MATH-UA 349: Homework 2

James Pagan, February 2024

Professor Kleiner

Contents

1 Problem 1 2

2 Problem 2 2

3 Problem 3 3

4 Problem 4 4

5 Problem 5 4

6 Problem 6 5

7 Problem 7 6

8 Problem 8 7

9 Problem 9 7

10 Problem 10 8

1 Problem 1

Let α be algebraic, and suppose n is the smallest integer for which there exist $b_n, \ldots, b_0 \in \mathbb{C}$ such that

$$b_n(\alpha)^n + \cdots + b_1(\alpha) + b_0 \;=\; 0.$$

Consider the complex vector space $\mathbb{C}[\alpha] \,/\, (b_n(\alpha)^n + \cdots + b_1(\alpha) + b_0)$. We claim that all polynomials $p \in \mathbb{C}[\alpha]$ with $\deg p \geq n$ are equivalent to some $p \in \mathbb{C}[\alpha]$, which is either zero or has degree smaller than n. We prove this via the division algorithm: there exists polynomials q and r such that

$$\begin{aligned} p &= q\big(b_n(\alpha)^n + \cdots + b_1(\alpha) + b_0\big) + r \\ &. = q(0) + r \\ &= r, \end{aligned}$$

where $r = 0$ or $\deg r < n$. Thus the elements of $\mathbb{C}[\alpha] \,/\, (b_n(\alpha)^n + \cdots + b_1(\alpha) + b_0)$ are of the form

$$c_{n-1}(\alpha)^{n-1} + \cdots + c_1(\alpha) + c_0$$

for $c_{n-1}, \ldots, c_0 \in \mathbb{C}$. None of these polynomials are zero by the minimality of n. It is clear that this space is spanned the linearly independent list $1, \alpha, \ldots, \alpha^{n-1}$ — thus it has dimension n.

The proof ends here, since the finite-dimensional vector space $\mathbb{C}[\alpha] \,/\, (b_n(\alpha)^n + \cdots + b_1(\alpha) + b_0)$ is spanned by $\{\alpha_n\}_{n \geq 0}$.

2 Problem 2

Part (a)

Proof. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of R. Let us verify the conditions that $\mathfrak{a} + \mathfrak{b}$ is an ideal:

1. **Additive**: Since $(R, +)$ is an Abelian group with subgroups $(\mathfrak{a}, +)$ and $(\mathfrak{b}, +)$, $\mathfrak{a} + \mathfrak{b}$ is an additive subgroup of R.
2. **Multiplicative**: Let $r \in R$ and $a + b \in \mathfrak{a} + \mathfrak{b}$ (with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$). Then $ra \in \mathfrak{a}$ and $rb \in \mathfrak{b}$, so $r(a + b) = ra + rb \in \mathfrak{a} + \mathfrak{b}$.

We conclude that $\mathfrak{a} + \mathfrak{b}$ is an ideal of R. To see that $\mathfrak{a} \cap \mathfrak{b}$ is an ideal, we have the following:

1. **Additive**: Since $(R, +)$ is an Abelian group with subgroups $(\mathfrak{a}, +)$ and $(\mathfrak{b}, +)$, $\mathfrak{a} \cap \mathfrak{b}$ is an additive subgroup of R.

2. **Multiplicative**: Let $r \in R$ and $x \in \mathfrak{a} \cap \mathfrak{b}$. Then $x \in \mathfrak{a}$ and $x \in \mathfrak{b}$, so $rx \in \mathfrak{a}$ and $rx \in \mathfrak{b}$. We deduce that $rx \in \mathfrak{a} \cap \mathfrak{b}$.

