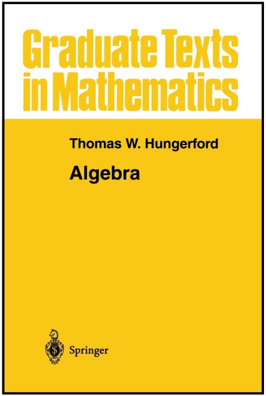
# Modern Algebra

## Chapter III. Rings

III.3. Supplement. Gaussian Integers—Proofs of Theorems



# Table of contents

# Theorem B (Fraleigh's Theorem 47.7)

**Theorem B.** (Fraleigh's Theorem 47.7) If $D$ is an integral domain with a multiplicative norm $N$, then $N(1_D) = 1$ and $|N(u)| = 1$ for every unit $u \in D$. If, furthermore, every $\alpha$ satisfying $|N(\alpha)| = 1$ is a unit in $D$, then an element $\pi \in D$ with $|N(\pi)| = p$, for a prime $p \in \mathbb{Z}$, is an irreducible of $D$.

**Proof.** Let $D$ be an integral domain with a multiplicative norm $N$. Then $N(1_D) = N((1_D)(1_D)) = N(1_D)N(1_D)$ and so $N(1_D)$ is either 0 or 1. By Property 1 of the definition of multiplicative norm, we have that $N(1_D) = 1$. If $u \in D$ is a unit then $1 = N(1_D) = N(uu^{-1}) = N(u)N(u^{-1})$. Since $N(u)$ is an integer then $N(u) = \pm 1$ and $|N(u)| = 1$.

# Theorem B (Fraleigh's Theorem 47.7)

**Theorem B.** (Fraleigh's Theorem 47.7) If $D$ is an integral domain with a multiplicative norm $N$, then $N(1_D) = 1$ and $|N(u)| = 1$ for every unit $u \in D$. If, furthermore, every $\alpha$ satisfying $|N(\alpha)| = 1$ is a unit in $D$, then an element $\pi \in D$ with $|N(\pi)| = p$, for a prime $p \in \mathbb{Z}$, is an irreducible of $D$.

**Proof.** Let $D$ be an integral domain with a multiplicative norm $N$. Then $N(1_D) = N((1_D)(1_D)) = N(1_D)N(1_D)$ and so $N(1_D)$ is either 0 or 1. By Property 1 of the definition of multiplicative norm, we have that $N(1_D) = 1$. If $u \in D$ is a unit then $1 = N(1_D) = N(uu^{-1}) = N(u)N(u^{-1})$. Since $N(u)$ is an integer then $N(u) = \pm 1$ and $|N(u)| = 1$.

Now suppose that the units of $D$ are exactly the elements of norm $\pm 1$. Let $\pi \in D$ be such that $|N(\pi)| = p$ where $p \in \mathbb{Z}$ is prime. Then if $\pi = \alpha\beta$ we have $p = |N(\pi)| = |N(\alpha)N(\beta)|$ so either $|N(\alpha)| = 1$ or $|N(\beta)| = 1$ since $p$ is prime. By hypothesis then either $\alpha$ or $\beta$ is a unit of $D$. So $\pi = \alpha\beta$ implies either $\alpha$ or $\beta$ is a unit; that is, $\pi$ is irreducible. □

# Theorem B (Fraleigh's Theorem 47.7)

**Theorem B.** (Fraleigh's Theorem 47.7) If $D$ is an integral domain with a multiplicative norm $N$, then $N(1_D) = 1$ and $|N(u)| = 1$ for every unit $u \in D$. If, furthermore, every $\alpha$ satisfying $|N(\alpha)| = 1$ is a unit in $D$, then an element $\pi \in D$ with $|N(\pi)| = p$, for a prime $p \in \mathbb{Z}$, is an irreducible of $D$.

**Proof.** Let $D$ be an integral domain with a multiplicative norm $N$. Then $N(1_D) = N((1_D)(1_D)) = N(1_D)N(1_D)$ and so $N(1_D)$ is either 0 or 1. By Property 1 of the definition of multiplicative norm, we have that $N(1_D) = 1$. If $u \in D$ is a unit then $1 = N(1_D) = N(uu^{-1}) = N(u)N(u^{-1})$. Since $N(u)$ is an integer then $N(u) = \pm 1$ and $|N(u)| = 1$.

