1

Proposition. Let $R$ be a commutative ring with identity and $I \subset R$ consist of $0_R$ and all zero-divisors. Then there exists a prime ideal $M$ of $R$ with $M \subseteq I$.

Proof. Let $I$ be the set of ideals contained in $I$; that is,

$$I = \{ J \subset I \mid J \text{ is an ideal of } R \}.$$ 

Note that $I$ is non-empty because \{0\} \subset I is an ideal. Also note that $I$ is partially-ordered by inclusion.

Let $A_1 \subseteq A_2 \subseteq \ldots \subseteq A_k \subseteq \ldots$ be a chain in $I$. Put

$$A = \bigcup_{i \in \mathbb{N}} A_i.$$ 

Certainly $0_R \in A$. Let $a, b \in A$. Then $a \in A_n$ and $b \in A_m$ for some $n, m \in \mathbb{N}$. Without loss of generality, assume $n \leq m$. This means $A_n \subseteq A_m$. So we have $a, b \in A_m$. Since $A_m$ is a subring, it follows that $-a \in A_m$, $a + b \in A_m$, and $ab \in A_m$. So also $-a \in A$, $a + b \in A$ and $ab \in A$. This means $A$ is closed under additive inverses, addition, and multiplication, so $A$ is a subring of $R$. Let $r \in R$. Since $A_n$ is an ideal, $ra \in A_n$. This implies $ra \in A$ and so $A$ is an ideal by definition.

Every $A_i$ is contained in $I$ by the definition of $I$. Hence, $A$, which is the union of such $A_i$, is also contained in $I$. So $A$ is an ideal contained in $I$ which means $A \in I$. But $A$ is an upper bound of the chain, and the chain was arbitrary, so every chain in $I$ has an upper bound. By Zorn’s Lemma, $I$ must have a maximal element, say $M$. We must show that $M$ is a prime ideal in $R$. By 3.2.16, since $R$ has identity, it will suffice to show that $M$ is maximal in $R$.

Let $B$ be an ideal in $R$ such that $M \not\subset B \subset R$. Since $M$ is maximal in $I$, $B$ must not be contained in $I$ so there exists $0_R \neq b \in B$ such that $b$ is not a zero-divisor.

I did not have enough time to show that $B = R$. If I had, then I would know that $M \subset I$ is maximal in $R$ and thus also prime.
We will show that \( I = (2, x) \subset \mathbb{Z}[x] \) is not a principal ideal.

Suppose to the contrary that \( I = (p) \) for some polynomial \( p \in \mathbb{Z}[x] \). Since the constant polynomial 2 is an element of \( I \), it must also be an element of \( (p) \). Hence, there exists \( q \in \mathbb{Z}[x] \) such that \( 2 = p \cdot q \). Let us define

\[
p = \sum_{i=0}^{n} p_i x^i \quad q = \sum_{j=0}^{m} q_j x^j,
\]

where \( p_n \) and \( q_m \) are non-zero coefficients (if they were zero, we would remove them from the sum). So we may now write

\[
2 = \left( \sum_{i=0}^{n} p_i x^i \right) \left( \sum_{j=0}^{m} q_j x^j \right)
= p_0 q_0 + (p_0 q_1 + p_1 q_0)x + \ldots + (p_n q_m)x^{n+m}.
\]

By the equality of polynomials, it follows that all coefficients of the right-hand side must be 0 except \( p_0 q_0 = 2 \). Since \( \mathbb{Z} \) has no zero-divisors, \( p_0 q_m = 0 \) implies \( p_n = 0 \) or \( q_m = 0 \). When \( n, m > 0 \) this is a contradiction based on our definition of \( p \) and \( q \). Thus, \( p \) and \( q \) must both be constant polynomials that divide 2.

Suppose \( p = \pm 2 \). This means \( I = (\pm 2) \). But this is impossible because \( (\pm 2) \subsetneq (2, x) \). Suppose \( p = \pm 1 \). But then \( p \) is a unit and by 3.3.4, \( (p) = R \neq (2, x) \). Therefore, \( p \) does not exist and \( I = (2, x) \) is not a principal ideal.

