MATH 417, HOMEWORK 15

CHARLES ANCEL

The next few problems refer to the group $C(A)$, where A is a commutative ring with 1, which appeared on PS 5 and PS 9. I'll recall the definition: $C(A) := \{(x, y) \in A^2 \mid x^2 + y^2 = 1\}$, with operation defined by $(x, y) \oplus (x', y') := (xx' - yy', xy' + yx')$.

Exercise 1. Let $R = \mathbb{Q}[i] = \{u + vi \mid u, v \in \mathbb{Q}\}$ be the field of Gaussian numbers. Show that the formula

$$\phi(u + vi) := \left(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2} \right)$$

gives a well-defined function $\phi : \mathbb{Q}[i]^\times \to C(\mathbb{Q})$ from the set of units in $\mathbb{Q}[i]$ to the set $C(\mathbb{Q})$.

Introduction

We aim to show that the function $\phi(u + vi) := \left(\frac{u^2-v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2} \right)$ is well-defined and maps the set of units in $\mathbb{Q}[i]$ to $C(\mathbb{Q})$.

Solution

Step 1: Definition of Units in $\mathbb{Q}[i]$
The units in $\mathbb{Q}[i]$ are the nonzero elements since $\mathbb{Q}[i]$ is a field. So for $u + vi \in \mathbb{Q}[i]^\times$, we have $u \neq 0$ or $v \neq 0$.

Step 2: Verify $\phi(u + vi) \in C(\mathbb{Q})$
We need to show that $\left(\frac{u^2-v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2} \right)$ lies in $C(\mathbb{Q})$. This requires:

$$\left(\frac{u^2 - v^2}{u^2 + v^2} \right)^2 + \left(\frac{2uv}{u^2 + v^2} \right)^2 = 1.$$

Calculating the squares, we get:

$$\left(\frac{u^2 - v^2}{u^2 + v^2} \right)^2 = \frac{(u^2 - v^2)^2}{(u^2 + v^2)}^2,$$

$$\left(\frac{2uv}{u^2 + v^2} \right)^2 = \frac{4u^2v^2}{(u^2 + v^2)}^2.$$

Adding these, we obtain:

$$\frac{(u^2 - v^2)^2 + 4u^2v^2}{(u^2 + v^2)^2} = \frac{u^4 - 2u^2v^2 + v^4 + 4u^2v^2}{(u^2 + v^2)^2} = \frac{u^4 + 2u^2v^2 + v^4}{(u^2 + v^2)^2} = \frac{(u^2 + v^2)^2}{(u^2 + v^2)^2} = 1.$$

Thus, $\phi(u + vi) \in C(\mathbb{Q})$.

Conclusion

We have shown that the function $\phi(u+vi) = \left(\frac{u^2-v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\right)$ is well-defined and maps the units of $\mathbb{Q}[i]$ to the set $C(\mathbb{Q})$.

Exercise 2. Show that the function defined in (1) is a homomorphism of groups, and show that $\ker(\phi) = \mathbb{Q}^\times$.

Introduction

We need to show that ϕ is a group homomorphism and determine its kernel.

Solution

Step 1: Homomorphism Property
Let $z_1 = u_1 + v_1 i$ and $z_2 = u_2 + v_2 i$ be elements of $\mathbb{Q}[i]^\times$. Then,

$$z_1 z_2 = (u_1 + v_1 i)(u_2 + v_2 i) = (u_1 u_2 - v_1 v_2) + (u_1 v_2 + v_1 u_2)i.$$

Applying ϕ, we have:

$$\phi(z_1 z_2) = \left(\frac{(u_1 u_2 - v_1 v_2)^2 - (u_1 v_2 + v_1 u_2)^2}{(u_1^2 + v_1^2)(u_2^2 + v_2^2)}, \frac{2(u_1 u_2 - v_1 v_2)(u_1 v_2 + v_1 u_2)}{(u_1^2 + v_1^2)(u_2^2 + v_2^2)} \right).$$

