Math 402 Homework 8

a lipson

March 12, 2025

Problem 1. Let F be a field, and R a nonzero ring. Let $f : F \to R$ be an epimorphism. Prove that f is an isomorphism.

Proof. Since f is an epimorphism, it is surjective and homomorphic.

Let K be the kernel of f. By Theorem 6.10, K is an ideal in F.

We will show that $K = 0$, meaning that f is injective and therefore an isomorphism.

Since F is a field, then the only ideals in f are (0) and F itself.

Suppose that I is a nonzero ideal of F. Then, for $a \in I$, for all $b \in F$, we have that $ab \in I$. Particularly, for $a^{-1} \in F$, we have that $1 = aa^{-1} \in I \implies I = F$; so any nonzero ideal must be equal to F.

If $K = F$, then $f(F) = \{0\} \neq R$, a contradiction with the fact that f is surjective.

Thus we must have $K = 0$, so f is injective.

Since f is injective, surjective, and homomorphic, then f is an isomorphism. □

Problem 2. Define the homomorphism of rings $\varphi : \mathbb{R}[x] \to \mathbb{R}$ by $f(x) \mapsto f(2)$. Find $\ker \varphi$.

Proof. By Theorem 4.16 with the field $\mathbb{R}$, for $f(x) \in \mathbb{R}[x]$ and $a \in \mathbb{R}$, a is a root of f iff $x - a$ is a factor of f.

By definition, we have that $\ker \varphi = \{f(x) \in \mathbb{R}[x] \mid f(2) = 0\}$, which is the set of polynomials in $\mathbb{R}[x]$ with a root at 2; these are the all polynomials of the form

$$\ker \varphi = (x - 2)g(x), \forall g(x) \in \mathbb{R}[x].$$

□

Problem 3. Assume $\mathbb{Z}[\sqrt{2}]$ is a ring. Define $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ by $a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Show the following:

a) f epimorphic.

b) f isomorphic by Theorem 6.11, assuming $\sqrt{2} \notin \mathbb{Q} \implies \sqrt{2} \notin \mathbb{Z}$.

Proof of a. Let $t = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

Then, for all $t \in f \subset \mathbb{Z}[\sqrt{2}]$, there is an $s \in \mathbb{Z}[\sqrt{2}]$ such that $f(s) = t$ where $s = a + (-b)\sqrt{2}$.

Thus, f is surjective.

We have that

$$\begin{aligned} f((a+b\sqrt{2}) + (c+d\sqrt{2})) &= f((a+c) + (b+d)\sqrt{2}) \\ &= (a+c) - (b+d)\sqrt{2} \\ &= (a-b\sqrt{2}) + (c-d)\sqrt{2} \\ &= f(a+b\sqrt{2}) + f(c+d\sqrt{2}), \end{aligned}$$

and

$$\begin{aligned} f((a+b\sqrt{2})(c+d)\sqrt{2}) &= f((ac+2bd) + (ad+bc)\sqrt{2}) \\ &= (ac+2bd) - (ad+bc)\sqrt{2} \\ &= (a-b\sqrt{2})(c-d\sqrt{2}) \\ &= f(a+b\sqrt{2})f(c+d\sqrt{2}), \end{aligned}$$

so f is a homomorphism.

Since f is a subjective homomorphism, then f is a epimorphism. □

Proof of b. We will show that $\ker f = (0_R)$.

By definition, $\ker f = \{a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \mid a - b\sqrt{2} = 0\}$, which only occurs when $a = b = 0$.

So, $\ker f = \{0\} = (0_R)$.

Thus, by Theorem 6.11, f is injective.

Since f is injective and epimorphic, then it must be isomorphic as well. □

Problem 4. Let I, J be ideals in the ring R. Define $f : R \to R/I \times R/J$ by $a \mapsto (a + I, a + J)$.

a) Prove f homomorphic.

b) Is f surjective?

c) Find $\ker f$.

Proof of a. We have that

$$f(a+b) = (a+b+I, a+b+J) = (a+I, a+J) + (b+I, b+J) = f(a) + f(b)$$

and

$$f(ab) = (ab+I, ab+J) = ((a+I)(b+I), (a+J)(b+J)) = (a+I, a+J)(b+I, b+J) = f(a)f(b).$$

Thus, f is homomorphic. □

Proof of b. Consider the example case $\mathbb{Z} \to \mathbb{Z}/(2) \times \mathbb{Z}/(4)$.

The element $(1,0) \in \mathbb{Z}/(2) \times \mathbb{Z}/(4)$ does not exist in the image of f because $a \equiv 1 \mod 2$ implies that a must be odd, but $a \equiv 0 \mod 4$ must be even, a contradiction.

So, f is not necessarily surjective. □

Proof of c. We have that $\ker f = \{a \in R \mid a + I = a + J = 0\}$.

So, for all $a \in R$, $a \equiv 0 \mod I$ and $a \equiv 0 \mod J$.

