MATH 415

Modern Algebra I

Lecture 21: Follow-up on Exam 2. Homomorphisms of rings.

Follow-up on Exam 2

Problem. Let M be the set of all numbers of the form $m + n\sqrt{3}$, where m and n are integers of the same parity. Under the usual addition and multiplication, is M a ring? Is it a field?

First let us get a better formula for a general element of M. If m and n are integers of the same parity, then $m = n + 2k$ for some $k \in \mathbb{Z}$. Consequently, $m + n\sqrt{3} = 2k + (1 + \sqrt{3})n$. In the latter representation, k and n can be arbitrary integers.

To check whether M is a ring is to check whether it is a subring of $\mathbb{R}$. For the latter, we only need to check if it is closed under addition, subtraction and multiplication.

Let $x_1, x_2 \in M$. We have $x_1 = 2k_1 + (1+\sqrt{3})n_1$ and $x_2 = 2k_2 + (1+\sqrt{3})n_2$ for some $k_1, n_1, k_2, n_2 \in \mathbb{Z}$. Then

$$x_1 + x_2 = 2(k_1 + k_2) + (1+\sqrt{3})(n_1 + n_2),$$

$$x_1 - x_2 = 2(k_1 - k_2) + (1+\sqrt{3})(n_1 - n_2),$$

$$\begin{aligned} x_1 x_2 &= 4k_1k_2 + 2(1+\sqrt{3})(k_1n_2 + n_1k_2) + (1+\sqrt{3})^2 n_1n_2 \\ &= 2(2k_1k_2) + (1+\sqrt{3})(2k_1n_2 + 2n_1k_2) + (4+2\sqrt{3})n_1n_2 \\ &= 2(2k_1k_2 + n_1n_2) + (1+\sqrt{3})(2k_1n_2 + 2n_1k_2 + 2n_1n_2). \end{aligned}$$

We conclude that M is a ring. However M is not a ring with unity since it does not contain 1. In particular, M is not a field.

Remark. In general, if a subring R_0 of a ring R with unity does not contain the unity 1_R of R, it may still have its own unity 1_{R_0}. But this is never the case if R is a domain (and hence satisfies cancellation laws). Indeed, we would have $1_{R_0}1_{R_0} = 1_{R_0} = 1_R 1_{R_0}$ and, after cancellation, $1_{R_0} = 1_R$.

Problem. Let $\mathbb{F}_4$ be a field with 4 elements and $\mathbb{F}_2$ be its subfield with 2 elements. Find a polynomial $p \in \mathbb{F}_2[x]$ that has no zeros in $\mathbb{F}_2$, but has a zero in $\mathbb{F}_4$.

Let $\mathbb{F}_4 = \{0, 1, a, b\}$. Then $\mathbb{F}_2 = \{0, 1\}$. Since $\{1, a, b\}$ is a multiplicative group (of order 3), it follows from Lagrange's Theorem that $x^3 = 1$ for all $x \in \{1, a, b\}$. In other words, 1, a and b are zeros of the polynomial $q(x) = x^3 - 1$.

We have $x^3 - 1 = (x - 1)(x^2 + x + 1)$, which holds over any field. It follows that a and b are also zeros of the polynomial $p(x) = x^2 + x + 1$. Note that $p(0) = p(1) = 1 \neq 0$.

Homomorphism of rings

Definition. Let R and R' be rings. A function $f : R \to R'$ is called a **homomorphism of rings** if $f(r_1 + r_2) = f(r_1) + f(r_2)$ and $f(r_1 r_2) = f(r_1) f(r_2)$ for all $r_1, r_2 \in R$.

That is, f is a homomorphism of the binary structure $(R, +)$ to $(R', +)$ and, simultaneously, a homomorphism of the binary structure $(R, \cdot)$ to $(R', \cdot)$. In particular, f is a homomorphism of additive groups, which implies the following properties:

- $f(0) = 0$,
- $f(-r) = -f(r)$ for all $r \in R$,
- if H is an additive subgroup of R then $f(H)$ is an additive subgroup of R',
- if H' is an additive subgroup of R' then $f^{-1}(H')$ is an additive subgroup of R,
- $f^{-1}(0)$ is an additive subgroup of R, called the **kernel** of f and denoted $\mathrm{Ker}(f)$.

More properties of homomorphisms

Let $f : R \to R'$ be a homomorphism of rings.

- If H is a subring of R, then $f(H)$ is a subring of R'.

