Algebraic Structures, Solutions for Exam 2018

June 16, 2019

1 Question 1

a. The element $2+\sqrt{3}$ works.

b. Consider the subgroup of $\mathbb{Z}[\sqrt{3}]^{\times}$ generated by the element above:

$$< 2+\sqrt{3} >= \{(2+\sqrt{3})^n : n \in \mathbb{Z}\}.$$

Notice that this set is infinite. Then, in particular, $\mathbb{Z}[\sqrt{3}]^{\times}$ is inifite.

c. Read the proof of VI.1.5 Theorem in lecture notes.

d. This is an easy calculation.

e. By definition, one inclusion is trivial. For the other, take $a+b\sqrt{3} \in \mathrm{Ker}(\varphi)$. Then $a+5b = 0 \bmod 11$ which means that $a+5b = 11k$ for some $k \in \mathbb{Z}$. Then we have

$$a+b\sqrt{3} = (11k-5b)+b\sqrt{3} = 11k + b(-5+\sqrt{3})$$

which implies that

$$\mathrm{Ker}(\varphi) \subset 11 \cdot \mathbb{Z} + (-5+\sqrt{3}) \cdot \mathbb{Z}.$$

Clearly,

$$11 \cdot \mathbb{Z} + (-5+\sqrt{3}) \cdot \mathbb{Z} \subset 11 \cdot \mathbb{Z}[\sqrt{3}] + (-5+\sqrt{3}) \cdot \mathbb{Z}[\sqrt{3}]$$

which gives the result.

f. We are looking for an element $a+b\sqrt{3}$ such that

$$(a+b\sqrt{3}) \cdot \mathbb{Z}[\sqrt{3}] = 11 \cdot \mathbb{Z}[\sqrt{3}] + (-5+\sqrt{3}) \cdot \mathbb{Z}[\sqrt{3}].$$

If this equality is true, there must be an element $c+d\sqrt{3}$ such that

$$(a+b\sqrt{3})(c+d\sqrt{3}) = 11.$$

Solving this equation, we get

$$c = \frac{11a}{a^2-3b^2}, \quad d = \frac{11b}{-a^2+3b^2}.$$

Notice that a^2-3b^2 is the norm of our potential generator. Since both c and d are integers, the element a^2-3b^2 must divide $11a$ and $11b$.

Let's pick $a = 1$ and $b = 2$ in which case $a^2 - 3b^2 = -11$ divides both $11a = 11$ and $11b = 22$. I claim that this element generates the kernel.

The equality
$$1 + 2\sqrt{3} = 1 \cdot 11 + 2 \cdot (-5 + \sqrt{3}),$$
gives one inclusion. On the other hand we have
$$11 = (1 + 2\sqrt{3})(-1 + 2\sqrt{3}), \quad -5 + \sqrt{3} = (1 + 2\sqrt{3})(1 - \sqrt{3})$$
which give the other inclusion.

2 Question 2

By $\mathrm{M}_2(\mathbb{F}_2)$ we denote the ring consisting of all 2×2 matrices with coefficients in $\mathbb{F}_2$. Let $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$[1]. Furthermore, $\mathrm{ev}_A : \mathbb{F}_2[x] \to \mathrm{M}_2(\mathbb{F}_2)$ denotes evaluation at A.

2.1 Preliminaries

Before we start answering the questions, note first that ev_A is a ring homomorphism as in Example III.2.4. Indeed, consider the ring homomorphism
$$\phi : \mathbb{F}_2 \to \mathrm{M}_2(\mathbb{F}_2) \tag{1}$$
given by
$$0 \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} =: O, \tag{2}$$
$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} =: I. \tag{3}$$
Then the matrix A commutes with all elements in the image of ϕ (as in Example III.2.4), so we can use Theorem III.2.1(c) to obtain the desired ring homomorphism $\mathrm{ev}_A : \mathbb{F}_2[x] \to \mathrm{M}_2(\mathbb{F}_2)$.

Secondly, note that $A^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, so that
$$A^2 + A + I = O. \tag{4}$$
This implies that $x^2 + x + 1 \in \mathbb{F}_2[x]$ maps to zero under the evaluation homomorphism ev_A. By using long division, we then obtain for every $f \in \mathbb{F}_2[x]$ a unique remainder r of degree < 2 such that
$$f = q \cdot (x^2 + x + 1) + r.$$
This representation will be used often in the upcoming questions.

[1] I changed the notation for the matrix because ϕ is usually used in the book for homomorphisms. This notation is also in line with the notation used in Example III.2.4.