3

Let \( R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\} \) and it is given that \( R \) is a subring of \( \mathbb{R} \). Define

\[
\hat{\cdot}: R \to R, \ a + b\sqrt{10} \mapsto a - b\sqrt{10},
\]

\[
N : R \to \mathbb{Z}, \ r \mapsto r \hat{r}.
\]

Observe that if \( r = a + b\sqrt{10} \) then \( \hat{r} = a - b\sqrt{10} \) and \( N(r) = a^2 - 10b^2 \).

(a) We will show that \( \hat{\cdot} \) is a ring isomorphism.

Let \( r = r_1 + r_2\sqrt{10} \) and \( s = s_1 + s_2\sqrt{10} \). Then \( r + s = (r_1 + s_1) + (r_2 + s_2)\sqrt{10} \) and

\[
\hat{r + s} = \hat{(r_1 + s_1) + (r_2 + s_2)\sqrt{10}}
= r_1 - r_2\sqrt{10} + s_1 - s_2\sqrt{10}
= \hat{r} + \hat{s}.
\]

We have \( rs = (r_1 s_1 + 10r_2 s_2) + (r_1 s_2 + r_2 s_1)\sqrt{10} \), so

\[
\hat{r}s = (r_1 s_1 + 10r_2 s_2) - (r_1 s_2 + r_2 s_1)\sqrt{10}
= r_1 s_1 - r_1 s_2\sqrt{10} - r_2 s_2\sqrt{10} + 10r_2 s_2
= r_1 (s_1 - s_2\sqrt{10}) - r_2\sqrt{10}(s_1 - s_2\sqrt{10})
= (r_1 - r_2\sqrt{10})(s_1 - s_2\sqrt{10})
= \hat{r} \hat{s}.
\]

It is clear from this that \( \hat{\cdot} \) is a ring homomorphism. We will now show that it is bijective.
Let \( a - b \sqrt{10} = c - d \sqrt{10} \) in the image of \( \bar{\cdot} \). Then \((a - c) + (d - b)\sqrt{10} = 0\). Now, a rational number plus an irrational number is always irrational. But this sum is 0, which is rational, so \((d - b)\sqrt{10}\) must be rational. The only integer scalar of \( \sqrt{10} \) that yields a rational number is 0, so \( d - b = 0 \) and \( d = b \). From here it is obvious that also \( a - c = 0 \) and \( a = c \). Thus, the preimages \( a + b \sqrt{10} \) and \( c + d \sqrt{10} \) are equal and \( \bar{\cdot} \) is one-one.

Let \( r = a + b\sqrt{10} \in R \). Consider \( s = a - b\sqrt{10} \in R \). We have \( \bar{s} = a - (b)\sqrt{10} = a + b\sqrt{10} = r \), so \( \bar{\cdot} \) is onto. Therefore, \( \bar{\cdot} \) is a ring isomorphism by definition.

(b) We will show that \( N(rs) = N(r)N(s) \).

By definition, \( N(rs) = (rs)(\bar{r}\bar{s}) \). We showed in part (a) that \( \bar{\cdot} \) is a homomorphism under multiplication, so \((rs)(\bar{r}\bar{s}) = (rs)(\bar{r}\bar{s}) \). It was given that \( R \) is a subring of \( \mathbb{R} \), and the real numbers are commutative, so \((rs)(\bar{r}\bar{s}) = rs\bar{r}\bar{s} = r\bar{r}s\bar{s} \). But from this it is clear that \( N(rs) = r\bar{r}s\bar{s} = N(r)N(s) \).

(c) We will show that \( r = 0 \) if and only if \( N(r) = 0 \).

Suppose \( r = 0 \); that is, \( r = a + b\sqrt{10} \) and \( a = b = 0 \). Then
\[
N(r) = a^2 - 10b^2 = 0 - 10(0) = 0.
\]

Suppose \( N(r) = 0 \); that is, \( a^2 - 10b^2 = 0 \). This implies \( a^2 = 10b^2 \) and equivalently \( a = b\sqrt{10} \). Since the left-hand side is rational \((a \in \mathbb{Z})\), the right-hand side must also be rational. The only integer multiple of \( \sqrt{10} \) that is rational is 0, so \( b = 0 \) and thus \( a = 0 \). This means \( r = 0 \).

(d) We will show that \( r \) is a unit if and only if \( N(r) = \pm 1 \).

