(a) Give an example of a non-commutative ring without an identity. [4]

$R = M_{2\times 2}(2\mathbb{Z}) \longrightarrow$ 2×2 matrices with entries even integers.

(b) Does the equation $(1+a)(1-a) = 1 - a^2$ hold for any element a of a ring with identity? Explain. [4]

$$(1+a)(1-a) = (1-a) + a(1-a)$$

(D)

$$= 1 - a + a + a(-a)$$

(A2)

$$= 1 + 0 + a(-a)$$

$$= 1 + a(-a)$$

we proved in any ring.

$$= 1 - a^2$$

Yes.

(c) Give an example of a subring of $\mathbb{Z}/14\mathbb{Z}$ having 4 elements, or explain why it does not exist. [4]

It does not exist, because any subring of $\mathbb{Z}/14\mathbb{Z}$ needs to have a cardinality that divides 14.

(d) Prove, using the axioms of a ring or the basic properties proved in the lectures, that any two elements a, b of a ring satisfy the equation $(-a)b = -(ab)$. [6]

To show this, we want to show that the additive inverse of ab is $(-a)\cdot b$.

We have

(D) (A2)

$$ab + (-a)b = (a + (-a))\cdot b = 0 \cdot b = 0$$

$$ab + (-a)b \overset{(A?)}{=} (a + (-a)) \cdot b \overset{(A2)}{=} 0 \cdot b = 0$$

proved in the lectures for any ring.

(e) Give an example of a commutative ring without identity having a subring with identity, or explain why such an example cannot exist. **[6]**

$$4\mathbb{Z}/12\mathbb{Z} = \{[0]_{12}, \underbrace{[4]_{12}}_{\text{identity in this ring!}}, [8]_{12}\}$$

is a subring of

$$2\mathbb{Z}/12\mathbb{Z} = \{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}$$

none of these elements are an identity.

(f) Explain what is wrong in the following "proof" that every finite commutative ring with identity is a field. **[6]**

"Proof": Suppose R is a finite commutative ring with identity. Let a be a non-zero element of R. We want to show that there exists an inverse of a in R, that is, an element b such that $ab = ba = 1$. Consider the set $S = \{a, a^2, a^3, \dots\}$. Since R is finite, this set S must be finite. This means that there exist positive integers $m > n$ such that $a^m = a^n$. We then have $a^{m-n} = 1$, which means that the element a^{m-n-1} is a multiplicative inverse of a. Thus every non-zero element of R has an inverse, and therefore R is a field.

The problem is the step where

$$a^m = a^n \implies a^{m-n} = 1$$

as this is using the cancellative law, which only holds if the ring has no zero-divisors.

Question 2 [20 marks]. Consider the ring $R = \mathbb{Z}/15\mathbb{Z}$ and its ideal $I = \{[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\}$. [You are not required to prove that I is an ideal of R.]

(a) Is the ideal I a ring with identity? Explain. **[4]**

(Hint: $[9]_{15} = [-6]_{15}$ and $[12]_{15} = [-3]_{15}$)

We can chek that $[6]_{15}$ is an identity.

since $[6]_{15} \cdot x = x$ for all $x \in \mathbb{Z}/15\mathbb{Z}$.

(b) Write down explicitly the partition of R into cosets of I. **[6]**

The cosets are

$I = \{[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\}$

$[1]_{15} + I = \{[1]_{15}, [4]_{15}, [7]_{15}, [10]_{15}, [13]_{15}\}$

$[2]_{15} + I = \{[2]_{15}, [5]_{15}, [8]_{15}, [11]_{15}, [14]_{15}\}$

(c) Give an explicit isomorphism between the rings $\mathbb{Z}/3\mathbb{Z}$ and R/I. [You do not need to prove that it is an isomorphism.] **[4]**

$$R/I \longrightarrow \mathbb{Z}/3\mathbb{Z}$$

$$I \longmapsto [0]_3$$

$$[1]_{15} + I \longmapsto [1]_3$$

$$[2]_{15} + I \longmapsto [2]_3.$$

(d) Does the equation $x^3 + x^5 + x^7 = 1$ have a solution in the ring R/I? Explain. **[6]**

This does not have a solution in R/I (or $\mathbb{Z}/3\mathbb{Z}$

because no matter what x is, we can check manually that $x^3+x^5+x^7=0$.

(a) Give an example of a domain R and an element $a \in R$ that is neither a unit nor a zero-divisor. [4]

$R = \mathbb{Z}$ $\quad a = 2$.