2.2 The question

(a) *Is* ev_A *surjective?* Answer: Consider the set S of all polynomials of degree strictly less than 2 inside $\mathbb{F}_2[x]$. We then have $\mathrm{ev}_A(S) = \mathrm{ev}_A(\mathbb{F}_2[x])$. Indeed, by the above considerations every element $f \in \mathbb{F}_2[x]$ can be uniquely written as $f = q\cdot(x^2+x+1)+r$, with r in S. Applying ev_A to this equation, we then have

$$\mathrm{ev}_A(f) = \mathrm{ev}_A(q)\mathrm{ev}_A(x^2+x+1) + \mathrm{ev}_A(r) = 0 + \mathrm{ev}_A(r) = \mathrm{ev}_A(r). \quad (5)$$

This shows that $\mathrm{ev}_A(f) \in \mathrm{ev}_A(S)$. Since f was arbitrary, we conclude that $\mathrm{ev}_A(\mathbb{F}_2[x]) \subset \mathrm{ev}_A(S)$. We already have $\mathrm{ev}_A(S) \subset \mathrm{ev}_A(\mathbb{F}_2[x])$ because $S \subset \mathbb{F}_2[x]$, so we conclude that $\mathrm{ev}_A(S) = \mathrm{ev}_A(\mathbb{F}_2[x])$.

Note now that S has 4 elements (namely: 0, 1, x, $x+1$), so $\mathrm{ev}_A(S) = \mathrm{ev}_A(\mathbb{F}_2[x])$ has at most 4 elements. Since $\mathrm{M}_2(\mathbb{F}_2)$ has 16 elements, we conclude that ev_A cannot be surjective.

(b) *Show that* x^2+x+1 *is the minimal polynomial of* A. Answer: By Example III.4.4, the minimal polynomial is the monic polynomial $m_A \in \mathbb{F}_2[x]$ such that $\mathrm{Ker}(\mathrm{ev}_A) = (m_{\mathrm{A}})$. We already saw in Equation 4 that $x^2+x+1 \in \mathrm{Ker}(\mathrm{ev}_A)$, so $(x^2+x+1) \subset \mathrm{Ker}(\mathrm{ev}_A)$. Since x^2+x+1 is irreducible (it has no zeros, so it is irreducible by Theorem V.1.3) in the principal ideal domain $\mathbb{F}_2[x]$, we find that (x^2+x+1) is maximal by Theorem V.2.4. The kernel of ev_A is not the entire ring (for instance I does not map to zero), so we conclude that $\mathrm{Ker}(\mathrm{ev}_A) = (x^2+x+1)$. We thus find that x^2+x+1 is the minimal polynomial of A.

(c) *Is* $\mathrm{Ker}(\mathrm{ev}_A)$ *a prime ideal?* Answer: As we saw in (*b*), it is maximal, so it is prime by Corollary IV.2.7.

(d) *Is* $\mathrm{ev}_A(\mathbb{F}_2[x])$ *a field?* Answer: By the first isomorphism theorem (Theorem II.3.7), we have that $\mathrm{ev}_A(\mathbb{F}_2[x]) \simeq \mathbb{F}_2[x]/(x^2+x+1)$. Since (x^2+x+1) is maximal, we have that $\mathbb{F}_2[x]/(x^2+x+1)$ is a field by Theorem IV.2.3. We conclude that $\mathrm{ev}_A(\mathbb{F}_2[x])$ is a field.

(e) *Determine a generator of the ideal* $\mathrm{Ker}(\mathrm{ev}_A)$. Answer: The minimal polynomial is the monic generator of the kernel of this homomorphism by definition. By part (*b*), the minimal polynomial is x^2+x+1. We conclude that x^2+x+1 is a generator of $\mathrm{Ker}(\mathrm{ev}_A)$.

(f) *How many elements does* $(\mathbb{F}_2[x]/\mathrm{Ker}(\mathrm{ev}_A))^\times$ *have?* Answer: By part (*d*), $\mathrm{ev}_A(\mathbb{F}_2[x])$ is a field. This implies that the unit group $(\mathbb{F}_2[x]/\mathrm{Ker}(\mathrm{ev}_A))^\times$ is the set of nonzero elements in this ring. By the considerations in part (*a*), $\mathrm{ev}_A(\mathbb{F}_2[x])$ has at most 4 elements. In fact, it has exactly four elements: x is mapped to $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $x+1$ is mapped to $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, 1 is mapped to I and 0 is mapped to O. We conclude that there are 3 nonzero elements in $\mathrm{ev}_A(\mathbb{F}_2[x])$ and thus $(\mathbb{F}_2[x]/\mathrm{Ker}(\mathrm{ev}_A))^\times$ has order 3.