Thus, we must have that $a = bc$ where $b \in I$ and $c \in J$, which implies that $a \in I \cap J$.

Since a was an arbitrary element of R, then we must have that

$$\ker f = I \cap J.$$

□

Problem 5. Use the First Isomorphism Theorem to show that $\mathbb{Z}_{20}/(5) \cong \mathbb{Z}_5$.

Proof. Let $f : \mathbb{Z}_{20} \to \mathbb{Z}_5$ be a map with kernel (5).

We will show that f is surjective.

Consider $\ker f = (5) = \{x \in \mathbb{Z}_{20} \mid x \equiv 0 \mod 5\}$.

Since $0, 1, 2, 3, 4 \in \mathbb{Z}_{20}$ are mapped to themselves in $\mathbb{Z}_5$ respectively by f, then all elements in the codomain $\mathbb{Z}_5$ are mapped by f, so f is surjective.

Thus, by the First Isomorphism Theorem, since f is surjective, then

$$\mathbb{Z}_{20}/(5) \cong \mathbb{Z}_5.$$

□

Problem 6. Do the following isomorphism hold?

a) $\mathbb{Z}_5 \times \mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_{20}$.

b) $\mathbb{Z}_4 \times \mathbb{Z}_{35} \cong \mathbb{Z}_5 \times \mathbb{Z}_{28}$.

Proof of a. By the Chinese Remainder Theorem,

$$\begin{aligned} (3,4) = 1 &\implies \mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4, \\ (4,5) = 1 &\implies \mathbb{Z}_{20} \cong \mathbb{Z}_4 \times \mathbb{Z}_5. \end{aligned}$$

Thus,

$$\mathbb{Z}_5 \times (\mathbb{Z}_3 \times \mathbb{Z}_4) \cong \mathbb{Z}_3 \times (\mathbb{Z}_4 \times \mathbb{Z}_5).$$

□

Proof of b. Similarly,

$$(5,7)=1 \implies \mathbb{Z}_{35} \cong \mathbb{Z}_5 \times \mathbb{Z}_7,$$
$$(4,7)=1 \implies \mathbb{Z}_{28} \cong \mathbb{Z}_4 \times \mathbb{Z}_7..$$

Thus,

$$\mathbb{Z}_4 \times (\mathbb{Z}_5 \times \mathbb{Z}_7) \cong \mathbb{Z}_5 \times (\mathbb{Z}_4 \times \mathbb{Z}_7).$$

□

Problem 7. a) Prove that for $p \in \mathbb{Z}$, $p \neq 0$, p prime iff the ideal (p) is maximal in $\mathbb{Z}$.

b) Let F be a field and $p(x) \in F[x]$. Prove that $p(x)$ is irreducible iff the ideal $(p(x))$ is maximal in $F[x]$.

Proposition 1. For a principal ideal domain (PID) R, $p \in \mathbb{R}$ is irreducible iff the principal ideal (p) is maximal in R.

Proof of Proposition. ($\implies$) Suppose that p is irreducible in R. Then, $(p) \subsetneq I \subsetneq R$ for some ideal I.

Since R is a PID, then $I = (a)$ where $a \in R$.

Then, $(p) \subsetneq (a) \implies a \mid p$, so $p = ab$ for some $b \in R$.

By Theorem 10.1, p irreducible implies that either a or b is a unit in R.

If a is a unit, then $(a) = R$, contradicting the assumption that $I \neq R$.

If b is a unit, then p and a must be associates, so $(p) = (a)$, contradicting the assumption that $(p) \neq I$.

Therefore, there is not an ideal I between (p) and R.

Thus, (p) is maximal.

($\impliedby$) Suppose that (p) is maximal and p is reducible in R.

Then, $p = ab$ for some $a, b \in R$ which are not units.

Consider the principal ideal (a), $a \mid p \implies (p) \subseteq (a)$, but a is not a unit, so $(a) \neq R$.

Since b is not a unit, then $p \notin (a)$, otherwise $a \mid p \implies a|ab$, where b would be a unit.

Therefore, $(p) \subsetneq (a) \subsetneq R$, contradicting the maximality of (p).

Thus, p must be irreducible. □

Proof of a. $\mathbb{Z}$ is a PID, and the irreducibles in $\mathbb{Z}$ are primes. So, by the Proposition, $p \in \mathbb{Z}$ is a prime iff (p) is maximal in $\mathbb{Z}$. □

Proof of b. $F[x]$ is a PID; By the Proposition, the polynomial $p(x) \in F[x]$ is irreducible iff $(p(x))$ is maximal in $F[x]$. □

Problem 8. Prove that the principal ideal $(x-1)$ in $\mathbb{Z}[x]$ is prime but not maximal

Proof of primeness. We will to show that $\mathbb{Z}[x]/(x-1)$ is an integral domain and hence the ideal $(x-1)$ is prime.

Consider $f(x)g(x) = 0$ in $\mathbb{Z}[x]/(x-1)$. Then we must have that $x-1 \mid f(x)g(x)$.

