Math 111B HW7

Zih-Yu Hsieh

March 6, 2025

1

Question 1 *Let R be an integral domain in which every nonzero element is either irreducible or a unit. Prove or disprove that R is a field.*

Pf:

We'll prove by contradiction.

Suppose it is not a field, then there exists nonzero element $a \in R$ that is not invertible. Since it's not a unit, a must be irreducible.

Yet, since $a^2 = a \cdot a$, then a^2 is not irreducible; and since $a \neq 0$, then because R is an integral domain, $a^2 \neq 0$. Hence, a^2 must be a unit.

Now, consider a^3: Using the same argument above, since $a^3 = a \cdot a \cdot a$, a^3 is not irreducible and is not 0, therefore it is also a unit.

So, $a^3 = a^2 \cdot a$, showing that $a = (a^2)^{-1}a^3$. It is a multiple of two units, therefore a is also a unit, which reaches a contradiction.

Hence, the assumption is false, R must be a field.

2

Question 2 *Let $d \neq 1$ be an integer which is not divisible by the square of a prime number. Let $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. For any $a + b\sqrt{d}$, we let $N(a + b\sqrt{d}) = |a^2 - db^2|$. Show the following:*

(1) $\mathbb{Z}[\sqrt{d}]$ is a subring of $\mathbb{C}$.

(2) $N(xy) = N(x)N(y)$ for $x, y \in \mathbb{Z}[\sqrt{d}]$.

(3) $x \in \mathbb{Z}[\sqrt{d}]$ is zero iff $N(x) = 0$.

(4) $N(x) = 1$ iff $x \in (\mathbb{Z}[\sqrt{d}])^\times$.

(5) If $N(x)$ is a prime, then x is irreducible in $\mathbb{Z}[\sqrt{d}]$.

Pf:

(1) – First, it's closed under both addition and multiplication: for any $(a+b\sqrt{d}), (e+f\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$, we have:

$$(a+b\sqrt{d}) + (e+f\sqrt{d}) = (a+e) + (b+f)\sqrt{d}$$
$$(a+b\sqrt{d})(e+f\sqrt{d}) = (ae+bfd) + (af+be)\sqrt{d}$$

Since $a, b, d, e, f \in \mathbb{Z}$, the above two expressions are having coefficients being integers. Hence, both the addition and multiplication ends up in $\mathbb{Z}[\sqrt{d}]$, showing the set is closed under both operation.

– Then, both zero and unity element exists: Since $0 = 0 + 0\sqrt{d}$ and $1 = 1 + 0\sqrt{d}$, so $0, 1 \in \mathbb{Z}[\sqrt{d}]$; also, since all $x \in \mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$, then $0 + x = x$, and $1 \cdot x = x$, showing that 0 is the zero element, while 1 is the unity element.

– Also, for all $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, since $a, b \in \mathbb{Z}$ satisfies $(-a), (-b) \in \mathbb{Z}$, so $-a - b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, while $(a+b\sqrt{d}) + (-a-b\sqrt{d}) = (a-a) + (b-b)\sqrt{d} = 0$, hence every element has its additive inverse in the set also.

Now, since associativity of the operations, commutativity of addition, and the distributive property are all inherited from $\mathbb{C}$, then we can say $(\mathbb{Z}[\sqrt{d}], +)$ is an abelian group (due to the closed operation, existence of zero element and additive inverse), while $(\mathbb{Z}[\sqrt{d}], \cdot)$ is a monoid (due to the closed operation, and the existence of unity element).

Hence, the above properties guarantees $\mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$ to be a subring.

(2) For all $x, y \in \mathbb{Z}[\sqrt{d}]$, $x = a + b\sqrt{d}$, and $y = e + f\sqrt{d}$ for some $a, b, e, f \in \mathbb{Z}$.