3 Question 3

Let $f := x^3 - 2 \in \mathbb{F}_7[x]$ be a polynomial.
(a) We want to prove that $f \in \mathbb{F}_7[x]$ is irreducible. Since it is a cubic polynomial,

by theorem **V.1.3**, it is enough to prove that f does not have a zero in $\mathbb{F}_7$. We can do it by hand, by computing all possible values of $f(x)$ and seeing that there is no value with $f(x) = 0$, as it is given in the table:

x	$f(x)$
0	5
1	6
2	6
3	4
4	5
5	4
6	4

We could do it in a easier way, as we know that in this field, for all $x \neq 0$ holds $x^6 = 1$, implying that $x^3 = \pm 1$, therefore $x^3 - 2$ does not have roots in $\mathbb{F}_7$ since $x = 0$ is not a zero of f.
(b) Let $R := \mathbb{F}_7[x]/(f \cdot \mathbb{F}_7[x])$. By theorem **V.2.7** we conclude that R is a field because f is irreducible (and by theorem **V.2.4** we know that the ideal $f \cdot \mathbb{F}_7[x]$ is maximal in $\mathbb{F}_7[x]$).
(c) A polynomial $g(y) := y^3 - y + 2 \in \mathbb{F}_7$ is also irreducible, because it has no zeros in $\mathbb{F}_7$, as we can check from the table:

y	$g(y)$
0	2
1	2
2	1
3	5
4	6
5	3
6	2

Therefore, as in (a), we conclude that $R' = \mathbb{F}_7[y]/(g \cdot \mathbb{F}_7[y])$ is a field. Denote by β a zero of g in its splitting field. Then $R' \cong \mathbb{F}_7(\beta)$, by theorem **VII.2.5**. Fields R and R' are extensions of $\mathbb{F}_7$ by algebraic numbers α and β, respectively, whose minimal polynomials, f and g, are of degree three (we know that polynomials f and g are irreducible, so minimal for α and β). Then, by theorem **VII.3.3**, we conclude that

$$[R : \mathbb{F}_7] = \deg(f) = 3 = \deg(g) = [R' : \mathbb{F}_7],$$

i.e. both of these fields are cubic extensions of $\mathbb{F}_7$. Theorem **IX.1.1** states that a cubic extension of $\mathbb{F}_7$ is unique up to isomorphism, giving a desired conclusion $R \cong R'$.
(d) We know already one zero of a polynomial f, this is α. We see that the other roots of a polynomial f differ from α "by a multiplication of some third root of unity". In $\mathbb{F}_7$, there are all three third roots of unity. Namely, in characteristics 7, we have $2^3 = 1$ and $4^3 = 1$ (and of course $1^3 = 1$). So, the roots of f are α, 2α and 4α, all of them are elements in R. So, Ω, the splitting field of f, is equal to R. As this is a cubic extension of $\mathbb{F}_7$, it has $7^3 = 343$ elements.
(e) Let α be a zero of a polynomial f in Ω. We want to determine its order in

a multiplicative group Ω^*. We know that $\alpha^3 = 2$. We also know that $2^3 = 1$ in $\mathbb{F}_7$, therefore in Ω too. So, $\alpha^9 = 1$ and if n is the order of α, then $n \mid 9$. As $\alpha \neq 1$ and we know that $\alpha^3 = 2 \neq 1$, the order cannot be smaller than 9. The order of α in Ω^* is 9.
(f) The map $\varphi : R \longrightarrow R$ is given by

$$\varphi(a + bx + cx^2 \pmod f) = a + 4bx + 2cx^2 \pmod f.$$

Since we know that $R \cong \mathbb{F}_7(\alpha)$, where $f(\alpha) = 0$, the map φ is the same as a map $\varphi : \mathbb{F}_7(\alpha) \longrightarrow \mathbb{F}_7(\alpha)$ given by

$$\varphi(a + b\alpha + c\alpha^2) = a + 4b\alpha + 2c\alpha^2.$$

(Recall that this is true because α is the image of x under the isomorphism $i : R \cong \mathbb{F}_7(\alpha)$, $i(x \pmod f) = \alpha$.) We need to check that φ is an automorphism. So, we need to check that
(1) $\varphi(0) = 0$, which follows when we put $a = b = c = 0$;
(2) $\varphi(1) = 1$, which follows for $a = 1$, $b = c = 0$;
(3) φ is compatible with $+$

$$\varphi((a_1+b_1\alpha+c_1\alpha^2))+(a_2+b_2\alpha+c_2\alpha^2)) = \varphi((a_1+a_2)+(b_1+b_2)\alpha+(c_1+c_2)\alpha^2) =$$
$$= (a_1+a_2)+4(b_1+b_2)\alpha+2(c_1+c_2)\alpha^2 = (a_1+4b_1\alpha+2c_1\alpha^2)+(a_2+4b_2\alpha+2c_2\alpha^2) =$$
$$= \varphi(a_1 + b_1\alpha + c_1\alpha^2) + \varphi(a_2 + b_2\alpha + c_2\alpha^2);$$

