# 2012 Q7)

Let $p \geq 2$ be a prime integer. Let $R$ be the subset of $\mathbb{Q}$ consisting of elements that can be written as $a/b$ where $a \in \mathbb{Z}$ and $b$ is a power of $p$, i.e.

$$R := \left\{ \frac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z},\ b = p^n, \text{ where } n \in \mathbb{Z},\ n \geq 0 \right\}.$$

i) Show that $R$ is a subring of $\mathbb{Q}$ (with identity).

ii) Show that $R$ is an integral domain but not a field.

iii) Find all units in $R$.

iv) Show that each ideal in $R$ is principal.

**Remark**

This ring $R$ is an example of a construction called 'localisation of a ring'. $R$ is the 'localisation' of $\mathbb{Z}$ at the prime $p$.

# Subrings - Q7i)

Q7i) Show that $R := \{ \frac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z},\ b = p^n, \text{ where } n \in \mathbb{Z},\ n \geq 0 \}$ is a subring of $\mathbb{Q}$ (with identity).

## Definition (Def 3.3, Subring)

A subring $R$ of a ring $S$ is a set $R \subseteq S$ such that

- The zero element $0_S \in R$
- The multiplicative identity $1_S \in R$
- For every $a, b \in R$, the sum $a + b \in R$
- For every $a, b \in R$, the product $ab \in R$
- For every $a \in R$, the (additive) inverse $-a \in R$

# Integral domains/Fields - Q7ii)

Q7ii) Show that $R = \{ \frac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z},\ b = p^n$, where $n \in \mathbb{Z},\ n \geq 0 \ \}$ is an integral domain but not a field

**Definition (Def 4.1, Integral domain)**

A ring $R$ is called an integral domain if

- it is commutative,
- has at least two elements $0_R \neq 1_R$, and
- has no zero divisors apart from 0. (I.e. in $R$, $ab = 0$ implies $a = 0$, or $b = 0$.)

**Definition (Def 3.7, Field)**

A ring $R$ is called a field if

- It is commutative,
- has at least two elements $0_R \neq 1_R$, and
- for any $a \neq 0 \in R$, there $b \in R$ such that $ab = 1$. (This $b$ is the inverse of $a$)

# Units - Q7iii)

Q7iii) Find all units in $R = \{ \frac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z},\ b = p^n$, where $n \in \mathbb{Z},\ n \geq 0 \}$.

## Definition (on pg 12, Units)

Let $R$ be a ring. Then $a \in R$ is called a unit if

- there exists $b \in R$ such that $ab = ba = 1$.

## Fact

If $F$ is a field, every non-zero element is a unit.

# Principal ideals - Q7iv)

Q7iv) Show that each ideal in $R = \{ \frac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z},\ b = p^n$, where $n \in \mathbb{Z},\ n \geq 0 \}$ is principal.

**Definition (In Eg 12.2, Principal ideal)**

An ideal $I \subseteq R$ is called principal if

- $I$ is generated by a single element.

I.e. $I = (a)_R := \{ ra \mid r \in R \}$, for some $a \in R$.

**Recall (In Thm 16.3)**

How to show every ideal $I \subseteq \mathbb{Z}$ is principal?

- Pick the smallest positive $n \in I$
- Use the division algorithm to show $I = (n)_{\mathbb{Z}}$

# 2014 Q8)

8a) List all irreducible polynomials of degree 2 in $\mathbb{Z}/2[x]$.

b) Show that $f(x) = x^4 + x^3 + x^2 + x + \overline{1} \in \mathbb{Z}/2[x]$ is irreducible.

c) Show that $\varphi\colon \mathbb{Z}/2[x] \to \mathbb{Z}/2[x]/(f(x))$ given by

$$\varphi(g(x)) = \overline{g(x) \cdot g(x)}$$

is a ring homomorphism.

d) Show that $\ker\varphi = (f(x))$, and $\varphi$ induces an automorphism

$$\overline{\varphi}\colon \mathbb{Z}/2[x]/(f(x)) \to \mathbb{Z}/2[x]/(f(x))$$

which is different from the identity.

**Remark**

The map $\overline{\varphi}$ in 8d) defines the so-called 'Frobenius' automorphism. It is an important object when studying the Galois Theory of finite fields.

# Irreducible polynomials - Q8a),b)

8a) List all irreducible polynomials of degree 2 in $\mathbb{Z}/2[x]$.

b) Show that $f(x) = x^4 + x^3 + x^2 + x + \overline{1} \in \mathbb{Z}/2[x]$ is irreducible.

### Definition (Def 7.1, Irreducible)

Let $R$ be a commutative ring. An element $r \in R$ is called irreducible if

- $r$ is not a unit, and
- if $r = ab$, for $a, b \in R$, then $a$ is a unit, or $b$ is a unit.

I.e. $r$ cannot be written as a non-trivial product.

### Fact (In Eg 7.3)

Let $F$ be a field, and $f(x) \in F[x]$ a polynomial.

- If $\deg f = 2$ or 3, then $f(x)$ is irreducible iff it has no roots in $F$.
- If $\deg f = 4$, then $f(x)$ is irreducible iff it has no roots in $F$, and it is not the product of two quadratic polynomials.

# Ring homomorphisms, Quotient rings - Q8c)

8c) Show that $\varphi\colon \mathbb{Z}/2[x] \to \mathbb{Z}/2[x]/(f(x))$ given by $\varphi(g(x)) = \overline{g(x) \cdot g(x)}$ is a ring homomorphism.

**Definition (Def 10,4, Ring homomorphism)**

If $R$ and $S$ are rings, a function $\varphi\colon R \to S$ is called a homomorphism if for all $a, b \in R$ we have

- $\varphi(1_R) = 1_S$
- $\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$
- $\varphi(a \cdot_R b) = \varphi(a) \cdot_S \varphi(b)$

**Definition (Def 13.1, Quotient ring)**

Let $R$ be a ring, $I \subseteq R$ an ideal. The quotient ring $R/I$ is the set

$$R/I := \{\, r + I : r \in R \,\} ,$$

with operations

- $(a + I) + (b + I) := (a + b) + I$, and
- $(a + I) \cdot (b + I) := (a \cdot b) + I$.

8d) Show that $\ker\varphi = (f(x))$, and $\varphi$ induces an automorphism $\overline{\varphi}\colon \mathbb{Z}/2[x]/(f(x)) \to \mathbb{Z}/2[x]/(f(x))$which is different from the identity.

**Definition (Def 10.4, Kernel, Image)**

Let $\varphi\colon R \to S$ be a ring homomorphism.

- The kernel of $\varphi$ is $\ker\varphi := \{ a \in R \mid f(a) = 0 \} \subseteq R$.
- The image of $\varphi$ is $\operatorname{im}\varphi := \{ f(a) \mid a \in R \} \subseteq S$.

**Theorem (Thm 13.2, First Isomorphism Theorem)**

*Let $\varphi\colon R \to S$ be a ring homomorphism. Define the associated map*

$$\begin{aligned}\overline{\varphi}\colon R/\ker\varphi &\to \operatorname{im}\varphi\\ x + \ker\varphi &\mapsto \varphi(x)\,.\end{aligned}$$

*Then $\overline{\varphi}$ is a well-defined isomorphism. In particular $R/\ker\varphi \cong \operatorname{im}\varphi$.*