Solutions to Exercises for TATA55, batch 4, 2022

January 19, 2023

1 Part two: no computer necessary

For this part, you may check your results using a computer, but you should do the exercises by hand. You may refer to any theorem and result in your texbook(s), prove your other assertions.

1. (3p) Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x]/(x^3 + cx^2 + 1)$ is a field.

   Solution: The quotient ring is a field iff the polynomial $f(x) = x^3 + cx^2 + 1 \in \mathbb{Z}_3[x]$ is irreducible, which, since it is of degree 3, occurs precisely when it lacks zeroes in Z_3. We have that

   $$f(0) = 2,\ f(1) = c + 2,\ f(-1) = c$$

   so for $c = 2$ we have that f has no zeroes in $\mathbb{Z}_3$.

2. (3p) Over which fields is the polynomial $f(x) = x^4 + x^3 + x + 1$ irreducible?

   Solution: If the characteristic is 2, then $f(1) = 1$, if the characteristic is not 2, then $f(-1) = 0$. In any case, $f(x)$ has zeroes in the prime subfieldm, so it is not irreducible.

3. (5p) Show that $f(x) = x^4 + 2x + 2$ is irreducible over $\mathbb{Q}$. Over which finite fields is it irreducible?

   Solution:

   - By Eisenstein, $f(x)$ is irreducible over Q.
   - Let p be a prime and $q = p^m$. If $f(x)$ is irreduciple over $GF(q)$, it will have a zero over the field $K = GF(q)[x]/(f(x)) \simeq GF(q^4)$, and in any extensions of that field. So it will always be reducible over $GF(p^{4n})$.
   - If $f(x)$ haz a zero in $\mathbb{Z}_p$, or equivalently if it has at least one linear factor over $\mathbb{Z}_p$, then it has a zero in any $GF(p^n)$, and is thus reducible over any $GF(p^n)$. This happens for

     $$p \in \{2, 5, 7, 11, 13, 17, 19, 23, 31, 47, 67, 71, 79, 83, 89, 101, 107, 109, 113, 131, 137, 151, 157, 173, 179, 181, 191, 193, 197, 211, 227, \dots\}$$

- It can happen that $f(x)$ factors as the product of two irreducible quadrics over $\mathbb{Z}_p$. It is then reduducible over all $GF(p^n)$. This happens for
$$p \in \{37, 43, 97, 101, 223, \dots\}$$
- For the remaining primes, $f(x)$ is irreducible over $\mathbb{Z}_p$ but splits over $GF(p^4)$, as well as over $GF(p^{4k})$ for all k. I believe that $f(x)$ factors as a product of two irreducible quadrics over $GF(p^{4k+2})$ and is irreducible over $GF(p^{4k+3})$ and over $GF(p^{4k+1})$.
- So it remains to explain the partitioning of the set of primes into three parts, as above. I can not. Maybe you can?

4. (4p) Show that $a = \sqrt{2} + \sqrt[3]{5}$ is algebraic over Q. Calculate $[\mathbb{Q}(a) : \mathbb{Q}]$.

   Solution:
$$\begin{aligned} a - \sqrt{2} &= \sqrt[3]{5} \\ (a - \sqrt{2})^3 &= 5 \\ a^3 - 3\sqrt{2}a^2 + 6a - 2\sqrt{2} &= 5 \\ a^3 + 6a - 5 &= 2\sqrt{2} \\ (a^3 + 6a - 5)^2 &= 8 \\ a^6 + 12a^4 - 10a^3 + 36a^2 - 60a + 25 &= 8 \\ a^6 + 12a^4 - 10a^3 + 36a^2 - 60a + 17 &= 0 \end{aligned}$$
   Since $x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$ is irreducible over $\mathbb{Q}$ (check!) we conclude that this is the minimal polynomial of a. Hence $[\mathbb{Q}(q) : \mathbb{Q}] = 6$, the degree of this polynomial.

5. (4p) Suppose that F is a finite field with q elements, and that $F \leq K$, and that $a \in K$ is algebraic over F. Show that $a^{q^m} = a$ for some positive integer m.

   Solution: Let $f(x) \in F[x]$ be irreducible, $f(a) = 0$. Let $m = \deg(f)$. Put $L = F(a)$. Then $[L : F] = m$.

   Since $L^* = L \setminus \{0\}$ is a group under multiplication, any $c \in L^*$ satisfies $c^{q^m - 1} = 1$. Multiplying with c, we have that any $c \in L$ satisfies $c^{q^m} = c$. In particular, $a^{q^m} = a$.

