NAME: GRADE:

Quiz 2

Rings, ideals and Arithmetic

Solution

1. Let $A, B \in \mathbb{R}[X]$ be polynomials. Consider the rational function $f(X) = \dfrac{A(X)}{B(X)}$.

Prove that there exist polynomials $\alpha, \beta \in \mathbb{R}[X]$ such that:

$$f(X) = \alpha(X) + \frac{\beta(X)}{B(X)} \qquad \textbf{and} \qquad d^\circ(\beta) < d^\circ(B).$$

By the Euclidean Division Theorem in $\mathbb{R}[X]$, there exist $\alpha, \beta \in \mathbb{R}[X]$ such that

$$A = B\alpha + \beta$$

with $d^\circ(\beta) < d^\circ(B)$. It follows that

$$f(X) = \frac{B(X)\alpha(X) + \beta(X)}{B(X)} = \frac{B(X)\alpha(X)}{B(X)} + \frac{\beta(X)}{B(X)} = \alpha(X) + \frac{\beta(X)}{B(X)}.$$

2. Let A be a commutative ring with identity 1_A and J an ideal in A.

a. Recall without justification what $0_{A/J}$ and $1_{A/J}$ are.

$$0_{A/J} = [0_A] = 0_A + J = J \quad \text{and} \quad 1_{A/J} = [1_A] = 1_A + J = \{1_A + j \ , \ j \in J\}$$

b. Let $x \in A$. Verify that the set $J_x = \{ax + j \ ; \ a \in A \ , \ j \in J\}$ is an ideal in A.

Verification is straightforward.

c. Prove that if J is a maximal ideal, then A/J is a field.

It is well-known that A/J is a commutative ring with identity. Let $X \neq 0$ in A/J. Then X has a representative $x \notin J$. The associated ideal J_x contains J (let $a = 0$) strictly (it contains x) and J is assumed maximal so $J_x = A$.

In particular, 1_A belongs to J_x, so there exists $a \in A$ and $j \in J$ such that $ax + j = 1_A$ and one checks that $[a]$ is an inverse for $[x] = X$ in A/J, which is therefore a field.

3. Let A and B be rings, I an ideal in A and $\varphi \in \mathrm{Hom}(A, B)$ a ring homomorphism.

Find a necessary and sufficient condition on φ for the function

$$\begin{array}{rcl} \tilde{\varphi} : A/I & \longrightarrow & B \\ [a] & \longmapsto & \varphi(a) \end{array}$$

to be well-defined.

If X is a class in A/I, the element $\tilde{\varphi}(X)$ should not depend on the representative of X in A. In other words, $\tilde{\varphi}$ will be well-defined if and only if

$$[a] = [b] \quad \Rightarrow \quad \tilde{\varphi}([a]) = \tilde{\varphi}([b]),$$

that is, if $[a] = [b]$ implies $\varphi(a) = \varphi(b)$.

Since $[a] = [b]$ is equivalent by definition to $a - b \in I$, the condition becomes

$$a - b \in I \quad \Rightarrow \quad \varphi(a) = \varphi(b).$$

Since φ is a homomorphism, $\varphi(a) = \varphi(b)$ amounts to $a - b \in \ker\varphi$ and a necessary and sufficient condition for $\tilde{\varphi}$ to be well-defined is the inclusion $\boxed{I \subset \ker\varphi}$.

4. Let A be a commutative ring. Recall that a proper ideal I in A is said *prime* if for $a, b \in A$, one has $ab \in I \quad \Rightarrow \quad a \in I$ or $b \in I$.

a. Determine all the prime ideals in $\mathbb{Z}$.

Every ideal in $\mathbb{Z}$ is of the form $\langle n \rangle = n\mathbb{Z} = \{\text{the multiples of } n\}$. Such an ideal is prime if and only if $n|ab$ implies $n|a$ or $n|b$. If n is a prime number, this holds true by Euclid's Lemma.

Conversely, if n is not prime, say $n = n_1 n_2$ with $|n_1| > 1$ and $|n_2| > 1$, then $n|n_1 n_2$ but n divides neither n_1 nor n_2 since they are both strictly smaller in absolute value.

The prime ideals in $\mathbb{Z}$ are therefore the ideals of the form $p\mathbb{Z}$ with p prime number[1].

[1] This is the reason why these ideals are called *prime* in the first place.

b. Assume that in the integral domain A, every ideal is of the form $\langle a \rangle = aA$ for some $a \in A$. Prove that in such a ring, prime ideals are maximal.

Let $I = \langle a \rangle$ be a prime ideal and K an ideal such that $I \subsetneq J \subset A$. Since all ideals in A are principal, there exists some element $x \in A$ such that $J = \langle x \rangle$ and the strict containment condition implies that x is not a multiple of a.

On the other hand, a is in J so it must be a multiple of x, that is $a = km$ for some $k \in A$. Since a is in the prime ideal I, either k or m must be in I. Since $m \notin I$, it implies that $k \in I$, that is, k is a multiple of a.

In other words, $k = a\ell$ with $\ell \in A$, so that $a = a\ell m$ which, by cancellation in the integral domain A, implies that ℓ is an inverse for m. It follows that K contains an invertible element, so that $K = A$.

c. Describe the ideal $\langle 4 \rangle \cap \langle 6 \rangle$ of $\mathbb{Z}$

$\langle 4 \rangle \cap \langle 6 \rangle = \langle 12 \rangle$. The argument is a special case of the one below.

d. Let $m, n \in \mathbb{Z}$. Describe the ideal $\langle m \rangle \cap \langle n \rangle$ of $\mathbb{Z}$.

Since every ideal of $\mathbb{Z}$ is principal, there exsists some number ℓ such that

$$\langle m \rangle \cap \langle n \rangle = \langle \ell \rangle .$$

Since $\ell \in \langle m \rangle$ and $\ell \in \langle n \rangle$, this generator must be a common multiple of m and n. We will prove that ℓ is the smallest such common multiple.

Indeed, if k is a common multiple of m and n, then k belongs to $\langle m \rangle \cap \langle n \rangle = \langle \ell \rangle$ so $\ell | k$. In other words, ℓ is a common multiple of m and n that divides all the common multiples of m and n, so it is a lowest common divisor of m and n and we have proved that $\boxed{\langle m \rangle \cap \langle n \rangle = \langle \mathrm{lcm}(m, n) \rangle}$.