Since $x-1$ is a linear and therefore irreducible polynomial in $\mathbb{Z}[x]$, then we must have that either $f(x) = 0$ or $g(x) = 0$ in $\mathbb{Z}[x]/(x-1)$.

Thus, there are no zero divisors, hence $\mathbb{Z}[x]/(x-1)$ is an integral domain. □

Proof of non maximality. We will show that there exists an ideal I in $\mathbb{Z}[x]$ such that $(x-1) \subsetneq I \subsetneq \mathbb{Z}[x]$.

Consider $I = (x-1, 2)$. Clearly $(x-1) \subset (x-1, 2)$.

But, $2 \in (x-1, 2)$ yet $2 \notin (x-1)$, so $(x-1) \subsetneq (x-1, 2)$.

Then, for all $h(x) \in (x-1, 2)$, $h(x) = (x-1)f(x) + 2g(x)$ for some $f, g \in \mathbb{Z}[x]$.

Then, at $x = 1$, h must be even. Therefore, the constant function $1 \notin (x-1, 2)$, but $1 \in \mathbb{Z}[x]$.

So, $(x-1, 2) \subsetneq \mathbb{Z}[x]$.

Thus, $(x-1)$ is not maximal. □

Problem 9. a) Prove that the Gaussian Integers $\mathbb{Z}[i]$ are a subring of $\mathbb{C}$, and prove that $M = \{a + bi \mid 3 \mid a \wedge 3 \mid b\}$ is a maximal ideal in $\mathbb{Z}[i]$.

b) Show that $\mathbb{Z}[i]/M$ is a field with nine elements.

Proof af a. Clearly, $\mathbb{Z}[i] \subset \mathbb{C}$. Then, there is a zero element, $0 \in \mathbb{Z}[i]$.

We have that $\mathbb{Z}[i]$ is closed under addition by the closure of $\mathbb{Z}$.

We also have that

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i,$$

so $\mathbb{Z}[i]$ is closed under multiplication by the closure of $\mathbb{Z}$ under addition and multiplication.

Therefore $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

Now, consider $z = a + bi \in \mathbb{Z}[i]$ where $z \notin M$.

$z \notin M$ gives that either 3 does not divide a or does not divide b.

We will show that 3 does not divide $N(z) = a^2 + b^2$.

Suppose that $3 \mid a^2 + b^2 = (a + bi)(a - bi)$. However, there is no such $a, b \in \mathbb{Z}$ with one not divisible by 3 which satisfy the above.

So we must have that 3 does not divide the factor $a + bi$ either, which means that $3 \notin M$.

Since $3 \in \mathbb{Z}[i]$, then $M \subsetneq \mathbb{Z}[i]$.

But, $1 \in a + bi$ as 3 does not divide $1 = a$.

So any ideal containing such $a + bi$ and M must be $\mathbb{Z}[i]$.

Hence M is maximal. $\square$

Proof of b. Since M is maximal, then $\mathbb{Z}[i]/M$ is a field.

Consider the cosets $(a + bi) + M \in \mathbb{Z}[i]/M$. There are three choice for each a and b,

$$0,\ 1,\ 2,\ i,\ 2i,\ 1+i,\ 2+i,\ 1+2i, 2+2i,$$

these canonical representations form the congruence classes of the field $\mathbb{Z}[i]/M$ $\square$

Problem 10. In $\mathbb{Z}[i]$, show that J is not maximal where $J = \{a + bi \ \mid\ 5 \mid a \wedge 5 \mid b\}$.

Proof. Consider $(2 + i)$. We have that $1 \notin (2 + i)$ so $(2 + i) \neq \mathbb{Z}[i]$.

Note that $(2 + i)^2 = 5 \in J$, but $2 + i \notin J$.

Therefore $J \subsetneq (2 + i) \subsetneq \mathbb{Z}[i]$ and J is not maximal. $\square$

Problem 11. Use norms to show in $\mathbb{Z}[i]$

a) $2 + 5i$ is not a factor of $1 + 6i$.

b) $1 + 2i$ is not a factor of $7 + 3i$.

Proof of a. Suppose there exists $a + bi \in \mathbb{Z}[i]$ such that $(2 + 5i)(a + bi) = 1 + 6i$. Then,

$$N((2 + 5i)(a + bi)) = N(1 + 6i)$$
$$N(2 + 5i)N(a + bi) = N(1 + 6i)$$

$$29(a^2 + b^2) = 37.$$

But, $(29, 37) = 1$, so there is no such $a^2 + b^2 \in \mathbb{Z}$ such that the above holds.

Thus, $2 + 5i$ is not a factor of $1 + 6i$. $\square$

Proof of b. Similarly, $N(1 + 2i) = 5$, and $N(7 + 3i) = 58$. But, $(5, 58) = 1$, therefore $1 + 2i$ is not a factor of $7 + 3i$. $\square$