Hence, the following formulas are true:

$$N(x) = |a^2 - db^2|, \quad N(y) = |e^2 - df^2|$$

$$N(x)N(y) = |a^2 - db^2| \cdot |e^2 - df^2| = |(ae)^2 - d(af)^2 - d(be)^2 + (bfd)^2|$$
$$= |((ae)^2 + 2abefd + (bfd)^2) + (-d(af)^2 - d(be)^2 - 2abefd)|$$
$$= |(ae+bfd)^2 - d((af)^2 + 2abef + (be)^2)| = |(ae+bfd)^2 - d(af+be)^2|$$

$$xy = (a+b\sqrt{d})(e+f\sqrt{d}) = (ae+bfd) + (af+be)\sqrt{d}$$
$$N(xy) = |(ae+bfd)^2 - d(af+be)^2|$$

Then, since $N(x)N(y) = |(ae+bfd)^2 - d(af+be)^2| = N(xy)$, the equation $N(x)N(y) = N(xy)$ is satisfied for all $x, y \in \mathbb{Z}[\sqrt{d}]$.

(3)$\Longrightarrow$: Suppose $x = 0 \in \mathbb{Z}[\sqrt{d}]$, then since $0 = 0 + 0\sqrt{d}$, then $N(0) = |0^2 - d \cdot 0^2| = 0$.

$\Longleftarrow$: Suppose $x = (a + b\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$ satisfies $N(x) = |a^2 - db^2| = 0$, then $a^2 = db^2$.

Notice that since $d \neq 1$ is not divisible by any square of prime numbers, which $d \neq 0$ (because 0 is divisible by all square of primes); so, if we do the unique prime factorization of d, $d = p_1^{q_1} ... p_n^{q_n}$, we must have $q_1 = ... = q_n = 1$ (if one $q_i > 1$, then p_i^2 actually divides d, which is a contradiction). So, $d = p_1 ... p_n$, where each p_i is a distinct prime.

Now, suppose the contrary that $a \neq 0$ (which implies $x \neq 0$), then since $p_1 \mid d$, then $p_1 \mid a^2$. Which, this implies that $p_1 \mid a$ (if not, by Euclid's Lemma, $(p_1, a) = 1$, which implies that $(p_1, a^2) = 1$, so p_1 no longer divides a^2, which is a contradiction).

Then, under the prime factorization of a^2, p_1 must have an even power (since a^2 is a perfect square), which implies that in the prime factorization of $db^2 = a^2$, p_1 must also have even power $2k$ for some $k \in \mathbb{N}$. Yet, since p_1 has power 1 in the prime factorization of d, then it can only have power of $(2k-1)$ in the prime factorization of b^2, which it appears ood times.

Notice that since b^2 is a perfect square, all prime factors must have even power in prime factorization of b^2; however, now p_1 has an odd power in the prime factorization of b^2, which creates a contradiction.

Therefore, our assumption must be false, $a = 0$. Which further implies that $db^2 = a^2 = 0$. Then, since $d \neq 0$, then since $\mathbb{Z}$ is an integral domain, $b^2 = 0$, and this implies $b = 0$.

So, $a = b = 0$, hence $x = a + b\sqrt{d} = 0$.

The above proves both direction, hence $x = 0$ iff $N(x) = 0$.

(4)$\Longrightarrow$: Suppose $N(x) = 1$. Since $x = a + b\sqrt{d}$ for some $a, b \in \mathbb{Z}$ that satisfies $N(x) = |a^2 - db^2| = 1$. Now, consider $x' = a - b\sqrt{d}$: Since $xx' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$, since $|a^2 - db^2| = 1$, then $a^2 - db^2 = 1$ or -1.

If $xx' = a^2 - db^2 = 1$, then x is already invertible; else if $xx' = a^2 - db^2 = -1$, then $(xx')^2 = x \cdot (x(x')^2) = 1$, showing that x is again invertible.

Hence, regardless of the case, $x \in (\mathbb{Z}[\sqrt{d}])^\times$.

$\Longleftarrow$: Suppose $x \in (\mathbb{Z}[\sqrt{d}])^\times$, then x^{-1} exists, and $xx^{-1} = 1$. Then, by previous statements, the following is true:

$$1 = |1^2 - d \cdot 0^2| = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$$

Since $N(x)$ is a nonnegative integer with $N(x) \mid 1$, then the only possibility is $N(x) = 1$.

Since above proves both direction, then we can conclude that $N(x) = 1$ iff $x \in (\mathbb{Z}[\sqrt{d}])^\times$.

(5) Suppose $x \in \mathbb{Z}[\sqrt{d}]$ satisfies $N(x) \in \mathbb{Z}$ being a prime number. Then, for all $y, z \in \mathbb{Z}[\sqrt{d}]$, if $yz = x$, then by the statement proven above, $N(yz) = N(y)N(z) = N(x)$ while $N(x)$ is a prime.