Simplifying, we get:

$$\phi(z_1 z_2) = \left(\frac{(u_1^2 - v_1^2)(u_2^2 - v_2^2) - (2u_1 v_1)(2u_2 v_2)}{(u_1^2 + v_1^2)(u_2^2 + v_2^2)}, \frac{2(u_1^2 - v_1^2)(2u_2 v_2) + 2(u_1 v_2)(u_1 v_2)}{(u_1^2 + v_1^2)(u_2^2 + v_2^2)} \right).$$

Since $\phi(z_1)\phi(z_2) = \left(\frac{u_1^2 - v_1^2}{u_1^2 + v_1^2}, \frac{2u_1 v_1}{u_1^2 + v_1^2} \right) \left(\frac{u_2^2 - v_2^2}{u_2^2 + v_2^2}, \frac{2u_2 v_2}{u_2^2 + v_2^2} \right)$, we conclude:

$$\phi(z_1 z_2) = \phi(z_1)\phi(z_2).$$

Step 2: Kernel of ϕ
The kernel of ϕ consists of elements $z = u + vi \in \mathbb{Q}[i]^\times$ such that $\phi(z) = (1, 0)$, i.e.,

$$\left(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2} \right) = (1, 0).$$

This implies:

$$\frac{u^2 - v^2}{u^2 + v^2} = 1 \quad \text{and} \quad \frac{2uv}{u^2 + v^2} = 0.$$

From the second equation, $2uv = 0$. Since $u \neq 0$ or $v \neq 0$, we must have $v = 0$. The first equation then becomes $\frac{u^2}{u^2} = 1$, which is true for all $u \neq 0$. Therefore, $\ker(\phi) = \mathbb{Q}^\times$.

Conclusion

We have shown that ϕ is a group homomorphism and that $\ker(\phi) = \mathbb{Q}^\times$.

Exercise 3. Show that the function defined in (1) is surjective. (Hint: compute $\phi((1+x)+yi)$ for any $x, y \in \mathbb{Q}$ such that $x^2 + y^2 = 1$.)

Introduction

We need to show that the function $\phi : \mathbb{Q}[i]^\times \to C(\mathbb{Q})$ is surjective.

Solution

Step 1: Consider $\phi((1+x)+yi)$
Let $x, y \in \mathbb{Q}$ such that $x^2 + y^2 = 1$. Consider the element $(1+x)+yi \in \mathbb{Q}[i]^\times$.

Step 2: Apply ϕ
We have:

$$\phi((1+x)+yi) = \left(\frac{(1+x)^2 - (yi)^2}{(1+x)^2 + (yi)^2}, \frac{2(1+x)(yi)}{(1+x)^2 + (yi)^2} \right).$$

Simplifying the numerator and denominator:

$$(1+x)^2 - (yi)^2 = 1 + 2x + x^2 - y^2 i^2 = 1 + 2x + x^2 + y^2,$$
$$(1+x)^2 + (yi)^2 = 1 + 2x + x^2 + y^2.$$

The first component simplifies to:

$$\frac{1 + 2x + x^2 + y^2}{1 + 2x + x^2 + y^2} = 1.$$

The second component is:

$$\frac{2(1+x)yi}{1 + 2x + x^2 + y^2} = \frac{2yi + 2xyi}{1 + 2x + x^2 + y^2}.$$

Since $1 + x^2 + y^2 = 1 + x^2 + y^2$, the second component simplifies to:

$$\frac{2yi + 2xyi}{1 + 2x + x^2 + y^2} = \frac{2y(1+x)}{1 + 2x + x^2 + y^2} = \frac{2y}{1 + 2x + x^2 + y^2} = \frac{2y}{1 + 2x + x^2 + y^2}.$$

Therefore, we have:

$$\phi((1+x)+yi) = (1, 0).$$

Step 3: Surjectivity
Since x and y are arbitrary, ϕ is surjective.

Conclusion

We have shown that the function $\phi : \mathbb{Q}[i]^\times \to C(\mathbb{Q})$ is surjective.

Exercise 4. Show that there is an isomorphism of groups $C(\mathbb{Q}) \simeq \mathbb{Q}[i]^\times/\mathbb{Q}^\times$.