Now suppose that the units of $D$ are exactly the elements of norm $\pm 1$. Let $\pi \in D$ be such that $|N(\pi)| = p$ where $p \in \mathbb{Z}$ is prime. Then if $\pi = \alpha\beta$ we have $p = |N(\pi)| = |N(\alpha)N(\beta)|$ so either $|N(\alpha)| = 1$ or $|N(\beta)| = 1$ since $p$ is prime. By hypothesis then either $\alpha$ or $\beta$ is a unit of $D$. So $\pi = \alpha\beta$ implies either $\alpha$ or $\beta$ is a unit; that is, $\pi$ is irreducible. □

# Lemma A

**Lemma A.** (Hungerford's Exercise III.3.3(a)) With $R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a + b\sqrt{10}) = (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$, we have that $N$ is a multiplicative norm on $R$.

**Proof.** Let $u = a + b\sqrt{10}$ and $v = c + d\sqrt{10}$. Then $uv = (a + b\sqrt{10})(c + d\sqrt{10}) = ac + 10bd + (ad + bc)\sqrt{10}$ and

$$\begin{aligned} N(uv) &= N(ac + 10bd + (ad + bc)\sqrt{10} \\ &= (ac + 10bd + (ad + bc)\sqrt{10})(ac + 10bd - (ad + bc)\sqrt{10}) \\ &= (ac + 10bd)^2 - 10(ad + bc)^2 \\ &= a^2c^2 + 10abcd + 100b^2d^2 - 10a^2d^2 - 20abcd - 10b^2c^2 \\ &= a^2c^2 - 10a^2d^2 - 10b^2c^2 + 100b^2d^2 \\ &= a^2(c^2 - 10d^2) - 10b^2(c^2 - 10d^2) \\ &= (a^2 - 10b^2)(c^2 - 10d^2) \\ &= N(a + b\sqrt{10})N(c + d\sqrt{10}) = N(u)N(v). \end{aligned}$$

# Lemma A

**Lemma A.** (Hungerford's Exercise III.3.3(a)) With $R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a + b\sqrt{10}) = (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$, we have that $N$ is a multiplicative norm on $R$.

**Proof.** Let $u = a + b\sqrt{10}$ and $v = c + d\sqrt{10}$. Then $uv = (a + b\sqrt{10})(c + d\sqrt{10}) = ac + 10bd + (ad + bc)\sqrt{10}$ and

$$\begin{aligned} N(uv) &= N(ac + 10bd + (ad + bc)\sqrt{10} \\ &= (ac + 10bd + (ad + bc)\sqrt{10})(ac + 10bd - (ad + bc)\sqrt{10}) \\ &= (ac + 10bd)^2 - 10(ad + bc)^2 \\ &= a^2c^2 + 10abcd + 100b^2d^2 - 10a^2d^2 - 20abcd - 10b^2c^2 \\ &= a^2c^2 - 10a^2d^2 - 10b^2c^2 + 100b^2d^2 \\ &= a^2(c^2 - 10d^2) - 10b^2(c^2 - 10d^2) \\ &= (a^2 - 10b^2)(c^2 - 10d^2) \\ &= N(a + b\sqrt{10})N(c + d\sqrt{10}) = N(u)N(v). \end{aligned}$$

# Lemma A (continued)

**Lemma A.** (Hungerford's Exercise III.3.3(a)) With $R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a + b\sqrt{10}) = (a + b\sqrt{10})(a - b\sqrt{10})$ $= a^2 - 10b^2$, we have that $N$ is a multiplicative norm on $R$.

**Proof (continued).** If $u = 0 = 0 + 0\sqrt{10}$ then $N(u) = N(0)$ $= (0)^2 - 10(0)^2 = 0$.

If $N(u) = N(a + b\sqrt{10}) = a^2 - 10b^2 = 0$ then $a^2 = 10b^2$. ASSUME either $a$ or $b$ in nonzero. Taking square roots, $\sqrt{a^2} = \sqrt{10b^2}$ or $|a| = \sqrt{10}|b|$. If $b \neq 0$ then we have $\sqrt{10} = |a|/|b| \in \mathbb{Q}$, a CONTRADICTION to the fact that $\sqrt{10}$ is irrational. So $b = a = 0$. That is, $u = 0$. □

# Lemma C

**Lemma C.** (Hungerford's Exercise III.3.3(c)) With $R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a + b\sqrt{10}) = a^2 - 10b^2$, we have that 2, 3, $4 + \sqrt{10}$, and $4 - \sqrt{10}$ are irreducible elements of $R$.