Hence, since both $N(y), N(z)$ are nonnegative integers, since $N(y)N(z)$ is prime, at least one of them must be 1.

So, WLOG, assume $N(y) = 1$. Which, by the statement proven in previous section, $y \in (\mathbb{Z}[\sqrt{d}])^\times$, this shows that x is irreducible, since all $y, z \in \mathbb{Z}[\sqrt{d}]$ with $yz = x$ must have at least one of them being a unit.

3

Question 3 *Prove or disprove that 7 is irreducible in* $\mathbb{Z}[\sqrt{5}]$.

Pf:

Suppose $x, y \in \mathbb{Z}[\sqrt{5}]$ satisfies $xy = 7$. Then, based on the norm problem in **Question 2**, the following is true:

$$49 = |7^2 - 5 \cdot 0^2| = N(7) = N(xy) = N(x)N(y)$$

Since $N(x), N(y)$ are nonnegative integers dividing 49, then they must be either $1, 7$, or 49.

First, ince $N(x)N(y) = 49$, then one of them is 1 iff the other one is 49. But, since in **Question 2** we've proven how the norm is 1 iff the element is invertible, then this case provides no information about irreducibility (since one of the element in x, y is already a unit, due to having a norm of 1).

Now, consider the case where both $N(x), N(y) \neq 1$, which $N(x) = N(y) = 7$. Yet, this is not possible: Suppose there exists $x = a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ with $N(x) = |a^2 - 5b^2| = 7$, then either $a^2 - 5b^2 = 7$, or $a^2 - 5b^2 = -7$.

For the first case, $(a^2 - 5b^2 = 7)$, if take modulo 5 on both sides, we get $(a \mod 5)^2 = (7 \mod 5) = 2$. Yet, this equation has no solution (Since $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9 \equiv 4$ $(mod\ 5)$, $4^2 = 16 \equiv 1$ $(mod\ 5)$, no element in $\mathbb{Z}_5$ satisfies $(a \mod 5)^2 = 2$).

Similarly, for the second case $(a^2 - 5b^2 = -7)$, if take modulo 5 on both sides again, we get $(a \mod 5)^2 = (-7 \mod 5) = 3$. However, by the same list above, no element in $\mathbb{Z}_5$ satisfies $(a \mod 5)^2 = 3$, so this equation also has no solution.

Since for both possiblities we eventually reach a contradiction, then there doesn't exist $x \in \mathbb{Z}[\sqrt{5}]$, with $N(x) = 7$.

Since if $xy = 7$, $N(x)N(y) = 49$, which the above proves that $N(x) = N(y) = 7$ is not possible, then WLOG, it must be the case $N(x) = 1$ and $N(y) = 49$. Since $N(x) = 1$, then $x \in \mathbb{Z}[\sqrt{5}]$ is invertible (by the statement in **Question 2**).

4

Question 4 *Find the smallest prime number which is irreducible in* $\mathbb{Z}[\sqrt{-1}]$.

Pf:

First, consider 2: Since $(1+\sqrt{-1})(1-\sqrt{-1}) = 1-(\sqrt{-1})^2 = 1-(-1) = 2$, while $N(1+i) = N(1-i) = |1^2-(-1)1^2| = 2$, this shows that both $(1+\sqrt{-1}), (1-\sqrt{-1})$ are not unit (since they have norm that's not 1, which based on **Problem 2**, they're not units), while $(1+\sqrt{-1})(1-\sqrt{-1}) = 2$, which implies that 2 is in fact reducible.

Now, consider 3: Recall that every prime element of a commutative ring is automatically irreducible, so to show if one element is irreducible, it's sufficient to show that it's a prime element.

If consider $\mathbb{Z}[\sqrt{-1}]/(3)$, it is in the form $\mathbb{Z}_3[i]$, which is in fact a field (proven in **HW 2 Problem 4**), hence it is an integral domain.

Then, since $\mathbb{Z}[\sqrt{-1}]/(3)$ is an integral domain, it implies that (3) is a prime ideal, hence 3 is a prime element, which is irreducible.

So, he smallest prime which is irreducible in $\mathbb{Z}[\sqrt{-1}]$, is 3.