6. (6p) Suppose that $a, b \in \mathbb{Q}$ and that $m \in \mathbb{Z}$ is not a perfect square. Let $p(x) \in \mathbb{Q}[x]$ be a polynomial having $u = a + b\sqrt{m}$ as a zero. Show that $a - b\sqrt{m}$ is a zero of p as well.

   Solution: We have that $\sqrt{m} \notin \mathbb{Q}$, so consider the extension $\mathbb{Q}(\sqrt{m}$. Define the map
$$\begin{aligned} \theta &: \mathbb{Q}(\sqrt{m}) \to \mathbb{Q}(\sqrt{m}) \\ \theta(x + y\sqrt{m}) &= x - y\sqrt{m} \end{aligned}$$

We check that $\theta(r+s) = \theta(r) + \theta(s)$, $\theta(rs) = \theta(r)\theta(s)$, and that if $r \in \mathbb{Q}$ then $\theta(r) = r$. So θ is an automorphism of $\mathbb{Q}(\sqrt{m}$ which fixes $\mathbb{Q}$.

Now write

$$p(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0, \qquad c_j \in \mathbb{Q}.$$

Then

$$0 = p(u) = \theta(p(u)) = \theta\left(\sum_{j=0}^{n} c_j u^j\right) = \sum_{j=0}^{n} \theta(c_j u^j) = \sum_{j=0}^{n} \theta(c_j)\theta(u^j) = \sum_{j=0}^{n} c_j \theta(u)^j = p(\theta(u))$$

so $\theta(u) = a - b\sqrt{m}$ is a zero of $p(x)$.

Alternative solution (from one of your hand-ins): let

$$q(x) = (x - a - b\sqrt{m})(x - a + b\sqrt{m}) = x^2 - 2ax + b^2 - ma^2.$$

Divide (with remainder) $p(x)$ with $q(x)$ to obtain

$$p(x) = k(x)q(x) + r(x), \quad \deg(r(x)) < 2.$$

Since $p(a+b\sqrt{m}) = q(a+b\sqrt{m}) = 0$ we get that $r(a+b\sqrt{m}) = 0$. But $r(x)$ is a polynomial of degree at most one, with rational coefficients. Clearly $r(x)$ can not be a non-zero constant, and if $r(x) = cx + d$ with $c \neq 0$ then $0 = r(a + b\sqrt{m}) = c(a + b\sqrt{m}) = bc\sqrt{m} + ac$, which shows that $b = 0$; in this case, our result follows trivially.

If instead $r(x)$ is the zero polynomial then $p(x) = k(x)q(x) = k(x)(x - a - b\sqrt{m})(x - a + b\sqrt{m})$ which shows that $p(a - b\sqrt{m}) = 0$.

7. (4p) Let p be a prime number. Calculate the splitting field of $x^{p-1}-1 \in \mathbb{Z}_p[x]$.

   Solution: Let $f(x) = x^{p-1} - 1$. By Fermat, $a^{p-1} = 1$ for all $a \in \mathbb{Z}_p^*$, hence every $a \in \mathbb{Z}_p^*$ is a zero of $f(x)$. But $f(x)$ has degree $p-1$, so can not have more than $p-1$ zeroes. Since $f(x)$ is monic, it follows that

   $$x^{p-1} - 1 = \prod_{j=1}^{p-1}(x - j) \mod p$$

   so the polynomial splits already in $\mathbb{Z}_p$.

8. (9p) Find the splitting fields of the following cubic polynomials in $\mathbb{Q}[x]$:

(i) $x^3 - 3x - 1$

(ii) $x^3 - 3x - 2$

(iii) $x^3 - 3x - 3$

Solution:

(i) Let $f(x) = x^3 - 3x - 1$, $K = \mathbb{Q}[x]/(f(x)) = \mathbb{Q}(\alpha)$, α the image of x in K, $\tilde{f}(x)$ the polynomial f but with coefficients in K. Then

$$\tilde{f}(x) = (x - \alpha) \cdot (x - \alpha^2 + \alpha + 2) \cdot (x + \alpha^2 - 2)$$

so K is the splitting field, and since $f(x)$ is irreducible over Q, $[K : \mathbb{Q}] = 3$.

(ii) Let $f(x) = x^3 - 3x - 2$. Then $f(x) = (x - 2) * (x + 1)^2$, so it splits already in $\mathbb{Q}$. Thus $K = \mathbb{Q}$ and $[K : Q] = 1$.