Hence, $\mathfrak{a} \cap \mathfrak{b}$ is an ideal of R. □

Part (b)

Proof. Suppose $\mathfrak{a} = (a)$ and $\mathfrak{b} = (b)$ are ideals of R. We claim that $\mathfrak{ab} = (ab)$ by the following:

1. Suppose $x \in \mathfrak{ab}$; then $x = a_0 b_0$ for some $a_0 \in (a)$ and $b_0 \in (b)$. In turn, $a_0 = ra$ and $b_0 = sb$ for some $r, s \in R$. Hence $x = rsab$, so $x \in (ab)$. We deduce that $\mathfrak{ab} \subseteq (ab)$.
2. Suppose $x \in (ab)$; then $x = rab$ for some $r \in R$. Since $ra \in (a)$ and $b \in (b)$, we see that $x = (ra)(b) \in \mathfrak{ab}$. We deduce that $(ab) \subseteq \mathfrak{ab}$.

Hence $\mathfrak{ab} = (ab)$, so $\mathfrak{ab}$ is an ideal. This result is false in general: consider the product of ideals

$$\boxed{(x, y) \times (z) \subseteq \mathbb{Z}[x, y, z]}.$$

It is clear that $z(x+y)$ and $z^2(x)$ lie in $(x, y) \times (z)$. However, their sum has the factorization

$$z(x + y) + z^2(x) = z(zx + x + y),$$

which does not belong to $(x, y) \times (z)$ since no factor lies in (x, y). We conclude that $(x, y) \times (z)$ is not an ideal.

□

3 Problem 3

Part (a)

Proof. Select $x \in [0, 1]$ arbitrarily. Define F as the set containing the sets $S_a \stackrel{\text{def}}{=} \{f \in \mathcal{C}\big([0, 1]\big) \mid f(0) = a\}$ for all $a \in \mathbb{R}$, endowed with the following operations:

$$S_a + S_b = S_{a+b} \qquad \text{and} \qquad S_a S_b = S_{ab}.$$

It is trivial that F is a field under these operations. The nontrivial properties of this verification are elaborated upon below:

1. **Additive Conditions**: The additive identity is clearly S_0, and the additive inverse of S_a for $a \in \mathbb{R}$ is S_{-a}.

2. **Multiplicative Conditions**: The multiplicative identity is clearly S_1, and the multiplicative inverse of S_a for nonzero $a \in \mathbb{R}$ is $S_{1/a}$.

3. **Distributive Laws**: The distributive laws on F follow from those on $\mathbb{R}$.

Thus F is a field. Define a mapping $\phi : \mathcal{C}\big([0,1]\big) \to F$ by $\phi(f) = S_{f(x)}$. Observe that for all $f, g \in \mathcal{C}\big([0,1]\big)$, we have

$$\phi(f+g) = S_{f(x)+g(x)} = S_{f(x)} + S_{g(x)} = \phi(f) + \phi(g)$$
$$\phi(fg) = S_{f(x)g(x)} = S_{f(x)}S_{g(x)} = \phi(f)\phi(g).$$

Noting that $\phi(1) = S_1$, yields that ϕ is a homomorphism. The kernel of ϕ is I_x: all $f \in \mathcal{C}\big([0,1]\big)$ such that $f(x) = 0$. Thus I_x is an ideal of $\mathcal{C}\big([0,1]\big)$, and

$$\mathcal{C}\big([0,1]\big) \,/\, I_x \cong F$$

is an isomorphism. Thus $\mathcal{C}\big(0,1\big) \,/\, I_x$ is a field, so I_x must be maximal. □

4 Problem 4

Proof. It is clear that $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$, so

$$\alpha^5 - 1 = (\alpha - 1)(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) = (\alpha - 1)(0) = 0$$

and $\alpha^5 = 1$. Therefore,

$$(\alpha^3 + \alpha^2 + \alpha)(\alpha^5 + 1) \;=\; (\alpha^3 + \alpha^2 + \alpha)2 = \boxed{2\alpha^3 + 2\alpha^2 + 2\alpha}.$$

□

5 Problem 5

Part (a)

Proof. Suppose that $\beta \in \overline{R}$ has the representation $\beta = r_n\alpha^n + \cdots + r_1\alpha + r_0$ for some $r_0, \ldots, r_n \in R$. Then

$$a^n\beta = r_n(a^n\alpha^n) + \cdots + r_1(a^n\alpha) + r_0(a^n) \tag{1}$$
$$= r_0a_n + r_1a^{n-1} + \cdots + r_n, \tag{2}$$

which is a constant polynomial. Then there exists b such that $\overline{b}$ is the expression (2), which is $a^n\beta$. We conclude that $\beta = \alpha^n\overline{b}$. □