5

Question 5 *Show that there is a surjective ring homomorphism $\phi : \mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[\sqrt{5}]$. Find the kernel of this ring homomorphism.*

Pf:

The Ring Hmomorphism ϕ:

Define the ring homomorphism $\phi : \mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[\sqrt{5}]$ by $\phi(f(X)) = f(\sqrt{5})$ (which is valid to perform, since $\mathbb{Z}$ has an inclusion into $\mathbb{Z}[\sqrt{5}]$, so the map is first sending $f(x) \in \mathbb{Z}[X]$ to $f(x) \in (\mathbb{Z}[\sqrt{5}])[X]$, then take the evaluation $f(\sqrt{5})$).

Since evaluation map of a ring is always a ring homomorphism, so it remains to check surjectivity: For all $a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$, the polynomial $a + bX \in \mathbb{Z}[X]$ satisfies $\phi(a + bX) = a + b\sqrt{5}$, showing that this map ϕ is in fact surjective.

The kernel of the map:

Consider the ideal $I = (X^2 - 5) \subset \mathbb{Z}[X]$:

First, for all $f(X) \in I$, since $f(X) = (X^2 - 5)g(X)$ for some $g(X) \in \mathbb{Z}[X]$, then, the following is true:

$$\phi(f(X)) = ((\sqrt{5})^2 - 5)g(\sqrt{5}) = (5 - 5)g(\sqrt{5}) = 0$$

Hence, $f(X) \in \ker(\phi)$, showing that $(X^2 - 5) \subseteq \ker(\phi)$.

Now, we'll prove that $(X^2 - 5) = \ker(\phi)$, by consider the relationship with $\mathbb{Q}[X]$ and $\mathbb{Q}[\sqrt{5}]$:

(1) First, for $X^2 - 5 \in \mathbb{Q}[X]$, by Rational Root Theorem, the only possible rational roots are $\pm 1, \pm 5$; yet, the following evaluations show that all of them are not a root:

$$1^2 - 5 = (-1)^2 - 5 = -4, \quad 5^2 - 5 = (-5)^2 - 5 = 20$$

Hence, $(X^2 - 5)$ has no roots in $\mathbb{Q}[X]$, and because it is degree 2 while $\mathbb{Q}$ is a field, we can conclude that $X^2 - 5$ is irreducible, hence a prime element in $\mathbb{Q}[X]$ (which, $(X^2 - 5) \subseteq \mathbb{Q}[X]$ is a prime ideal, and because $\mathbb{Q}[X]$ is a PID, the nonzero ideal $(X^2 - 5)$ is in fact maximal).

(2) Now, define the evaluation map $\bar{\phi} : \mathbb{Q}[X] \twoheadrightarrow \mathbb{Q}[\sqrt{5}]$ by $\bar{\phi}(f(X)) = f(\sqrt{5})$, which this map is surjective, since all $a + b\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$ has $\bar{\phi}(a + bX) = a + b\sqrt{5}$.

We know that for $X^2 - 5 \in \mathbb{Q}[X]$, $(X^2 - 5) \subseteq \ker(\bar{\phi})$ (since for any $g(X) \in \mathbb{Q}[X]$, $(X^2 - 5)g(X)$ has an evaluation at $\sqrt{5}$ being 0); on the other hand, by Generalized First Isomorphism Theorem, there exists a well-defined ring homomorphism $\bar{\phi}' : \mathbb{Q}[X]/(X^2 - 5) \twoheadrightarrow \mathbb{Q}[\sqrt{5}]$, such that the composition with canonical map $\pi(f(X)) = f(X) \mod (X^2 - 5)$, we have $\bar{\phi}(f(X)) = \bar{\phi}'(\pi(f(X))) = f(\sqrt{5})$.

Now, notice that since $(X^2 - 5) \subseteq \mathbb{Q}[X]$ is a maximal ideal, then $\mathbb{Q}[X]/(X^2 - 5)$ is actually a field; since $\bar{\phi}' : \mathbb{Q}[X]/(X^2 - 5) \twoheadrightarrow \mathbb{Q}[\sqrt{5}]$ is surjective, then the domain is a field implies that $\ker(\bar{\phi}') = (0)$ (since the only ideal for prime is (0) or itself, $\ker(\bar{\phi}')$ must be one of them; and since the map is surjective, then $\ker(\bar{\phi}') = (0)$ is enforced).