**Proof.** ASSUME that 2 is *not* irreducible. Notice that 2 is a nonzero nonunit (since $N(2) = 4 \neq \pm 1$, by part (a)). So, by definition (Definition III.3.3) 2 can be written as a product of two nonunits, $2 = uv$. By part (a), $4 = N(2) = N(uv) = N(u)N(v)$ where $N(u), N(v) \in \mathbb{Z}$. Since $u$ and $v$ are nonunits then by part (b) $N(u), N(v) \neq \pm 1$, and so we must have $N(u) = N(v) = 2$ or $N(u) = N(v) = -2$. With $u = a + b\sqrt{10}$ and $N(u) = 2$ we have $N(u) = a^2 - 10b^2 = 2$ and so $a^2 = 2 + 10b^2$. But this means that $a^2 \equiv 2 \pmod{10}$.

# Lemma C

**Lemma C.** (Hungerford's Exercise III.3.3(c)) With $R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a + b\sqrt{10}) = a^2 - 10b^2$, we have that 2, 3, $4 + \sqrt{10}$, and $4 - \sqrt{10}$ are irreducible elements of $R$.

**Proof.** ASSUME that 2 is *not* irreducible. Notice that 2 is a nonzero nonunit (since $N(2) = 4 \neq \pm 1$, by part (a)). So, by definition (Definition III.3.3) 2 can be written as a product of two nonunits, $2 = uv$. By part (a), $4 = N(2) = N(uv) = N(u)N(v)$ where $N(u), N(v) \in \mathbb{Z}$. Since $u$ and $v$ are nonunits then by part (b) $N(u), N(v) \neq \pm 1$, and so we must have $N(u) = N(v) = 2$ or $N(u) = N(v) = -2$. With $u = a + b\sqrt{10}$ and $N(u) = 2$ we have $N(u) = a^2 - 10b^2 = 2$ and so $a^2 = 2 + 10b^2$. But this means that $a^2 \equiv 2 \pmod{10}$.

# Lemma C (continued 1)

**Proof (continued).** But this means that $a^2 \equiv 2 \pmod{10}$. ...
This cannot happen since:

| $a \pmod{10}$ | $a^2 \pmod{10}$ |
|---|---|
| 0 | 0 |
| 1 | 1 |
| 2 | 4 |
| 3 | 9 |
| 4 | 6 |
| 5 | 5 |
| 6 | 6 |
| 7 | 9 |
| 8 | 4 |
| 9 | 1 |

With $u = a + b\sqrt{10}$ and $N(u) = -2$ we have $N(u) = a^2 - 10b^2 = -2$ and so $a^2 = -2 + 10b^2$. But this means that $a^2 \equiv 8 \pmod{10}$.

# Lemma C (continued 2)

**Proof (continued).** But this means that $a^2 \equiv 8 \pmod{10}$. ... This cannot happen, as shown in the table above. These CONTRADICTIONS show that the assumption that 2 is *not* irreducible is false and hence 2 is irreducible.

ASSUME 3 is *not* irreducible, say $3 = uv$ for nonunits $u$ and $v$. As argued for 2, we must have $9 = N(3) = N(u)N(v)$ where $N(u), N(v) \in \mathbb{Z}$, and we must have either $N(u) = N(v) = 3$ or $N(u) = N(v) = -3$. With $u = a + b\sqrt{10}$ and $N(u) = 3$ we have $N(u) = a^2 - 10b^2 = 3$ and so $a^2 = 3 + 10b^2$. But this means that $a^2 \equiv 3 \pmod{10}$. This cannot happen as shown in the table above. With $u = a + b\sqrt{10}$ and $N(u) = -3$ we have $N(u) = a^2 - 10b^2 = -3$ and so $a^2 = -3 + 10b^2$. But this means that $a^2 \equiv 7 \pmod{10}$. This cannot happen as shown in the table above. These CONTRADICTIONS show that the assumption that 3 is not irreducible is false and hence 3 is irreducible.

# Lemma C (continued 2)

**Proof (continued).** But this means that $a^2 \equiv 8 \pmod{10}$. ... This cannot happen, as shown in the table above. These CONTRADICTIONS show that the assumption that 2 is *not* irreducible is false and hence 2 is irreducible.

ASSUME 3 is *not* irreducible, say $3 = uv$ for nonunits $u$ and $v$. As argued for 2, we must have $9 = N(3) = N(u)N(v)$ where $N(u), N(v) \in \mathbb{Z}$, and we must have either $N(u) = N(v) = 3$ or $N(u) = N(v) = -3$. With $u = a + b\sqrt{10}$ and $N(u) = 3$ we have $N(u) = a^2 - 10b^2 = 3$ and so $a^2 = 3 + 10b^2$. But this means that $a^2 \equiv 3 \pmod{10}$. This cannot happen as shown in the table above. With $u = a + b\sqrt{10}$ and $N(u) = -3$ we have $N(u) = a^2 - 10b^2 = -3$ and so $a^2 = -3 + 10b^2$. But this means that $a^2 \equiv 7 \pmod{10}$. This cannot happen as shown in the table above. These CONTRADICTIONS show that the assumption that 3 is not irreducible is false and hence 3 is irreducible.

