, 4).$$

The image is the $\mathbb{C}$-algebra R generated by C.

The kernel of the map is $(t-3)^2$, so by the first isomorphism theorem $R \simeq \mathbb{C}[t]/((t-3)^2)$.

For any $a \in \mathbb{C}$, the map

$$\mathbb{C}[t] \ni g(t) \mapsto g(t+a) \in \mathbb{C}[t]$$

is a $\mathbb{C}$-algebra automorphism. If I is an ideal in $\mathbb{C}[t]$, the map

$$\mathbb{C}[t] \ni g(t) \mapsto g(t+a) + I \in C[t]/I$$

is surjective, and has kernel $I_a = \{\, g(t-a) | g(t) \in I \,\}$, so we get that

$$\mathbb{C}[t]/I_a \simeq C[t]/I.$$

This shows that

$$\mathbb{C}[t]/((t-3)^2) \simeq C[t]/((t)^2).$$

5. Let $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$, $g(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$.

   (a) Show that $E_1 = \mathbb{Z}_2[x]/(f(x))$ is a field, and find an inverse to $x + 1 + (f(x))$. 2 p

   (b) Show that $E_2 = \mathbb{Z}_2[x]/(g(x))$ is a field, and find all generators to its multiplicative group. 2 p

   (c) Show that $\mathbb{Z}_2[x]/(f(x)g(x))$ is isomorphic to the product of two fields. 1 p

   (d) Find the splitting fields of $f(x)$ and of $g(x)$. 1 p

   (e) Find the splitting fields of $f(x)g(x)$. 1 p

Solution: $f(x)$, which has degree 3, has no zero in $\mathbb{Z}_2$, hence it is irreducible, and its corresponding quotient is a field. Since

$$x^3 + x + 1 = (x + 1)(x^2 + x) + 1 \in \mathbb{Z}_2[x]$$

we have that $x_2 + x$ is an inverse of $x + 1$ in the quotient.

$g(x)$ is irreducible since it lacks zeroes. The quotient field has $2^3 = 8$ elements, so the multiplicative group has 7 elements, meaning that every element except for the identity is a generator.

We check that $f(x)$ and $g(x)$ are relatively prime, so the Chinese Remainder theorem shows that $\mathbb{Z}_2[x]/(f(x)g(x)) \simeq \mathbb{Z}_2[x]/(f(x)) \times \mathbb{Z}_2[x]/(g(x))$.

Let α be the image of x in E_1). Then α is a zero of f in E_1, hence $x - \alpha$ is a factor; in fact,

$$f(x) = (x + \alpha)(x + \alpha^2)(x + \alpha + \alpha^2) \in E_1$$

so $f(x)$ splits in E_1, which is the splitting field of $f(x)$.

Let similarly β be the image of x in E_2. We have that

$$g(x) = (x + \beta)(x + \beta^2)(x + \beta^2 + \beta + 1) \in E_2,$$

so $g(x)$splits in E_2, which is its splitting field.

Finally, viewing $g(x)$ as a polynomial in $E_1[x]$, it has the distinct zeroes $1 + \alpha$, $1 + \alpha^2$, and $1 + \alpha + \alpha^2$, hence

$$g(x) = (x + 1 + \alpha)(x + 1 + \alpha^2)(x + 1 + \alpha + \alpha^2)$$

splits in E_1 as well as in E_2. So E_1 is the splitting field for $f(x)(g(x)$.

6. Find the splitting fields for the following rational polynomials. Give the dimensions, as well as vector space bases, as well as primitive element for the extension.

   (a) $x^3 - 11$, 3 p

   (b) $x^4 + x^2 + 1$. 3 p

   Solution: The first case is similar to $x^3 - 2$, which we did in class, and which is treated in the textbook. The splitting field is $\mathbb{Q}(11^{1/3}, \omega)$ with $\alpha = 11^{1/3}$, and $\omega = \exp(2\pi i/3)$. The degree of the extension is $2 * 3 = 6$. One checks that $\omega + \alpha$ is a primitive element (it has neither degree 2 nor degree 3).

   We have that $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1) = (x - \omega)(x - \omega^2)(x + \omega)(x + \omega^2)$. Hence, the splitting field is $\mathbb{Q}(\omega)$, and the extension has degree 2. Clearly, ω is a primitive element.