(4) φ is compatible with $\cdot$, we compute both expressions

$$\varphi((a_1 + b_1\alpha + c_1\alpha^2)) \cdot (a_2 + b_2\alpha + c_2\alpha^2)) =$$
$$= \varphi((a_1a_2 + 2b_1c_2 + 2c_1b_2) + (a_1b_2 + b_1a_2 + 2c_1c_2)\alpha + (a_1c_2 + b_1b_2 + c_1a_2)\alpha^2)) =$$
$$= (a_1a_2 + 2b_1c_2 + 2c_1b_2) + 4(a_1b_2 + b_1a_2 + 2c_1c_2)\alpha + 2(a_1c_2 + b_1b_2 + c_1a_2)\alpha^2,$$
$$\varphi(a_1+b_1\alpha+c_1\alpha^2)\cdot\varphi(a_2+b_2\alpha+c_2\alpha^2) = (a_1+4b_1\alpha+2c_1\alpha^2))\cdot(a_2+4b_2\alpha+2c_2\alpha^2) =$$
$$= (a_1a_2 + 2b_1c_2 + 2c_1b_2) + 4(a_1b_2 + b_1a_2 + 2c_1c_2)\alpha + 2(a_1c_2 + b_1b_2 + c_1a_2)\alpha^2,$$

keeping in mind that we compute in characteristics 7, i.e. $7x = 0$, for all x. We see that we get the same expressions, so φ is compatible with $\cdot$;
(5) φ is injective. We already know that as all field homomorphisms are injective, and from (1)-(4) it follows that φ is a field homomorphism. But we can explicitly check that as

$$\varphi(a + b\alpha + c\alpha^2) = a + 4b\alpha + 2c\alpha^2 = 0$$

implies $a = b = c = 0$, so $\ker(\varphi) = 0$.
(6) φ is surjective. We want to find a preimage for any $A + B\alpha + C\alpha^2$. From the definition of φ, we see that

$$\varphi(A + 2B\alpha + 4C\alpha^2) = A + B\alpha + C\alpha^2,$$

remembering that $7B = 7C = 0$. So, φ is indeed the automorphism of R.

There is an easier way to prove this fact. We know by theorem **VIII.1.5**(i) that all $\mathbb{F}_7$-automorphisms of $\mathbb{F}_7(\alpha)$ map α into some other root of a polynomial f. So, α can be mapped to α, 2α or 4α. We see that $\varphi(\alpha) = 4\alpha$. It is enough to give the image $\varphi(\alpha)$ to determine a homomorphism since all elements of $\mathbb{F}_7(\alpha)$ can be expressed as a combination of α and elements of $\mathbb{F}_7$. We want to extend the map φ. Then

$$\varphi(\alpha^2) = \varphi(\alpha \cdot \alpha) = \varphi(\alpha) \cdot \varphi(\alpha) = 4\alpha \cdot 4\alpha = 2\alpha^2$$

and then by additivity

$$\varphi(a + b\alpha + c\alpha^2) = a + 4b\alpha + 2c\alpha^2.$$

By construction of φ, it is a field homomorphism. To prove that it is an automorphism, it is enough to do the final part and to prove that $\varphi \circ \varphi \circ \varphi = \mathrm{id}$ because then follows that $\varphi \circ \varphi$ is an inverse of φ. There are (at least) three ways to do it. The first one is to prove it by direct computation. The other one is to note that the map φ is linear and can be represented in a basis $[1, \alpha, \alpha^2]$ as a matrix

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

and to compute that M^3 is the identity matrix. Finally, the third way is determine the image of α. We compute that $\varphi(\varphi(\varphi(\alpha))) = \varphi(\varphi(4\alpha)) = \varphi(2\alpha) = \alpha$, and since it is identity on $\mathbb{F}_7$ and on α it is the identity on the whole $\mathbb{F}_7(\alpha)$. So, φ has the order 3 because $\varphi \neq \mathrm{id}$.