1. Let \( R \) be a ring and \( M \subset R \) an ideal. Assume \( M \neq R \) (but do not assume \( M \) is maximal). Let \( a \in R \).

   (a) Assume there exists an ideal \( N \) with \( M \subset N \subset R \) and \( M \neq M, R \) and \( a \in N \). Prove that \( a \) has no multiplicative inverse in \( R/M \).

   Solution: For any \( r \in R \), \( \overline{a} \cdot \overline{r} = \overline{ar} \). Setting \( n = ar \), as \( N \) is an ideal \( n \in N \). We claim \( n \neq 1 \). For if \( n = 1 \) then \( n - 1 = m \in M \subset N \) so \( 1 = n - (n - 1) \in N \) and \( N = R \).

   (b) Assume there does not exist an ideal \( N \) with \( M \subset N \subset R \) and \( M \neq M, R \), and \( a \in N \). Prove that \( \overline{a} \) has a multiplicative inverse in \( R/M \).

   Solution: Set 
   \[
   M^+ = \{ m + ar : m \in M, r \in R \}
   \]
   Then \( a \in M^+ \) so \( M \neq M^+ \) and \( M \subset M^+ \) and therefore (as there is no intermediate size ideal) \( M^+ = R \) so \( 1 \in M^+ \) and \( 1 = m + ar \) for some \( r \in R \) and so \( \overline{1} = \overline{ar} \).

2. Let \( R \) be a ring and let \( a, b \in R \). Set 
\[
M = \{ ar + bs : r, s \in R \}
\]
Prove that \( M \) is an ideal.

Solution:

(a) Identity: \( 0 = a(0) + b(0) \in M \)

(b) Closure under Addition. Let \( \alpha, \beta \in M \) so that \( \alpha = ar_1 + bs_1, \beta = ar_2 + bs_2 \). Then \( \alpha + \beta = a(r_1 + r_2) + b(s_1 + s_2) \in M \).

(c) Closure under Additive Inverse. Let \( \alpha \in M \) so that \( \alpha = ar + bs \). Then \( -\alpha = a(-r) + b(-s) \in M \).

(d) Closure under Multiplication by Anything. Let \( \alpha \in M \) so that \( \alpha = ar + bs \). For any \( t \in R \), \( t\alpha = a(rt) + b(st) \in M \).

3. Let \( \mathbb{Z}[i] = \{ a + bi : a, b \in \mathbb{Z} \} \) where \( i = \sqrt{-1} \), the usual Gaussian Integers.
(a) For \( \alpha \in \mathbb{Z}[i] \) define (this is called a norm) \( N(\alpha) = |\alpha|^2 \), where \( |\cdot| \) is the usual complex number absolute value, that is \( |c+di| = \sqrt{c^2 + d^2} \). Give a formula for \( N(\alpha) \) for \( \alpha \in R \). Show \( N(\alpha\beta) = N(\alpha)N(\beta) \).

Solution: \( N(a+bi) = a^2 + b^2 \). We need show 
\[(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (bc + ad)^2\]
This follows from elementary (high-school) algebra. Or we may think of this as the writing of complex numbers \( \alpha = a + bi = \text{Re}e^{i\theta} \), so that \( |\alpha| = \text{Re} \). When we multiply complex numbers the \( \text{Re} \) values multiply so that \( |\alpha\beta| = |\alpha| \cdot |\beta| \) and, squaring, \( N(\alpha\beta) = N(\alpha)N(\beta) \).

(b) Precisely which elements of \( \mathbb{Z}[i] \) have multiplicative inverses? (Use the norm to show that you have everything.)

Solution: \(+1, -1, i, -i\). To be a unit you must have norm one (as norms can’t go down under multiplication by nonzero elements) and so \( a^2 + b^2 = 1 \) which has these four solutions.

(c) Define \( \phi : \mathbb{Z}[i] \to \mathbb{Z}[i] \) by \( \phi(a+bi) = a - bi \). (This is generally known as complex conjugation.) Show that \( \phi \) is a homomorphism by showing \( \phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta) \) and \( \phi(\alpha\beta) = \phi(\alpha)\phi(\beta) \). Show that \( \phi \) has kernel \( \{0\} \).

Solution: Straightforward calculation.

(d) A number \( \alpha \in \mathbb{Z}[i] \) is called composite if we can write \( \alpha = \beta\gamma \) where neither \( \beta \) not \( \gamma \) have multiplicative inverses. (That last condition is to avoid “trivial” factorizations like \( 23 = i(-23i) \).)

If it is nonzero, not a unit, and not composite it is called prime. Show that \( 2 \) is composite. Show that \( 41 \) is composite. Show \( 7+2i \) is prime. (Idea: Use the norm)

Solution: \( 2 = (1+i)(1-i) \), \( 41 = (5+4i)(5-4i) \), but \( 7+2i \) has norm 53. If \( 7+2i = \alpha\beta \) then \( 53 = N(\alpha)N(\beta) \) and the norm is a positive integer and 53 is a prime in the integers so one of \( N(\alpha), N(\beta) = 1 \), say \( \alpha \), and thus \( \alpha \) is a unit.

4. Set 
\[ R = \{a+b\sqrt{-5} : a, b \in \mathbb{Z} \} \]

(a) Give a formula for \( N(\alpha) \) (as defined above) for \( \alpha = a+b\sqrt{-5} \in R \).

Solution: 
\[ N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2 + 5b^2 \]
(b) Precisely which elements of $R$ have multiplicative inverses? (Use the norm to argue that you have all of them.)

**Solution:** Only $+1, -1$. As norm goes up under multiplication by a nonzero element the norm must be one and these are the only two solutions to $a^2 + 5b^2 = 1$.

(c) Set

$$I = \{2\alpha + (1 + \sqrt{-5})\beta : \alpha, \beta \in R\}$$

Plot those $(a, b)$ with $-4 \leq a, b \leq +4$ so that $a + b\sqrt{-5} \in I$.

**Solution:** It will be a checkerboard pattern with every other element. That is, every $(a, b)$ with $a + b$ even.

(d) Show that $I$ is an ideal.

**Solution:** Special case of general result in second problem above.

(e) Show that $1 \not\in I$.

**Solution:** For any $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$ we have $2\alpha + (1 + \sqrt{-5})\beta = x + y\sqrt{-5}$ where $x = 2a + c - 5d$ and $y = 2b + c + d$. But then $x + y = 2a + 2b + 2c - 4d$ is even. That is, every element $x + y\sqrt{-5} \in I$ must have $x + y$ even. So $1 + 0\sqrt{-5} \not\in I$.

(f) Show that $I$ is not a principal ideal. (Idea: Assume $I = \langle \kappa \rangle$ and use the properties of $N(\cdot)$ above.)

**Solution:** If $I = \langle \kappa \rangle$ then $\kappa|2$ so $N(\kappa)|N(2) = 4$ and $\kappa|(1 + \sqrt{-5})$ so $N(\kappa)|N(1 + \sqrt{-5}) = 6$. So $N(\kappa)|2$. But no $\kappa \in R$ has norm two so $N(\kappa) = 1$ so $\kappa = \pm 1$ but we know $1, -1 \not\in I$.

(g) Find representatives of $R/I$. What well known field is it isomorphic to?

**Solution:** $R/I = \{0, 1\}$ and is isomorphic to $\mathbb{Z}_2$. 