Suppose \( r \in R \) is a unit. So by definition, \( s \in R \) exists such that \( rs = sr = 1 \). We showed in part (b) that \( N \) is a multiplicative homomorphism, so by 2.5.6(b) we have \( N(s) \) the multiplicative inverse of \( N(r) \) in \( \mathbb{Z} \). Hence, \( N(r) \) is a unit in \( \mathbb{Z} \) and so \( N(r) \) must be \( \pm 1 \) because these are the only units.

Suppose \( N(r) = \pm 1 \) for some \( r \in R \). Let us look at \( s \), the inverse of \( r \) in \( \mathbb{R} \). We will show that \( s \) is necessarily in \( R \), thus making \( r \) a unit. Let \( r = r_1 + r_2\sqrt{10} \) and \( s = s_1 + s_2\sqrt{10} \). If \( rs = 1 \), then \( r_1s_1 + 10r_2s_2 = 1 \) and \( r_1s_2 + r_2s_1 = 0 \). It follows that \( s_2 = -\frac{r_2s_1}{r_1} \) and substitution yields
\[
\begin{align*}
  r_1s_1 + 10r_2s_2 \left( \frac{-r_2s_1}{r_1} \right) &= 1 \\
  r_1s_1^2 - 10r_2^2s_1 &= r_1 \\
  s_1 &= \frac{r_1}{r_1^2 - 10r_2^2} = \frac{r_1}{N(r)}.
\end{align*}
\]

We can plug this representation of \( s_1 \) into the earlier expression of \( s_2 \) to get
\[
s_2 = \frac{-r_2 \frac{r_1}{r_1}}{r_1} = \frac{-r_2}{N(r)}.
\]

Since \( r \in R \) we know \( r_1 \) and \( r_2 \) are integers. Since \( N(r) = \pm 1 \) we know \( N(r) \mid r_1 \) and \( N(r) \mid -r_2 \); that is, the denominators divide the numerators in \( s_1 \) and \( s_2 \). This means \( s_1, s_2 \in \mathbb{Z} \) and consequently, \( s \in R \). Hence, the inverse of \( r \) exists in \( R \) and \( r \) is a unit.

(e) We will show that 2, 3, and \( 4 \pm \sqrt{10} \) are irreducible in \( R \).

Suppose to the contrary that \( ab = 2 \) and \( a, b \) are not units. We know \( N(2) = 2^2 - 10(0) = 4 \) so also \( N(ab) = 4 \). By part (b), \( N(ab) = N(a)N(b) = 4 \). But \( a \) and \( b \) are not units, so by part (d) we have \( N(a) \neq \pm 1 \) and \( N(b) \neq \pm 1 \). Since \( N(a) \) and \( N(b) \) must both be factors of 4 without being \( \pm 1 \), it is necessarily the case that \( N(a) = N(b) = \pm 2 \). Thus, \( N(a) = N(b) \equiv 2, 3 \) (mod 5).

Now, in terms of modulus 5, \( N(a) \) and \( N(b) \) are determined by \( a_1^2 \) and \( b_1^2 \), respectively, because the
Subtraction of a multiple of 5 (i.e., 10a₁² and 10b₂²) does not alter the congruence class. This means \(N(a) \equiv N(b) \equiv a₁² \equiv b₂²\). But observe the square of an integer is congruent to 0, 1, or 4 (mod 5):

\[
\begin{align*}
(0)² & \equiv 0 \\
(1)² & \equiv 1 \\
(2)² & \equiv 4. 
\end{align*}
\]

This contradicts the fact that \(N(a)\) and \(N(b)\) are congruent to 2 or 3 (mod 5). Therefore, \(a\) and \(b\) do not exist and \(2 \in R\) is irreducible.

Suppose \(ab = 3\) and \(a, b\) are not units. Then \(N(3) = N(ab) = N(a)N(b) = 9\). By part (d), \(N(a) \neq \pm 1\) and \(N(b) \neq \pm 1\) so it must be \(N(a) = N(b) = \pm 3\). Thus, \(N(a) \equiv N(b) \equiv 2, 3 \pmod{5}\). We reach the same contradiction, and conclude \(3 \in R\) is irreducible.