Part (b)

Proof. A clear corollary of Part (a) is that $\phi(b) = \alpha^k \overline{b}$ for some integer k. Therefore,

$$\begin{aligned} \phi(b) = 0 &\iff \alpha^k b = 0 \quad \text{for some } k \\ &\iff \alpha^k b(a^{2k}) = 0(a^{2k}) = 0 \quad \text{for some } k \\ &\iff a^k b = 0 \quad \text{for some } k, \end{aligned}$$

as desired. □

Part (c)

Proof. Using the result from Part (b), we utilize the following chain of equivalencies: for all $b \in R$,

$$\begin{aligned} \phi(b) = 0 \quad \text{for all } b \in R &\iff a^k b = 0 \quad \text{for all } b \in R \text{ and some } k \\ &\iff a^k(1) = 0 \quad \text{for some } k \\ &\iff a \text{ is nilpotent.} \end{aligned}$$

This completes the proof. □

6 Problem 6

Part (a)

Proof. Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are disjoint relateively prime ideals of R. We claim that

$$R \cong (R \,/\, \mathfrak{b}) \times (r \,/\, \mathfrak{a})$$

by the following isomorphism: if $x \in R$ and $x = a + b$ for $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$, then $\phi(a + b) = (a, b)$.

Claim 1. *ϕ is a homomorphism.*

Proof. We are ready to prove the two homomorphism identities. If we let $x = a_1 + b_1$ and $y = a_2 + b_2$, we have

$$\begin{aligned} \phi(x + y) &= \phi(a_1 + a_2 + b_1 + b_2) \\ &= (a_1 + a_2, b_1 + b_2) \\ &= (a_1, b_1) + (a_2, b_2) \\ &= \phi(x) + \phi(y). \end{aligned}$$

As for the multiplicative condition, observe that $a_1 b_2 \in \mathfrak{a}$ and $a_1 b_2 \in \mathfrak{b}$, so $a_1 b_2 = 0$. Similarly $b_1 a_2 = 0$, so

$$\begin{aligned}
\phi(xy) &= \phi\big((a_1 + b_1)(a_2 + b_2)\big) \\
&= \phi(a_1 a_2 + a_1 b_2 + b_1 a_2 + b_1 b_2) \\
&= \phi(a_1 a_2 + b_1 b_2) \\
&= (a_1 a_2, b_1 b_2) \\
&= (a_1, b_1)(a_2, b_2) \\
&= \phi(x)\phi(y).
\end{aligned}$$

Since the unital condition is trivial, we conclude that ϕ is a homomorphism.

It is clear that ϕ is surjective: for all $(a, b) \in (R \,/\, \mathfrak{b}) \times (R \,/\, \mathfrak{a})$, we have $\phi(a + b) = (a, b)$. Injectivity follows from the fact the representation $x = a + b$ is unique. Suppose we set $x = a_1 + b_1 = a_2 + b_2$ (for $a_1, a_2 \in \mathfrak{a}$ and $b_1, b_2 \in \mathfrak{b}$). Then $a_1 - a_2 = b_1 - b_2$ thus each side must be zero, implying $a_1 = a_2$ and $b_1 = b_2$. We deduce that ϕ is the desired isomorphism. □

Part (b)

Proof. The idempotents that generate $(R \,/\, \mathfrak{b}) \times (R \,/\, \mathfrak{a})$ are the elements $(0, 1)$ and $(1, 0)$ — which if we let $a + b = 1$, are

$$\boxed{b \text{ and } a},$$

or equivalently $1 - a$ and $1 - b$. This may be verified by a quick computation. □

7 Problem 7

Part (a)

Proof. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of R such that $\mathfrak{a} + \mathfrak{b} = R$. We make two claims:

1. Suppose $ab \in \mathfrak{ab}$ for $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. Then as $\mathfrak{a}$ is an ideal, $ab \in \mathfrak{a}$; likewise, $ab \in \mathfrak{b}$. We deduce that $ab \in \mathfrak{a} \cap \mathfrak{b}$, so $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

2. Suppose $x \in \mathfrak{a} \cap \mathfrak{b}$; then $x \in \mathfrak{a}$ and $x \in \mathfrak{b}$. If we define $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$, we obtain $xa \in \mathfrak{ba}$ and $xb \in \mathfrak{ab}$. Thus $x = xa + xb \in \mathfrak{ab}$, so $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab}$.