(iii) Let $f(x) = x^3 - 3x - 3$, $K = \mathbb{Q}[x]/(f(x)) = \mathbb{Q}(\alpha)$, α the image of x in K, $\tilde{f}(x)$ the polynomial f but with coefficients in K. Then

$$\tilde{f}(x) = (x - \alpha) * (x^2 + \alpha * x + \alpha^2 - 3)$$

where the quadratic factor $q(x) \in K[x]$ is irreducible over K, since it has no zero in K. The splitting field is hence not K, but rather $L = K[y]/(q(y))$. By the tower theorem,

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 2 * 3 = 6.$$

2 Part one: computer assistance is helpful

1. (5p) Let $f(x) = x^5 + x^3 + 1 \in \mathbb{Z}_2[x]$. Let $K = \mathbb{Z}_2[x]/(f(x))$, and denote by $\bar{x}$ the coset $x + (f(x))$.

   (i) Show that K is a field, and vector space over $\mathbb{Z}_2$, with basis given by $\bar{x}^k$ for $0 \leq k \leq 4$.

   (ii) Show that $K \ni u \mapsto u\bar{x} \in K$ is an invertible linear map and give its matrix M w.r.t. the given basis.

   (iii) Find the eigenvalues (they live in some field extension)

   (iv) Find the dimension of $\mathrm{span}_{\mathbb{Z}_2}(M^0, M^1, M^2, \dots)$

   (v) Tabulate all possible values of M^k.

   Solution:

   (i) Follows if we can show that $f(x)$ is irreducible over $\mathbb{Z}_2$. It has no zeroes in $\mathbb{Z}_2$, so if it is reducible it has an irreducible quadratic factor; but the only irreducible quadric is $x^2 + x + 1$, and the remainder when dividing $f(x)$ by this quadric is $x + 1$, not zero.

(ii) Call the map T. Then $T(v+w) = (v+w)\bar{x} = u\bar{x} + w\bar{x} = T(v) + T(w)$ and $T(cv) = (cv)\bar{x} = c(v\bar{x}) = cT(v)$. Thus T is linear. Its matrix w.r.t. the given basis has as the j-th column (counting indices from zero) the coordinates of $\bar{x}^j\bar{x} = \bar{x}^{j+1}$; for the last column we need to use the relation

$$\bar{x}^5 = \bar{x}^3 + 1,$$

so the matrix is

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The determinant (in $\mathbb{Z}_2$ is 1, so the matrix, and hence the transformation, is invertible.

(iii) By construction, the characteristic polynomial of M is $f(x)$. The eigenvalues are thus the zeroes of $f(x)$, in the splitting field $F = \mathbb{Z}_2[x]/(f(x))$. In F we have have that $f(x)$ splits as

$$f(x) = (x+\alpha)*(x+\alpha^2)*(x+\alpha^3+\alpha^2)*(x+\alpha^4)*(x+\alpha^4+\alpha^3+\alpha)$$

where α is the image of x in the quotient. This gives the eigenvalues.

(iv) The ring homomorphism

$$\begin{aligned} \mathbb{Z}_2[2] &\to \mathrm{Mat}(\mathbb{Z}_2, 5, 5) \\ g(x) &\mapsto g(M) \end{aligned}$$

has as its image the subring generated by M. The kernel I is a principal ideal generated by an irreducible polynomial; by the Cayley-Hemilton theorem, it contains the characteristic polynomial. Since this is $f(x)$, which is irreducible, we get that $I = (f(x))$ and that the image is ismomorphic to K, which is a 5-dimensional vector space over $\mathbb{Z}_2$.

(v) We know that $M^5 = I + M^3$ and that

$$M^k = a_0(k)I + a_1(k)M + a_2(k)M^2 + a_3(k)M^3 + a_4(k)M^4$$

where

$$\alpha^k = a_0(k) + a_1(k)\alpha + a_2(k)\alpha^2 + a_3(k)\alpha^3 + a_4(k)\alpha^4$$

Since K^* is cyclic with $2^5 - 1 = 31$ elements, this sequence will be periodic with period 31. We tabulate the first 33 elements α^k, starting from $k = 0$:

$$\begin{gathered}\mathbf{1}, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^3 + 1, \alpha^4 + \alpha, \alpha^3 + \alpha^2 + 1, \\ \alpha^4 + \alpha^3 + \alpha, \alpha^4 + \alpha^3 + \alpha^2 + 1, \alpha^4 + \alpha + 1, \alpha^3 + \alpha^2 + \alpha + 1, \\ \alpha^4 + \alpha^3 + \alpha^2 + \alpha, \alpha^4 + \alpha^2 + 1, \alpha + 1, \alpha^2 + \alpha, \\ \alpha^3 + \alpha^2, \alpha^4 + \alpha^3, \alpha^4 + \alpha^3 + 1, \alpha^4 + \alpha^3 + \alpha + 1, \\ \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1, \alpha^4 + \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, \\ \alpha^3 + \alpha^2 + \alpha, \alpha^4 + \alpha^3 + \alpha^2, \alpha^4 + 1, \alpha^3 + \alpha + 1, \\ \alpha^4 + \alpha^2 + \alpha, \alpha^2 + 1, \alpha^3 + \alpha, \alpha^4 + \alpha^2, \mathbf{1}, \alpha, \alpha^2, \ldots\end{gathered}$$