Similarly, suppose \(ab = 4 \pm \sqrt{10}\). Then \(N(4 \pm \sqrt{10}) = N(ab) = N(a)N(b) = 4² - 10(1) = 6\). By part (d), \(N(a) \neq \pm 1\) and \(N(b) \neq \pm 1\) so it must be \(N(a) = \pm 2\), \(N(b) = \pm 3\) or \(N(a) = \pm 3\), \(N(b) = \pm 2\). In any case, \(N(a) \equiv 2, 3 \pmod{5}\) and \(N(b) \equiv 2, 3 \pmod{5}\). This leads to the same contradiction as above. Therefore, \(a\) and \(b\) do not exist and \(4 \pm \sqrt{10} \in R\) are irreducible.

(f) We will show that 2, 3, and \(4 \pm \sqrt{10}\) are not prime in \(R\).

Observe \(2 \cdot 3 = 6\) and \((4 + \sqrt{10})(4 - \sqrt{10}) = 16 - 10 = 6\). So \(2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})\). This means \(2 | (4 + \sqrt{10})(4 - \sqrt{10})\). But \(2 \not{|} (4 + \sqrt{10})\) and \(2 \not{|} (4 - \sqrt{10})\). Thus, 2 is not prime in \(R\).

Similarly, \(3 | (4 + \sqrt{10})(4 - \sqrt{10})\) while \(3 \not{|} (4 + \sqrt{10})\) and \(3 \not{|} (4 - \sqrt{10})\). Thus, 3 is not prime in \(R\).

Again, using \(2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})\), we see that \((4 \pm \sqrt{10})\) \(2 \cdot 3\) but \((4 \pm \sqrt{10}) \not{|} 2\) and \((4 \pm \sqrt{10}) \not{|} 3\). So neither of these are prime in \(R\).

(g) We will show that every proper element in \(R\) is a product of irreducible elements. We will use induction on \(|N|\).

For \(r \in R\), if \(|N(r)| = 0\) or \(|N(r)| = 1\) then \(r = 0\) by part (c) or \(r\) is a unit by part (d), respectively. These are not proper elements. So for our Base Step, assume \(|N(r)| = 2\) and \(r\) is proper. If \(r\) is irreducible, we are done. Suppose \(r \in R\) is not irreducible. Then by definition, there exist \(a, b \in R\) such that \(r = ab\) and \(a, b\) are not units. We have \(|N(r)| = |N(ab)| = |N(a)N(b)| = 2\). Since \(a\) and \(b\) are not units, \(|N(a)| \neq 1\) and \(|N(b)| \neq 1\) By part (d), \(|N(a)| \neq 1\) and \(|N(b)| \neq 1\) so \(|N(a)|\) and \(|N(b)|\) must both be strictly smaller than \(n + 1\). This means \(a\) and \(b\) are products of irreducible elements. But \(r = ab\) so we can write \(r\) as the product of irreducible elements. Thus, the inductive step holds.

For the Inductive Step, assume any proper element \(r \in R\) is the product of irreducible elements whenever \(|N(r)| \leq n\). Let \(r \in R\) be a proper element with \(|N(r)| = n + 1\). If \(r\) is irreducible we are done. Suppose \(r\) is not irreducible. Then there exist \(a, b \in R\) such that \(r = ab\) and \(a, b\) are not units. We have \(|N(r)| = |N(ab)| = |N(a)N(b)| = n + 1\). By part (d), \(|N(a)| \neq 1\) and \(|N(b)| \neq 1\) so \(|N(a)|\) and \(|N(b)|\) must both be strictly smaller than \(n + 1\). This means \(a\) and \(b\) are products of irreducible elements. But \(r = ab\) so we can write \(r\) as the product of irreducible elements. Thus, the inductive step holds.

4

**Proposition.** Let \(R\) be a Unique Factorization Domain (UFD). If \(I\) is a non-zero principal ideal in \(R\), then \(I\) is contained in only a finite number of principal ideals of \(R\).

**Proof.** Define \(I = \{Rb \mid b \in R, I \subseteq Rb\}\). If \(I = R\) then \(I\) itself is the only principal ideal containing \(I\) and \(|I| = 1\) is obviously finite. So let us assume that \(I = Ra\) for some \(a \in R\) and \(\{0_R\} \neq Ra \neq R\); that is, \(a\) is a proper element of \(R\). We will show that \(|I|\) is finite.

Since \(a\) is a proper element and \(R\) is a UFD, there exist primes \(p_i, 1 \leq i \leq n\), such that \(a = p_1 \ldots p_n\). Note that by 3.3.12 this prime factorization of \(a\) is unique up to association and permutation. We will use \(q_j\) to denote prime elements of \(R\) with \(q_j \neq p_i\) for any \(1 \leq i \leq n\).