We conclude that $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. □

Part (b)

Proof. Suppose $\mathfrak{a} + \mathfrak{b} = R$, and $c, d \in R$. Let $a + b = 1$ (where $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$); we claim $\boxed{ad + bc}$ lies in $c + \mathfrak{a}$ and $d + \mathfrak{b}$. For the first relation, we have

$$ad + bc \equiv bc \equiv (1 - a)c \equiv c \pmod{\mathfrak{a}}$$

and for the second relation, we have

$$ad + bc \equiv ad \equiv (1 - b)d \equiv d \pmod{\mathfrak{b}}.$$

This completes the proof. □

8 Problem 8

Proof. The answer is $\boxed{\text{false}}$; there are no integral domains of order 15. Suppose for contradiction that such an ring R exists. We utilze the following claim:

Claim 2. *All finite domains are fields.*

Proof. Let R be a finite domain. Then for nonzero $a \in R$, consider the set

$$\{a, a^2, \ldots, a^{|R|+1}\}.$$

By the Pigeonhole Principle, two elements of this set must be equal: $a^i = a^j$ for $i, j \in \{1, \ldots, n\}$ with $i < j$. Then $a^{i-j} = 1$ and $a^{i-j-1} = a^{-1}$, so all nonzero elements of R are invertible. We conclude that R is a field.

Thus, R is a field. We attain the desired contradiction noting that no finite field of order 15 exists. □

9 Problem 9

Proof. Let R be a ring of order 10. The additive group $(R, +)$ is a finite Abelian group of order ten, of which there is one possibility: C_{10}. Then R has four additive generators — namely, elements of order 10.

Claim 3. *The multiplicative identity e of R has additive order* 10.

Proof. Let $g \in R$ have additive order 10. Lagrange's Theorem ensures that the additive order of e must divide ten; if e has order 2, then

$$0 \neq g + g = g(e + e) = e(0) = 0,$$

a contradiction. Assuming that e has order 5 yields similar nonsense:

$$0 \neq g + g + g + g + g = g(1 + 1 + 1 + 1 + 1) = g(0) = 0.$$

We conclude that e must have additive order 10.

Then we can define an isomorphism $R \cong \mathbb{Z}_{10}$ that maps the additive identity to 0 and the multiplicative identity to 1. Hence $\boxed{\text{all rings of order 10 are isomorphic to } \mathbb{Z}_{10}}$. □

10 Problem 10

Proof. The elements of the commutative ring $\mathbb{Z}_2[x] / (x^3 + x + 1)$ are precisely the eight polynomials in $\mathbb{Z}_2[x]$ of degree 2 or smaller, as ensured by the Division Algorithm. We must demonstrate that the seven nonzero polynomials are units: we have that

1. $1 \times 1 = 1$.
2. $x(x^2 + 1) = x^3 + x = 1$.
3. $(x + 1)(x^2 + x) = x^3 + 2x^2 + x = x^3 + x = 1$.
4. $(x^2 + x + 1)(x^2) = x^4 + x^3 + 1 = (x + 1)(x^3 + x + 1) - 2x - 1 = 1$.

We conclude that $\mathbb{Z}_2[x] / (x^3 + x + 1)$ is a field. Likewise, $\mathbb{Z}_3[x] / (x^3 + x + 1)$ consists of polynomials of degree two or smaller — however,

$$(x - 1)(x^2 + x - 1) = x^3 - 2x + 1 = x^3 + x + 1 = 0.$$

Thus $\mathbb{Z}_3[x] / (x^3 + x + 1)$ is not an integral domain, so it cannot be a field. □