Then, for all $f(X) \in \ker(\bar{\phi})$, since $\bar{\phi}(f(X)) = \bar{\phi}'(\pi(f(X))) = \bar{\phi}'(f(X) \mod (X^2 - 5)) = 0$, while $\bar{\phi}'$ is injective, then $f(X) \mod (X^2 - 5) = 0$, showing that $f(X) \in (X^2 - 5)$. Hence, $\ker(\bar{\phi}) \subseteq (X^2 - 5)$, showing that $\ker(\bar{\phi}) = (X^2 - 5)$.

(3) Finally, consider the following commutative diagram:

6

Question 6 *Prove or disprove that $\mathbb{Z}[\sqrt{5}]$ is a pid.*

Pf:

We'll prove that $\mathbb{Z}[\sqrt{5}]$ is not a PID. Recall that for a PID, all irreducible elements are prime elements also, we'll use this to prove the statement.

2 is irreducible

Now, consider $2 \in \mathbb{Z}[\sqrt{5}]$: Suppose $x, y \in \mathbb{Z}[\sqrt{5}]$ satisfies $xy = 2$, then by the statements in **Question 2**, using the same norm function, we get:

$$4 = |2^2 - 5 \cdot 0^2| = N(2) = N(x)N(y)$$

So, since $N(x), N(y)$ are nonnegative integers that multiply to be 4, they must be either $1, 2$, or 4.

First, one of the element is 1 iff the other element is 4 (since $1 \cdot 4 = 4$); if any element satisfies the norm being 1 (for instance, if $N(x) = 1$), then using the statements in **Question 2**, we know $x \in (\mathbb{Z}[\sqrt{5}])^\times$, hence it is a unit, which shows nothing about irreducibility.

Now, consider the case where both $N(x), N(y) \neq 1$ (hence $N(x), N(y) = 2$). Yet, this is not possible: Suppose $x = a + b\sqrt{5}$ satisfies $N(x) = |a^2 - 5b^2| = 2$, then either $a^2 - 5b^2 = 2$, or $a^2 - 5b^2 = -2$.

For the first possibility ($a^2 - 5b^2 = 2$), if we take modulo 5 on both sides, we get that $(a \mod 5)^2 = (2 \mod 5)$. However, this equation has no solution (since $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9 \equiv 4$ $(mod\ 5)$, and $4^2 = 16 \equiv 1$ $(mod\ 5)$).

Similarly, for the second possibility ($a^2 - 5b^2 = -2$), if we take modulo 5 on both sides again, we get that $(a \mod 5)^2 = (-2 \mod 5) = (3 \mod 5)$, which from the above list of equations, we know it also has no solutions.

Hence, both possibilities are not satisfied, showing that $N(x) \neq 2$, which is a contradiction.

Therefore, we can conclude that if $xy = 2$, then we can't have both $N(x), N(y) \neq 1$ (since this implies $N(x) = N(y) = 2$, which is impossible), so at least one of the element has norm 1, which is equivalent to being a unit.

Since $xy = 2$ implies one of the element is a unit, then 2 is irreducible.

2 is not prime:

However, 2 is not prime: If we consider $\mathbb{Z}[\sqrt{5}]/(2)$, notice that since $1 + \sqrt{5}$ has none of its coefficients divisible by 2, hence $(1 + \sqrt{5}) \notin (2)$, which under the quotient, $(1 + \sqrt{5}) \mod (2)$ is nonzero.

Yet, since $(1 + \sqrt{5})^2 = 1 + 5 + 2\sqrt{5} = 6 + 2\sqrt{5} = 2(3 + \sqrt{5})$, then $(1 + \sqrt{5})^2 \mod (2) = 0$, showing that $(1 + \sqrt{5}) \mod (2)$ is actually a nonzero nilpotent element in $\mathbb{Z}[\sqrt{5}]/(2)$, hence this ring is not an integral domain.

Because $\mathbb{Z}[\sqrt{5}]/(2)$ is not an Integral Domain, then (2) is not a prime ideal, showing that 2 is not a prime element.

Since there exists an irreducible element that's not prime, then $\mathbb{Z}[\sqrt{5}]$ cannot be a PID.