Math 402 Homework 7

a lipson

March 5, 2025

Problem 1. Determine the rules for addition and multiplication of the congruence classes of $\mathbb{Q}[x]/(x^2-2)$.

Proof. Addition follows directly,

$$[ax+b]+[cx+d]=[(a+c)x+(b+d)].$$

By Problem 4, we have that $\mathbb{Q}[x]/(x^2-2)\cong Q[\sqrt{2}]$ with isomorphism $ax+b\mapsto a\sqrt{2}+b$.

For multiplication, consider

$$(a\sqrt{2}+b)(c\sqrt{2}+d)=(ad+bc)\sqrt{2}+(bd+2ac),$$

which, by the above isomorphism, maps back to $(ad+bc)x+(bd+2ac)$.

So,

$$[ax+b][cx+d]=[(ad+bc)x+(bd+2ac)].$$

□

Problem 2. Show that $\mathbb{Q}[x]/(x^2)$ is not a field.

Proof. Since x^2 is reducible in $\mathbb{Q}[x]$, factoring as $x\cdot x$, then x is a zero divisor in $\mathbb{Q}[x]/(x^2)$, and hence $\mathbb{Q}[x]/(x^2)$ is not a field. □

Problem 3. Show that $[f(x)]$ is a unit in $F[x]/(p(x))$ and find its inverse.

a) $[f(x)]=[2x-3]\in\mathbb{Q}[x]/(x^2-2)$.

Note that $2x-3$ is irreducible in $\mathbb{Q}[x]/(x^2-2)$ because it is linear.

Consider $-(2x+3)$. Then,

$$-(2x+3)(2x-3)=-(4x^2-9)=1-4(x^2-2)\equiv 1 \mod (x^2-2).$$

Thus, $-2x-3$ is the inverse of $2x-3$ in $\mathbb{Q}[x]/(x^2-2)$.

b) $[f(x)] = [x^2 + x + 1] \in \mathbb{Z}_3[x]/(x^2 + 1)$.

Note that $[x^2 + x + 1] = [x]$ in $\mathbb{Z}_3[x]/(x^2 + 1)$, so $[x^2 + x + 1]$ is irreducible.

We will consider the system of equations for a, b, c, d given by the linear representation

$$1 = (x^2 + x + 1)(ax + b) + (x^2 + 1)(cx + d),$$

which becomes

$$1 = (x^2 + 1)(x + 1) - x(x^2 + x + 1).$$

So, $[-x]$ is the inverse of $[x^2 + x + 1]$.

Problem 4. Prove $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/(x^2 - 2)$.

Proof. Define $\varphi : Q[x] \to Q[\sqrt{2}]$ by $f(x) \mapsto f(\sqrt{2})$. It follows quickly that φ is homomorphic.

Note that $\ker \varphi = \{f(x) \in \mathbb{Q}[x] \mid f(\sqrt{2}) = 0\}$. So, $x^2 - 2 \in \ker \varphi$.

Since $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ and $x^2 - 2$ is the minimal polynomial in $\mathbb{Q}[x]$ with root $\sqrt{2}$, then, by the same reasoning as in lecture, we have that

$$(x^2 - 2) = \ker \varphi.$$

Since for any $a\sqrt{2} + b \in \mathbb{Q}[\sqrt{2}]$, there is $ax + b \in \mathbb{Q}[x]$ such that $\varphi(ax + b) = a\sqrt{2} + b$, then φ is surjective.

Thus, by the First Isomorphism Theorem, since φ is epimorphic, then

$$\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/(x^2 - 2).$$

□

Problem 5. If $f(x) \in F[x]$ has degree n, prove that there exists an extension field E of F such that $f(x) = c_0(x - c_1)(x - c_2) \cdots (x - c_n)$ for some (not necessarily distinct) $c_i \in E$. In other words, E contains all the roots of $f(x)$.

Proof. We will construct the extension field E inductively.

For the base cases, consider $n = 0$ and $n = 1$. For $n = 0$, $f(x)$ is a constant polynomial of the form c_0. For $n = 1$, $f(x)$ is a linear polynomial which can be expressed as $c_0(x - c_1)$.

Assume the result holds for all polynomials less than degree n.