We already know that $f(H)$ is an additive subgroup of R'. It remains to show that it is closed under multiplication in R'. Let $r_1', r_2' \in f(H)$. Then $r_1' = f(r_1)$ and $r_2' = f(r_2)$ for some $r_1, r_2 \in H$. Hence $r_1'r_2' = f(r_1)f(r_2) = f(r_1r_2)$, which is in $f(H)$ since H is closed under multiplication in R.

- If H' is a subring of R', then $f^{-1}(H')$ is a subring of R.

We already know that $f^{-1}(H')$ is an additive subgroup of R. It remains to show that it is closed under multiplication in R. Let $r_1, r_2 \in f^{-1}(H')$, that is, $f(r_1), f(r_2) \in H'$. Then $f(r_1r_2) = f(r_1)f(r_2)$ is in H' since H' is closed under multiplication in R'. Hence $r_1r_2 \in f^{-1}(H')$.

More properties of homomorphisms

- If H' is a left ideal in R', then $f^{-1}(H')$ is a left ideal in R.

We already know that $f^{-1}(H')$ is a subring of R. It remains to show that $r \in R$ and $a \in f^{-1}(H')$ imply $ra \in f^{-1}(H')$. We have $f(a) \in H'$. Then $f(ra) = f(r)f(a)$ is in H' since H' is a left ideal in R'. In other words, $ra \in f^{-1}(H')$.

- If H' is a right ideal in R', then $f^{-1}(H')$ is a right ideal in R.

- If H' is a two-sided ideal in R', then $f^{-1}(H')$ is a two-sided ideal in R.

- The kernel $\mathrm{Ker}(f)$ is a two-sided ideal in R.

Indeed, $\mathrm{Ker}(f)$ is the pre-image of the trivial ideal $\{0\}$ in R'.

More properties of homomorphisms

- If an element $a \in R$ is idempotent in R (that is, $a^2 = a$) then $f(a)$ is idempotent in R'.

Indeed, $(f(a))^2 = f(a^2) = f(a)$.

- If 1_R is the unity in R then $f(1_R)$ is the unity in $f(R)$.

Let $r' \in f(R)$. Then $r' = f(r)$ for some $r \in R$. We obtain $r' f(1_R) = f(r) f(1_R) = f(r \cdot 1_R) = f(r) = r'$ and $f(1_R) r' = f(1_R) f(r) = f(1_R \cdot r) = f(r) = r'$.

- If 1_R is the unity in R and R' is a domain with unity, then either $f(1_R)$ is the unity in R' or else the homomorphism f is identically zero.

If $f(1_R) = 0$ then f is identically zero: $f(r) = f(r \cdot 1_R) = f(r) f(1_R) = f(r) \cdot 0 = 0$ for all $r \in R$. Otherwise $f(1_R)$ is a nonzero idempotent element. We know that in a domain with unity, the only idempotent elements are the zero and the unity.

Examples of homomorphisms

- Trivial homomorphism.

Given any rings R and R', let $f(r) = 0_{R'}$ for all $r \in R$, where $0_{R'}$ is the zero element in R'. Then $f : R \to R'$ is a homomorphism of rings.

- Residue modulo n of an integer.

For any $k \in \mathbb{Z}$ let $f(k)$ be the remainder of k after division by n. Then $f : \mathbb{Z} \to \mathbb{Z}_n$ is a homomorphism of rings.

- Homomorphisms of $\mathbb{Z}$.

Let R be any ring and i be any idempotent element in R. Then there exists a unique homomorphism $f : \mathbb{Z} \to R$ such that $f(1) = i$. It can be defined inductively: $f(1) = i$, $f(k+1) = f(k) + i$ for all $k \geq 1$, $f(0) = 0$ and $f(-k) = -f(k)$ for all $k \geq 1$.

Suppose $f : R \to R'$ is a homomorphism of rings. It induces homomorphisms of certain rings built from R and R'.

- Rings of functions.

Given a nonempty set S, let $\mathcal{F}(S, R)$ be the ring of all functions $h : S \to R$. A homomorphism $\phi : \mathcal{F}(S, R) \to \mathcal{F}(S, R')$ is given by $\phi(h) = f \circ h$.

- Rings of polynomials.

A homomorphism $\phi : R[x] \to R'[x]$ is given by
$\phi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) =$
$f(a_0) + f(a_1)x + f(a_2)x^2 + \cdots + f(a_n)x^n$.

- Rings of matrices.

Let $\mathcal{M}_{n,n}(R)$ be the ring of all $n\times n$ matrices with entries from R. A homomorphism $\phi : \mathcal{M}_{n,n}(R) \to \mathcal{M}_{n,n}(R')$ is given by $\phi\big((a_{ij})_{1\le i,j\le n}\big) = (f(a_{ij}))_{1\le i,j\le n}$.