# Lemma C (continued 3)

**Lemma C.** (Hungerford's Exercise III.3.3(c)) With $R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a + b\sqrt{10}) = a^2 - 10b^2$, we have that 2, 3, $4 + \sqrt{10}$, and $4 - \sqrt{10}$ are irreducible elements of $R$.

**Proof (continued).** ASSUME $4 + \sqrt{10}$ is *not* irreducible, say $4 + \sqrt{10} = uv$ for nonunits $u$ and $v$. As argued for 2, we must have $N(4 + \sqrt{10}) = (4)^2 - 10(1)^2 = 6 = N(u)N(v)$ where $N(u), N(v) \in \mathbb{Z}$ and we must have either $N(u) = \pm 2$ and $N(v) = \pm 3$ (respectively) or $N(u) = \pm 3$ and $N(v) = \pm 2$ (respectively). However, we have seen above that we cannot have $N(u) = \pm 2$ nor $N(u) = \pm 3$, a CONTRADICTION. So the assumption that $4 + \sqrt{10}$ is irreducible.

For the irreducibility of $4 - \sqrt{10}$, the argument is the same as for $4 + \sqrt{10}$, since $N(4 + \sqrt{10}) = N(4 - \sqrt{10}) = 6$. □

# Lemma C (continued 3)

**Lemma C.** (Hungerford's Exercise III.3.3(c)) With $R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a + b\sqrt{10}) = a^2 - 10b^2$, we have that 2, 3, $4 + \sqrt{10}$, and $4 - \sqrt{10}$ are irreducible elements of $R$.

**Proof (continued).** ASSUME $4 + \sqrt{10}$ is *not* irreducible, say $4 + \sqrt{10} = uv$ for nonunits $u$ and $v$. As argued for 2, we must have $N(4 + \sqrt{10}) = (4)^2 - 10(1)^2 = 6 = N(u)N(v)$ where $N(u), N(v) \in \mathbb{Z}$ and we must have either $N(u) = \pm 2$ and $N(v) = \pm 3$ (respectively) or $N(u) = \pm 3$ and $N(v) = \pm 2$ (respectively). However, we have seen above that we cannot have $N(u) = \pm 2$ nor $N(u) = \pm 3$, a CONTRADICTION. So the assumption that $4 + \sqrt{10}$ is irreducible.

For the irreducibility of $4 - \sqrt{10}$, the argument is the same as for $4 + \sqrt{10}$, since $N(4 + \sqrt{10}) = N(4 - \sqrt{10}) = 6$. □

# Lemma E

**Lemma E.** (Hungerford's Exercise III.3.6(a)) If $a$ and $n$ are integers, $n > 0$, then there exist integers $q$ and $r$ such that $a = qn + r$, where $|r| \leq n/2$.

**Proof.** By the Division Algorithm (Theorem 0.6.3) there are integers $q'$ and $r'$ such that $a = q'n + r'$ with $0 \leq r' < |n| = n$. If $0 \leq r' \leq n/2$ then $q = q'$ and $r = r'$ are the desired integers. If $n/2 < r' < n$, then take $q = q' + 1$ and $r = r' - n$. This gives $-n/2 < r = r' - n < 0$ and so $|r| < n/2$ and $qn + r = (q' + 1)n + (r' - n) = q'n + r' = a$, so $q$ and $r$ are the desired integers. □

# Lemma E

**Lemma E.** (Hungerford's Exercise III.3.6(a)) If $a$ and $n$ are integers, $n > 0$, then there exist integers $q$ and $r$ such that $a = qn + r$, where $|r| \leq n/2$.

**Proof.** By the Division Algorithm (Theorem 0.6.3) there are integers $q'$ and $r'$ such that $a = q'n + r'$ with $0 \leq r' < |n| = n$. If $0 \leq r' \leq n/2$ then $q = q'$ and $r = r'$ are the desired integers. If $n/2 < r' < n$, then take $q = q' + 1$ and $r = r' - n$. This gives $-n/2 < r = r' - n < 0$ and so $|r| < n/2$ and $qn + r = (q' + 1)n + (r' - n) = q'n + r' = a$, so $q$ and $r$ are the desired integers. □