If $f(x)$ already has a root r in F, then we can write

$$f(x) = (x - r)g(x)$$

where $g(x)$ has degree $n - 1$. By the inductive hypothesis, there is an extension field E' of F where $g(x)$ factors completely. So $E = E'$ works for $f(x)$ as well.

If $f(x)$ has no roots in F, then we must construct a different extension field.

Consider the extension field $F[x]/(f(x))$ where $f(x)$ is a non-constant irreducible polynomial with root α.

We can write $f(x) = (x - \alpha)q(x)$ where $f(x)$ has degree $n - 1$. By the inductive hypothesis, there is an extension field where $q(x)$ factors completely as $d_0(x - d_1) \cdots (x - d_{n-1})$. Thus, $f(x) = (x - \alpha)d_0(x - d_1) \cdots (x - d_{n-1})$, so this extension field allows f to factors completely and we're done. $\square$

Problem 6. List the distinct principal ideas in each ring.

i) $\mathbb{Z}_5$.

   $(0) = \{0\}$. Since 5 is prime, then all elements are units. Hence $(1) = (2) = (3) = (4) = \mathbb{Z}_5$

ii) $\mathbb{Z}_{12}$. $(0) = \{0\}$. Note that all elements coprime with 12 are units in $\mathbb{Z}_{12}$. Hence $(1) = (5) = (7) = (11) = \mathbb{Z}_{12}$.

   We are left with the distinct ideals

$$(1) = \mathbb{Z}_{12},\ (2) = \{0, 2, 4, 6, 8, 10\},\ (3) = \{0, 3, 6, 9\},\ (4) = \{0, 4, 8\},\ (6) = \{0, 6\}.$$

   The other ideals match one of the above.

Problem 7. If I and J are ideals in R , prove that $I \cap J$ is an ideal.

Proof. Both I and J are nonempty, so there intersection is as well.

Both I and J are closed under the addition operation of R, so $a \in I$ and $b \in J$ gives that $a + b$ must belong to both I and J, and hence their intersection as well.

Similarly, for multiplication. $\square$

Problem 8.

Proof. $\square$

Problem 9.

Proof. $\square$

Problem 10. Consider the ring of integers Z.

a) Show that for each nonnegative integer n, (n) is an ideal of $\mathbb{Z}$, and that all these ideals are distinct.

b) Prove that these are all the ideals of $\mathbb{Z}$.

Proof of a. First, (n) is non empty for all nonnegative integers n.

Second (n) is closed under subtraction. For $a, b \in (n)$, $k_1, k_2 \in \mathbb{Z}$,

$$a + b = nk_1 - nk_2 = n(k_1 - k_2) \in (n).$$

Third, (n) is closed under multiplication with $\mathbb{Z}$. For $a = nk \in (n)$ and $r, k \in \mathbb{Z}$, then

$$ra = n(rk) \in (n).$$

So (n) is an ideal in $\mathbb{Z}$ for any nonnegative integer. $\square$

Proof of b. Let I be a nonzero ideal of $\mathbb{Z}$. Since I is nonzero, it contains at least one nonzero element.

Since I contains nonzero elements, it must contain some positive integers (if $x \in I$ is negative, then $-x \in I$ is positive because ideals are closed under multiplication by -1).

Let c be the smallest positive integer in I.

First, $(c) \subset I$. Since $c \in I$, and I is an ideal, then $c \cdot k \in I \forall k \in \mathbb{Z}$. Since all multiples of c are in I, then $(c) \subset I$.

Next, $I \subset (c)$. For any $a \in I$, we have, by the division algorithm, $a = cq + r$ where $0 \leq r \leq c$.

So, $r = a - cq$. Since $a, c \in I$, which is an ideal, then $r = a - cq \in I$.

But c is the smallest positive integer in I, so if $r > 0$, then this contradicts the minimality of c.

Therefore $r = 0$ and $a = cq \in (c)$, which implies that $I \subset (c)$.

Thus $I = (c)$, so every nonzero ideal of $\mathbb{Z}$ is of the form (c) for some positive integer c.

(0) is also included as $(0) = 0$.

Thus, all ideals of $\mathbb{Z}$ are of the form (n) for some nonnegative integer n . $\square$