2. (7p) Solve the reccurence equation

$$a_n = a_{n-2} - a_{n-3} \in \mathbb{Z}_3$$

with initial conditions $a_0 = 1$,$a_1 = a_2 = 0$, in the following way:

(i) Show that $f(x) = x^3 - x + 1 \in \mathbb{Z}_3[x]$ is irreducible.

(ii) Relate the splitting field K of f, the field $E = \mathbb{Z}_3[x]/(f(x))$, the cosets $x^k + (f(x))$, and the elements a_k.

(iii) Find the roots of r_1, r_2, r_3 in K.

(iv) The general formula is now

$$a_n = c_1 r_1^n + c_2 r_2^n + c_3 r_3^n$$

Determine $c_1, c_2, c_3 \in K$ using the initial conditions. If possible, simplify the resulting formula for a_n.

(v) The sequence $(a_n)_{n=0}^{\infty}$ is ultimately periodic. Determine the period! Does it divide the order of K^*?

Solution:

(i) $f(x)$ is of degree 3 and has no zeroes in $\mathbb{Z}_3$.

(ii) In E, we have that

$$f(x) = (x + 2\alpha) * (x + 2\alpha + 1) * (x + 2\alpha + 2)$$

where α is the image of x in the quotient, so $E = K$ is the splitting field. The relation $\alpha^3 = \alpha - 1$ gives that the sequence α^k is given by

$$\begin{gathered}1, \alpha, \alpha^2, \alpha + 2, \alpha^2 + 2 * \alpha, 2 * \alpha^2 + \alpha + 2, \alpha^2 + \alpha + 1, \alpha^2 + 2 * \alpha + 2, \\ 2 * \alpha^2 + 2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 2, \alpha^2 + 2, 2, \\ 2*\alpha, 2*\alpha^2, 2*\alpha+1, 2*\alpha^2+\alpha, \alpha^2+2*\alpha+1, 2*\alpha^2+2*\alpha+2, 2*\alpha^2+\alpha+1, \alpha^2+1, \\ 2 * \alpha + 2, 2 * \alpha^2 + 2 * \alpha, 2 * \alpha^2 + 2 * \alpha + 1, 2 * \alpha^2 + 1, 1, \alpha, \alpha^2, \alpha + 2\end{gathered}$$

and is periodic with period $K^* = 3^3 - 1 = 26$. If we look at constant coefficients

$$0, 0, 1, 0, 0, 2, 0, 2, 1, 2, 2, \ldots$$

they coincide with the a_k's! Se e.g. the wikipedia page on Linear feedback shift registers.

(iii) We have already seen that the roots are

$$\alpha, \alpha - 1, \alpha + 1$$

(iv) We get the equations

$$a_0 = 1 = c_1 + c_2 + c_3$$
$$a_1 = 0 = c_1\alpha + c_2(\alpha - 1) + c_3(\alpha + 1)$$
$$a_2 = 0 = c_1\alpha^2 + c_2(\alpha - 1)^2 + c_3(\alpha + 1)^2 = c_1\alpha^2 + c_2(\alpha^2 + \alpha + 1) + c_3(\alpha^2 - \alpha + 1)$$

This is equivalent to

$$\begin{pmatrix} 1 & 1 & 1 \\ a & a+2 & a+1 \\ a^2 & a^2+a+1 & a^2+2a+1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

which has the solution

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 2 * \alpha^2 + 1 \\ 2 * \alpha^2 + 2 * a \\ 2 * \alpha^2 + \alpha \end{pmatrix}$$

The general formula is thus

$$a_k = (1 - \alpha^2)\alpha^k + (-\alpha^2 - \alpha)(\alpha - 1)^k + (-\alpha^2 + \alpha)(\alpha + 1)^k.$$

(v) We have seen that the period length is maximal, i.e. $3^3 - 1 = 26$, and that the sequence is periodic, not just ultimately periodic.