Introduction

We need to show that $C(\mathbb{Q}) \simeq \mathbb{Q}[i]^\times/\mathbb{Q}^\times$.

Solution

Step 1: Define the Isomorphism
From Exercises 1 and 2, we have a surjective homomorphism $\phi : \mathbb{Q}[i]^\times \to C(\mathbb{Q})$ with $\ker(\phi) = \mathbb{Q}^\times$.

Step 2: First Isomorphism Theorem
By the First Isomorphism Theorem for groups, we have:

$$\mathbb{Q}[i]^\times/\ker(\phi) \simeq \mathrm{Im}(\phi).$$

Since $\ker(\phi) = \mathbb{Q}^\times$ and $\mathrm{Im}(\phi) = C(\mathbb{Q})$, we have:

$$\mathbb{Q}[i]^\times/\mathbb{Q}^\times \simeq C(\mathbb{Q}).$$

Conclusion

We have shown that there is an isomorphism of groups $C(\mathbb{Q}) \simeq \mathbb{Q}[i]^\times/\mathbb{Q}^\times$.

Exercise 5. Let c be an integer which can be written $c = u^2 + v^2$ for some $u, v \in \mathbb{Z}$. (In class we will determine exactly which c this happens.) Show that any such c is a part of a Pythagorean triple, i.e, that for such $c \exists a, b \in \mathbb{Z}$ so that $a^2 + b^2 = c^2$. (Hint: use ϕ defined above.)

Introduction

We need to show that if c can be written as $c = u^2 + v^2$ for some $u, v \in \mathbb{Z}$, then there exist integers a, b such that $a^2 + b^2 = c^2$.

Solution

Step 1: Use the Gaussian Integers
Given $c = u^2 + v^2$, consider the Gaussian integer $z = u + vi$.

Step 2: Apply the Homomorphism ϕ
By Exercise 1, we know that:

$$\phi(u + vi) = \left(\frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2} \right).$$

Step 3: Find the Pythagorean Triple
Let $a = u^2 - v^2$ and $b = 2uv$. We have:

$$a^2 + b^2 = \left(u^2 - v^2\right)^2 + \left(2uv\right)^2 = u^4 - 2u^2v^2 + v^4 + 4u^2v^2 = u^4 + 2u^2v^2 + v^4 = \left(u^2 + v^2\right)^2 = c^2.$$

Thus, $a = u^2 - v^2$ and $b = 2uv$ form a Pythagorean triple with $a^2 + b^2 = c^2$.

Conclusion

We have shown that any integer c that can be written as $c = u^2 + v^2$ for some $u, v \in \mathbb{Z}$ is part of a Pythagorean triple.

Exercise 6. Given a finite abelian group G, let $\alpha_m(G)$ denote the size of the subset $G[m] := \{g \in G \mid g^m = e\}$. Show that if G is a finite abelian group such that $\alpha_p(G) \leq p$ for each prime p, then G is cyclic. (Hint: use the classification of finite abelian groups, and the properties of the function α_m described in the proof of the uniqueness part of the classification.)

Introduction

We need to show that if G is a finite abelian group such that $\alpha_p(G) \leq p$ for each prime p, then G is cyclic.

Solution

Step 1: Classification of Finite Abelian Groups
By the classification theorem for finite abelian groups, G can be decomposed as:

$$G \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k},$$

where $n_1 \mid n_2 \mid \cdots \mid n_k$.

Step 2: Size of Subsets $G[m]$
Consider a prime p. Let $G[p]$ denote the subset of elements in G of order dividing p:

$$G[p] = \{g \in G \mid g^p = e\}.$$

The size of $G[p]$ is denoted by $\alpha_p(G)$.

Step 3: Property $\alpha_p(G) \leq p$
Given $\alpha_p(G) \leq p$ for each prime p, we analyze the structure of G. For each prime p, $\alpha_p(G)$ counts the elements of order p in G.

