Exercises for TATA55, batch 3, 2018

December 13, 2018

Solutions to the exercises below should be handed in no later than January 12, 2019.

You may use the result of the preceding (sub)exercises when solving the succeding ones, even if you have not managed to solve the earlier ones.

1 (30p) Elementary questions

1. (3p) Show that $p(t) = t^3 + t + 1 \in \mathbb{Z}_2[t]$ is irreducible, and find the inverse of $\alpha + 1$ in $E = \mathbb{Z}_2[t]/(p(t))$, where α is the image of t in E.
2. (3p) The element $\gamma \in \mathbb{C}$ has minimal polynomial $t^3 + t + 1$ over $\mathbb{Q}$. What is the minimal polynomial of $\gamma + \sqrt{2}$ over $\mathbb{Q}$?
3. (3p) Does $f(x) = 2x + 1 \in \mathbb{Z}_4[x]$ have a multiplicative inverse?
4. (4p) Let $\alpha = \sqrt{3} + i \in \mathbb{C}$. Determine the minimal polynomial of α over
   (a) $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$,
   (b) $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i)$, and $\mathbb{Q}(\sqrt{3}, i)$.
5. (5p) Determine the degrees of the splitting fields of the following polynomials with rational coefficients.
   (a) $x^4 + x^3 + x + 1$,
   (b) $x^4 + x^3 + x^2 + x + 1$,
   (c) $x^4 - 8x^2 + 8$,
   (d) $x^4 - 6x^2 + 2$,
   (e) $x^4 + x^3 + x^2 + x + 2$.
6. (3p) Find $\alpha \in \mathbb{C}$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(i\sqrt{2}, i\sqrt{3})$. What is the minimal polynomial of α over $\mathbb{Q}$?
7. (3p) Let p be a prime number, and let $f(x) = x^p - x \in \mathbb{Z}_p[x]$. Factor $f(x)$ into irreducible factors.
8. (3p) Let $f(x) = x^2 + x + 1 \in \mathbb{Q}[x]$, $I = (f(x))$, $R = \mathbb{Q}[x]/I$. For each positive integer n, determine $x^n + I$. Use this to show that $f(x) \mid (x^n + x + 1)$ iff $n \equiv 2 \mod 3$.
9. (3p) Let $\mathbb{Z}[i] = \{ a + ib \mid a, b \in \mathbb{Z} \} \subseteq \mathbb{C}$ be the ring of Gaussian integers. Let $z = 1 + i \in \mathbb{Z}[i]$, and let $I = (z)$. Show that I is a maximal ideal, and that $\mathbb{Z}[i]/I$ is a field with two elements.

2 (12p) Elaborate problems

1. (3p) Let R denote the set of all subsets of S_3. Introduce the addition $A + B = A \Delta B$ (symmetric difference) and multiplication

$$A * B = \{\, \sigma \in S_3 \,|\, ab = \sigma,\ a \in A,\ b \in B \text{ has an odd number of solutions} \,\}.$$

   (a) Show that R becomes a ring.

   (b) Show, by an example, that R is not commutative, nor a field.

   (c) Calculate

$$\{(), (1,2), (1,2,3)\} * \{(1,3), (2,3)\}$$

   (d) Let $u = \{(2,3), (1,2), (1,3)\}$, and put $v = u^2$. Show that v is a central idempotent, i.e., $v^2 = v$ and v commutes with everything.

2. (4p) Let $A \in M_n(\mathbb{C})$, the $\mathbb{C}$-algebra of n-by-n complex matrices.

   (a) Show that there exists a $\mathbb{C}$-sub-algebra S of $M_n(\mathbb{C})$ that is smallest among those that contain A. Show furthermore that S is commutative, and that it is of finite vector space dimension. Is it always a domain?

   (b) Show that for a polynomial $p(t) \in \mathbb{C}[t]$, $p(A) \in S \subseteq M_n(\mathbb{C})$. Show furthermore that the map

$$\mathbb{C}[t] \ni f(t) \mapsto f(A) \in S$$

   is a surjective $\mathbb{C}$-algebra homomorphism.

   (c) Denote the kernel of this map by $I = (g)$. The polynomial g is called the minimal polynomial of A. Show that g divides any polynomial $h(t)$ for which $h(A) = 0$. Is g necessarily irreducible?

   (d) Let

$$A = \begin{bmatrix} 0 & -1 & 1 \\ 1 & 2 & -1 \\ 1 & 1 & 0 \end{bmatrix}.$$

   Calculate the characteristic polynomial $p(t) = \det(tI - A)$, and evaluate it at A. Factor $p(t)$, then try to find the minimal polynomial of A.

3. (4p) Let $R = \mathbb{Z}_2[t]$, let $S = \mathbb{Z}_2[[t]]$, and let $p(t) = t^5 + t^3 + 1 \in R \subseteq S$.

$$U = \left\{ \sum_{n \geq 0} c_n t^n \in S \,\middle|\, c_{m+5} + c_{m+3} + c_m = 0 \text{ for all } m \geq 0 \right\}$$

$$V = \{\, f(t) \in S \,|\, p(t)f(t) \in R,\ \deg(p(t)f(t)) < 5 \,\}$$

   (a) Show that $p(t)$ is irreducible.

   (b) Show that there is a unique $f(t) = \sum_{n \geq 0} c_n t^n \in U$ with $c_0 = c_1 = 1$,$c_2 = c_3 = c_4 = 0$, and determine a somewhat explicit formula for c_n.

   (c) Write this particular $f(t)$ as

$$f(t) = \frac{q(t)}{p(t)}, \quad \deg(q(t)) < 5$$

   (d) Factorize $p(t)$ in some extension field of $\mathbb{Z}_2$, and find an even more explicit formula for c_n.