7. Consider the recurrence equation

$$s_t + s_{t-3} + s_{t-5} = 0, \qquad s_0 = 1, s_1 = 0, s_2 = 0, s_3 = 0, s_4 = 0 \in \mathbb{Z}_2.$$

   Let $f(x) = x^5 + x^2 + 1$, and let $g(x) = \frac{1}{x^5} f(x)$.

   (a) Show that $f(x)$ and $g(x)$ are irreducible. 1 p

   (b) Put $R_1 = \mathbb{Z}_2[x]/(f(x))$ and $R_2 = \mathbb{Z}_2[x]/(g(x))$. Denote by ϕ_1 the linear map on R_1 given by multiplication with the image of x. Determine its matrix A_1 w.r.t. the basis $[1, x, x^2, x^3, x^4]$, and calculate the smallest n_1 such that $A_1^{n_1} = I$. Use this to determine the order of the image of x in the multiplicative group of R_1. Do the same for g. 1 p

   (c) Calculate the smallest positive integer m_1 such that $x^m - 1$ is divisible by $f(x)$. 1 p

   (d) Give an explicit formula for c_j for all $j \geq 0$. 2 p

Solution: $f(x)$ and $g(x)$ has no zeroes in $\mathbb{Z}_2$, and one can show that neither can be writted as a product of a quadratic and a qubic factor.

In R_1, we have the relation $x^5 = x^2 + 1$, so

$$\begin{aligned} x * 1 &= x \\ x * x &= x^2 \\ x * x^2 &= x^3 \\ x * x^3 &= x^4 \\ x * x^4 &= x^5 = x^2 + 1 \end{aligned}$$

and the matrix for multiplication by x is

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

Since the cyclic group R_1^* has 31 elements, x has order 31, so $A^{31} = I$.

From an exercise in the textbook we know that $x^{32} - x$ factors into the product of all irreducible polynomials of degree 1 or 5; hence $f(x)$ divides this polynomial, so it also divides $x^{31} - 1$. It is easy to see that it can divide no $x^s - 1$ for smaller s.

To give an explicit formula, we either calculate the 31 first values (after which the sequence repeats), or we find the roots of $f(x)$ in its splitting field. In fact, the splitting field is $E = Z_2/(f(x))$, and if we denote by γ the image of x in the quotient, we have that the zeroes are

$$\gamma, \gamma^2, \gamma^4, \gamma^8, \gamma^{16}.$$

Since $\gamma^5 = \gamma^2 + 1$ thses zeroes can also be expressed as

$$\gamma, \gamma^2, \gamma^4, \gamma^3 + \gamma^2 + 1, \gamma^4 + \gamma^3 + \gamma + 1.$$

So the general formula is

$$s_n = a_1\gamma^n + a_2\gamma^{2n} + a_3\gamma^{4n} + a_4\gamma^{8n} + a_5\gamma^{16n},$$

where the coefficients $a_i \in E$ are uniquely determined from initial conditions, by solving the system of 5 linear equations

$$\begin{aligned} 1 = s_0 &= a_1 + a_2 + a_3 + a_4 + a_5 \\ 0 = s_1 &= a_1\gamma^1 + a_2\gamma^2 + a_3\gamma^4 + a_4\gamma^8 + a_5\gamma^{16} \\ 0 = s_2 &= a_1\gamma^2 + a_2\gamma^4 + a_3\gamma^8 + a_4\gamma^{16} + a_5\gamma^{32} \\ 0 = s_3 &= a_1\gamma^3 + a_2\gamma^6 + a_3\gamma^{12} + a_4\gamma^{24} + a_5\gamma^{48} \\ 0 = s_4 &= a_1\gamma^4 + a_2\gamma^8 + a_3\gamma^{16} + a_4\gamma^{32} + a_5\gamma^{64} \end{aligned}$$

This yields

$$\begin{aligned} a_1 &= 1 + \gamma + \gamma^2 + \gamma^4 \\ a_2 &= \gamma^3 + \gamma^4 \\ a_3 &= 1 + \gamma + \gamma^2 \\ a_4 &= 1 + \gamma^2 + \gamma^4 \\ a_5 &= \gamma^2 + \gamma^3 + \gamma^4 \end{aligned}$$