**Case 1:** Suppose \(I \subseteq Rb = R\). All such elements whose generated ideal is \(R\) only contribute a total of \(1\) element to \(I\); namely, \(R, I \subseteq I\). So the finiteness of \(I\) will depend on the following cases where we will assume \(b\) is proper.
Case 2: Suppose $I \subseteq Rb$ and $a = rb$ where $r \in R$ is a unit. By definition, $r^{-1}$ exists in $R$ and so $r^{-1}a = r^{-1}(rb) = b$. So $b \in I$ and it follows that $Rb \subseteq I$. In fact, $Rb = I$. All such elements whose generated ideal is $I$ only contribute a total of 1 element to $\mathcal{I}$; namely, $I \in \mathcal{I}$. So the finiteness of $\mathcal{I}$ still depends on the following cases where we will assume that if $a = rb$, then $r$ is proper.

Case 3: Suppose $I \subseteq Rb$ with $b = q_1 \ldots q_m$ for primes $q_j$, $1 \leq j \leq m$. So the primes dividing $b$ are entirely distinct from the primes dividing $a$. Now, $a \in I \subseteq Rb$ so $a = rb = r(q_1 \ldots q_m)$ for some $r \in R$. Since $r$ is a proper element, then $r$ can be factored into primes $l_1 \ldots l_k$ and we have

$$a = p_1 \ldots p_n = (l_1 \ldots l_k)(q_1 \ldots q_m).$$

But this contradicts the unique factorization of $a$ since we assumed at least the $q$’s to not be associate with the $p$’s. Therefore, this case contributes no elements to $\mathcal{I}$.

Case 4: Suppose $I \subseteq Rb$ with $b = p_1 \ldots p_n q_1 \ldots q_m$ for primes $p_i$, $1 \leq h < n$, and $q_j$, $1 \leq j \leq m$. Since $a \in I \subseteq Rb$ we must have $a = rb$ for some $r \in R$. Since $r$ is proper, it can be factored into primes $r = l_1 \ldots l_k$. Hence,

$$a = p_1 \ldots p_n = (l_1 \ldots l_k)(p_1 \ldots p_n q_1 \ldots q_m) = p_1 \ldots p_n(l_1 \ldots l_k q_1 \ldots q_m),$$

because $R$ is commutative. Since $R$ is an integral domain we can cancel, yielding

$$p_{h+1} \ldots p_n = l_1 \ldots l_k q_1 \ldots q_m.$$ 

But this contradicts unique factorization because the $q$’s are not associate with the $p$’s. Therefore, this case contributes no elements to $\mathcal{I}$.

Case 5: Suppose $I \subseteq Rb$ with $b = p_1 \ldots p_n q_1 \ldots q_m$ (its prime factorization). Again, since $a \in I \subseteq Rb$ we must have $a = rb$ for some proper $r \in R$, $r = l_1 \ldots l_k$ (its prime factorization). But then

$$a = p_1 \ldots p_n = (l_1 \ldots l_k)(p_1 \ldots p_n q_1 \ldots q_m) = p_1 \ldots p_n(l_1 \ldots l_k q_1 \ldots q_m).$$

Since a UFD is an integral domain, we can cancel $p_1 \ldots p_n$ to get $1_R = l_1 \ldots l_k q_1 \ldots q_m$. But this implies the primes on the right-hand side are invertible, which means their generated ideal is $R$ (3.3.3) and so they are not proper elements. This contradicts the definition of a prime element. Therefore, this case contributes no elements to $\mathcal{I}$.

Case 6: Suppose $I \subseteq Rb$ with $b = p_1 \ldots p_h$ for primes $p_i$, $1 \leq i \leq h < n$. There is no contradiction here because $a = (p_{h+1} \ldots p_n)b \in Rb$. Note that this case contributes at most $2^n - 2$ elements to $\mathcal{I}$, a finite number.

In summary, we found $R, I \in \mathcal{I}$ and for proper elements $b$, $I \subseteq Rb$ if and only if the prime factorization of $b$ contains no primes other than those from the prime factorization of $a$. Thus, $\mathcal{I}$ is a finite set; in particular, $|\mathcal{I}| \leq 2^n$. □
Let \( R = \{a + bi \mid a, b \in \mathbb{Z}\} \) and it is given that \( R \) is a subring of \( \mathbb{C} \). Define
\[
\phi : R \to \mathbb{N}, \quad a + bi \to a^2 + b^2.
\]
We will show that \( \phi \) is a Euclidean function.