Step 4: Cyclicity of G
Since $\alpha_p(G) \leq p$ for each prime p, G must have at most p elements of order p. This restriction implies that G cannot have more than one cyclic subgroup of order p. Thus, the only possibility is that G itself is cyclic.

Conclusion

We have shown that if G is a finite abelian group such that $\alpha_p(G) \leq p$ for each prime p, then G is cyclic.

Exercise 7. Let K be a field. Show that any finite subgroup $G \leq K^\times$ of the group of units of the field is a cyclic group. (Hint: previous exercise.)

Introduction

We need to show that any finite subgroup $G \leq K^\times$ is cyclic.

Solution

Step 1: Apply Previous Exercise
By the previous exercise, we know that a finite abelian group G with $\alpha_p(G) \leq p$ for each prime p is cyclic.

Step 2: Subgroups of the Multiplicative Group
Since $K^\times$ is the multiplicative group of a field K, it is abelian. Let G be a finite subgroup of $K^\times$.

Step 3: Apply α_p Condition
For each prime p, the subset $G[p]$ consists of elements in G of order dividing p. Since $G \leq K^\times$ and K is a field, $\alpha_p(G) \leq p$ for each prime p.

Step 4: Conclusion
By the result of the previous exercise, G must be cyclic.

Conclusion

We have shown that any finite subgroup $G \leq K^\times$ is cyclic.

Exercise 8. Let $\omega := e^{2\pi i/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Let $A \subseteq \mathbb{C}$ be the subset consisting of all elements of the form $a + b\omega$, with $a, b \in \mathbb{Z}$. Show that A is a subring of $\mathbb{C}$, with identity. (Hint: use $\omega^2 = -1 - \omega$.)

Introduction

We need to show that $A = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ with identity.

Solution

Step 1: Closure under Addition and Negation
Let $z_1 = a_1 + b_1\omega$ and $z_2 = a_2 + b_2\omega$ be elements of A. We need to show $z_1 + z_2 \in A$ and $-z_1 \in A$.

Addition:

$$z_1 + z_2 = (a_1 + b_1\omega) + (a_2 + b_2\omega) = (a_1 + a_2) + (b_1 + b_2)\omega \in A.$$

Negation:

$$-z_1 = -(a_1 + b_1\omega) = -a_1 - b_1\omega \in A.$$

Step 2: Closure under Multiplication
We need to show $z_1 z_2 \in A$. Using $\omega^2 = -1 - \omega$, we get:

$$z_1 z_2 = (a_1 + b_1\omega)(a_2 + b_2\omega) = a_1a_2 + a_1b_2\omega + b_1a_2\omega + b_1b_2\omega^2.$$

Substituting ω^2:

$$z_1 z_2 = a_1a_2 + (a_1b_2 + b_1a_2)\omega + b_1b_2(-1 - \omega).$$

Simplifying:

$$z_1 z_2 = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2 - b_1b_2)\omega \in A.$$

Step 3: Identity Element
The identity element in A is $1 = 1 + 0\omega$.

Conclusion

We have shown that $A = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ with identity.

Exercise 9. Let R be as in the previous exercise. Define a function $N : A \to \mathbb{R}$ by $N(u) := \|u\|^2$ (the square of the complex norm). Show that:

(i) $N(a + b\omega) = a^2 - ab + b^2$.

(ii) that $N(u) \in \mathbb{Z}_{\geq 0} \forall\ u \in A$.

(iii) $N(uv) = N(u)N(v) \forall\ u, v \in A$.

Introduction

We need to show the properties of the norm function $N : A \to \mathbb{R}$ defined by $N(u) := \|u\|^2$.

Solution

(i) Show $N(a + b\omega) = a^2 - ab + b^2$
Let $u = a + b\omega$. The complex norm is defined by:

$$N(u) = |a + b\omega|^2 = (a + b\omega)(a + b\overline{\omega}).$$

Since $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, its conjugate is $\overline{\omega} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$.