(b) For which integers $m \geq 2$ does the ring $\mathbb{Z}/m\mathbb{Z}$ satisfy the cancellative law for multiplication? Explain. [4]

The cancellative law is satisfied in integral domains, and $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if <u>m is prime</u>.

(c) Consider the subring $S = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$ of the ring $\mathbb{R}$ of real numbers.

(i) Explain why S is an integral domain. [4]

(ii) Show that the element $2+\sqrt{3}$ is a unit of S. [4]

(iii) Find a factorisation of the element $6 \in S$ as a product of two elements of S that are not in $\mathbb{Z}$. [4]

(iv) Given that the element $6 \in S$ can also be factored as $6 = 2 \cdot 3$, can we conclude that S is not a unique factorisation domain? Explain. [4]

(i) S is an integral domain because it is a subring with identity of an integral domain ($\mathbb{R}$).

(ii) $2+\sqrt{3}$ is a unit because

$$(2+\sqrt{3})\underbrace{(2-\sqrt{3})}_{\text{inverse}} = 4-3 = 1$$

(iii) $6 = 9 - 3 = (3+\sqrt{3})(3-\sqrt{3})$.

(iv) No, we cannot conclude it is a UFD as we don't know these are factorisations into irreducibles, nor that they are not the same factorisation up to irreducibles.

(d) Suppose R is a domain and $a \in R$ is a non-zero element satisfying $a^3 = a$. Show that a is either a unit or a zero-divisor. [**6**]

$$a^3 = a$$

$$a^3 - a = 0$$

$$a(a^2-1) = 0.$$

If a^2-1 is not zero, a is a zero divisor.

If $a^2 - 1 = 0 \Rightarrow a^2 = 1 \Rightarrow a$ is a unit $(a^{-1} = a)$. ∎

Question 4 [20 marks]. Consider the field of 2 elements $K = \mathbb{Z}/2\mathbb{Z}$ and the polynomial $f = x^3 + x + 1 \in K[x]$.

(a) Explain why f is an irreducible element of $K[x]$. [**6**]

If f could be factored as $f = g \cdot h$ then one factor must have degree 2 (say g) and the have degree 2 (say g) and

other would have degree 1 (say h).

If $h = x + a$ then $-a$ is a root of h, and so $-a$ is also a root of f. But $f(0) = 1$ and $f(1) = 1$ so f has no roots.

WARNING

Q: Is $f = x^4 + 2x^2 + 1$ irreducible in $\mathbb{R}[x]$.

No: $f = (x^2+1)(x^2+1)$.

But f has no roots.

(b) Let F be the quotient ring $F = K[x]/\langle f\rangle$, which contains the field K.

(i) Explain why F is a field. [You may use any result proved in the lectures.] [4]

(ii) How many elements does the field F have? [4]

(iii) Let α be an element of F such that $f(\alpha) = 0$. Find an expression for the inverse α^{-1} of the form $\alpha^{-1} = a \cdot \alpha^2 + b \cdot \alpha + c$ with $a, b, c \in K$. [6]

(i) Since f is irreducible then $\langle f \rangle$ is a maximal ideal, so $K[x]/\langle f \rangle$ is a field.

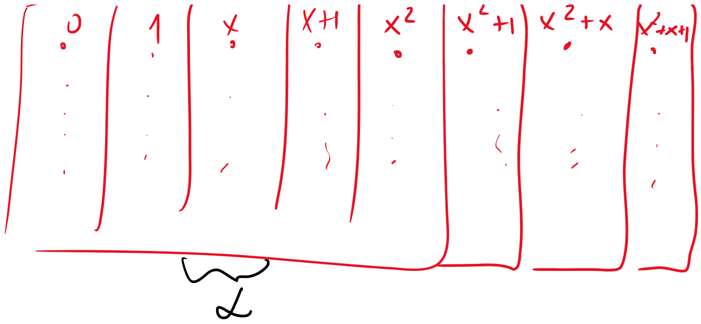
(ii) $f = x^3 + x + 1$

$\mathbb{Z}_2[x]$

0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1

$K[x]/$

Every coset of $K[x]/\langle f \rangle$



can be represented uniquely as $a\alpha^2 + b\alpha + c$ where $a, b, c \in \mathbb{Z}/2\mathbb{Z}$

$\alpha = [x]$.

So there are 8 possibilities.

(iii) If $\alpha^3 + \alpha + 1 = 0$ then

$$\alpha^3 + \alpha = 1$$

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

So $\alpha^{-1} = \alpha^2 + 0\alpha + 1$.