Let \( a + bi, c + di \in R \) with \( c + di \neq 0 \).

(i) We must show that \( \phi(0) < \phi(c + di) \). Clearly, \( \phi(0) = 0 \). Since \( c + di \neq 0 \), \( c \neq 0 \) or \( d \neq 0 \). In either case, \( \phi(c + di) = c^2 + d^2 \geq 1 > 0 = \phi(0) \).

(ii) We must show that \( (a + bi)(c + di) \neq 0 \) implies \( \phi(c + di) \leq \phi((a + bi)(c + di)) \). Suppose \( (a + bi)(c + di) \neq 0 \). Then \( a + bi \neq 0 \). Now, consider \( \phi((a + bi)(c + di)) \). We can rewrite this as
\[
\phi((ac - bd) + (ad + bc)i) = (ac - bd)^2 + (ad + bc)^2
= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2
= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2
= a^2(c^2 + d^2) + b^2(c^2 + d^2)
= (a^2 + b^2)(c^2 + d^2).
\]
We noted that \( a + bi \neq 0 \), so by (i) we have \( \phi(a + bi) = a^2 + b^2 \geq 1 \). Since \( c + di \neq 0 \) by assumption, \( \phi(c + di) = c^2 + d^2 \geq 1 \). Hence, \( c^2 + d^2 \leq (a^2 + b^2)(c^2 + d^2) \). But we know that this is the same as \( \phi(c + di) \leq \phi((a + bi)(c + di)) \).

(iii) We must show that there exist \( q, r \in R \) such that \( a + bi = q(c + di) + r \) and \( \phi(r) < \phi(c + di) \). Recall \( c + di \neq 0 \). Put \( x = (a + bi)/(c + di) \) and note that \( x \in \mathbb{C} \) and we have left \( R \). We will use \( x \) as a bridge to \( q \) and \( r \), which will be back in \( R \). Define \( y = y_1 + y_2i \in \mathbb{C} \) by
\[
y_1 = \begin{cases} 
  x_1 - \lfloor x_1 \rfloor & \text{if } |x_1 - \lfloor x_1 \rfloor| \leq |x_1 - \lceil x_1 \rceil| \\
  x_1 - \lceil x_1 \rceil & \text{if } |x_1 - \lfloor x_1 \rfloor| > |x_1 - \lceil x_1 \rceil|.
\end{cases}
y_2 = \begin{cases} 
  x_2 - \lfloor x_2 \rfloor & \text{if } |x_2 - \lfloor x_2 \rfloor| \leq |x_2 - \lceil x_2 \rceil| \\
  x_2 - \lceil x_2 \rceil & \text{if } |x_2 - \lfloor x_2 \rfloor| > |x_2 - \lceil x_2 \rceil|.
\end{cases}
\]
Then \( y \) has the properties that \( (x - y) \in R \) because the “decimal portions” of \( x \) have been subtracted away by \( y \), and \( |y_1| \leq 1/2 \), \( |y_2| \leq 1/2 \) because they were defined to be the distance to the nearest integer. So we put \( q = x - y \in R \) and \( r = (a + bi) - q(c + di) \in R \). Observe that
\[
q(c + di) + r = q(c + di) + (a + bi) - q(c + di)
= a + bi.
\]
It remains to be shown that \( \phi(r) < \phi(c + di) \).

Since \( |y_i| \leq 1/2, 1 \leq i \leq 2 \), we know \( \phi(y) \leq (1/2)^2 + (1/2)^2 = 1/2 \) (where \( \phi \) has been extended naturally to \( \mathbb{C} \)). Now, by construction
\[
r = \begin{cases} 
  (a + bi) - q(c + di) & = x(c + di) - q(c + di) = (x - q)(c + di) = (x - (x - y))(c + di) = y(c + di),
\end{cases}
\]
So \( \phi(r) = \phi(y(c + di)) \), and
\[
\phi(r) = \phi(y(c + di)) \overset{(1)}{=} \phi(y)\phi(c + di) \leq \frac{1}{2} \phi(c + di)
\]
and we are done.