
Problem Sheet 2

1. Show that operations in the definition of quotient ring are well-defined.
2. Prove the following lemma from the lectures.

Lemma. *A non-empty subset $S \subseteq R$ of a ring R is a subring of R iff it satisfies:*

- (1) $\forall a, b \in S, a - b \in S$
- (2) $\forall a, b \in S, ab \in S$

3. Prove the ‘correspondence theorem’ from lectures.
4. Show that a field F has only two ideals, namely F and $\{0\}$. Conversely, show that if a commutative ring R with identity has exactly two ideals, then R must be a field.
5. The *characteristic* of a ring R with 1 is the smallest number n such that

$$0 =_R 1 + 1 + \cdots + 1 \text{ (} n \text{ times)}$$

if such an n exists; otherwise the characteristic is defined to be 0. Explain why the map from $\mathbb{Z} \rightarrow R$ sending $1_{\mathbb{Z}}$ to 1_R and m to $(1_R + 1_R + \cdots + 1_R)$ (m times) is a homomorphism with kernel $(n) \subseteq \mathbb{Z}$, and that R therefore contains an isomorphic copy of $\mathbb{Z}/(n)$. Show that the characteristic of an integral domain is either zero or a prime.

6. A *prime field* is by definition a field with no proper subfields. Show that a prime field is isomorphic to either \mathbb{Q} or \mathbb{Z}_p for some prime p .
7. Let $f, g \in \mathbb{Z}_5[x]$ be given by $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ and $g(x) = x^2 - 2x + 3$. Use ‘long division’ to find $q, r \in \mathbb{Z}_5[x]$ such that $\deg(r) < \deg(g)$ and $f(x) = q(x)g(x) + r(x)$.
8. Prove the following corollary to the division algorithm for $F[x]$:

Corollary. *Let F be a field, $f \in F[x]$ and $a \in F$. Then*

$$a \text{ is a root of } f \iff (x - a) \text{ divides } f \text{ in } F[x].$$

9. Using the previous question, show that $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$. Show that $x^2 - 2$ is *not* irreducible in $\mathbb{R}[x]$.
10. (**Field of Quotients**) In this exercise you will prove that every integral domain can be embedded in a field. The construction mimics the way in which \mathbb{Q} is built from \mathbb{Z} . Let D be an integral domain and define

$$F = \{(a, b) \mid a, b \in D, b \neq 0\} / \sim \quad \text{where } (a, b) \sim (c, d) \text{ if } ad = bc.$$

Define operations on F by:

$$\begin{aligned} (a, b) + (c, d) &= (ad + bc, bd) \\ (a, b)(c, d) &= (ac, bd) \end{aligned}$$

Show that:

- (a) These operations on F are well-defined;
- (b) F , with these operations, is a ring;
- (c) F is a field;
- (d) $\varphi : D \rightarrow F, \varphi(a) = (a, 1)$ is an injective homomorphism (and therefore its image is isomorphic to D).

11. Show that the element $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but not prime.