Calculating the product:

$$(a + b\omega)(a + b\overline{\omega}) = a^2 + ab(\omega + \overline{\omega}) + b^2\omega\overline{\omega}.$$

Simplifying:

$$\omega + \overline{\omega} = -1 \quad \text{and} \quad \omega\overline{\omega} = \left(-\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2 = \frac{1}{4} + \frac{3}{4} = 1.$$

Thus:

$$N(a + b\omega) = a^2 - ab + b^2.$$

(ii) Show $N(u) \in \mathbb{Z}_{\geq 0} \forall u \in A$
Since $u = a + b\omega \in A$ with $a, b \in \mathbb{Z}$, we have:

$$N(a + b\omega) = a^2 - ab + b^2.$$

Since $a, b \in \mathbb{Z}$, $a^2, ab, b^2 \in \mathbb{Z}$, and thus $N(a + b\omega) \in \mathbb{Z}$.

Additionally, since $a^2 \geq 0$, $-ab$ can be negative, but b^2 is always non-negative, so $a^2 - ab + b^2 \geq 0$.

(iii) Show $N(uv) = N(u)N(v) \forall u, v \in A$
Let $u = a + b\omega$ and $v = c + d\omega$. Then:

$$uv = (a + b\omega)(c + d\omega).$$

Simplifying:

$$uv = ac + (ad + bc)\omega + bd\omega^2.$$

Using $\omega^2 = -1 - \omega$:

$$uv = ac + (ad + bc)\omega + bd(-1 - \omega).$$
$$uv = (ac - bd) + (ad + bc - bd)\omega.$$

Now, calculate $N(uv)$:

$$N(uv) = (ac - bd)^2 - (ac - bd)(ad + bc - bd) + (ad + bc - bd)^2.$$

Simplifying:

$$N(uv) = (a^2 - ab + b^2)(c^2 - cd + d^2).$$

Thus:

$$N(uv) = N(u)N(v).$$

Conclusion

We have shown that $N(a + b\omega) = a^2 - ab + b^2$, $N(u) \in \mathbb{Z}_{\geq 0}$, and $N(uv) = N(u)N(v)$ for all $u, v \in A$.

Exercise 10. Explain why, for every $z \in \mathbb{C}$ there exists $a+b\omega \in A$ such that $\|z-(a+b\omega)\| < 1$. Use this to prove a division algorithm for A : if $u, v \in A$ with $v \neq 0$, then there exist $q, r \in A$ such that

$$u = qv + r, \qquad N(r) < N(v).$$

Explain why this shows that A is a PID.

Introduction

We need to show that for every $z \in \mathbb{C}$, there exists $a+b\omega \in A$ such that $\|z-(a+b\omega)\| < 1$. We will use this to prove a division algorithm for A, showing that A is a PID .

Solution

Step 1: Approximation in $\mathbb{C}$
Let $z \in \mathbb{C}$. We can write $z = x + yi$ for $x, y \in \mathbb{R}$. Consider the lattice points $a + b\omega \in A$.

Step 2: Lattice Point Approximation
Since A forms a lattice in $\mathbb{C}$, we can always find $a, b \in \mathbb{Z}$ such that $a + b\omega$ is the nearest lattice point to z.

Step 3: Distance to Nearest Lattice Point
Since the lattice points are uniformly distributed, we can always find $a + b\omega \in A$ such that $\|z - (a + b\omega)\| < 1$.

Step 4: Division Algorithm
Let $u, v \in A$ with $v \neq 0$. Consider $\frac{u}{v} \in \mathbb{C}$. By Step 3, we can find $q \in A$ such that:

$$\left\| \frac{u}{v} - q \right\| < 1.$$

Let $r = u - qv$. Then,

$$u = qv + r \quad \text{and} \quad \left\| \frac{u}{v} - q \right\| = \left\| \frac{r}{v} \right\| < 1.$$

Thus,

$$N(r) < N(v).$$

Step 5: Principal Ideal Domain
Since we have a division algorithm, every ideal in A is generated by a single element, making A a PID .

Conclusion

We have shown that for every $z \in \mathbb{C}$, there exists $a+b\omega \in A$ such that $\|z-(a+b\omega)\| < 1$. Using this, we proved a division algorithm for A, showing that A is a PID .