Algebra III: Rings and Modules
Solutions for Problem Sheet 1, Autumn Term 2022-23

John Nicholson

1. For sets X and Y, let $\mathrm{Fun}(X,Y)$ denote the set of all functions $f : X \to Y$.

   (i) Let X be a set and R a ring. Given $f, g \in \mathrm{Fun}(X,R)$, we can define $f+g, f \cdot g \in \mathrm{Fun}(X,R)$ via $(f+g)(x) = f(x) +_R g(x)$ and $(f \cdot g)(x) = f(x) \cdot_R g(x)$ for $x \in X$. Given $a \in R$, we can consider the constant function $c_a : x \mapsto a$ for all $x \in X$. Show that $\mathrm{Fun}(X,R)$ is a ring with $0 = c_0$ and $1 = c_1$.

   (ii) Let $X = [0,1] \subseteq \mathbb{R}$, the interval, and let $R = \mathbb{R}$. Show that the subset of $\mathrm{Fun}([0,1],\mathbb{R})$ of continuous functions is a subring, and that the subset of differentiable functions is a further subring.

   (iii) Show that, if X has at least two elements, then $\mathrm{Fun}(X,R)$ is not an integral domain (regardless of what R is). [Hint: For a complete solution you will have to consider separately the trivial case $R = \{0\}$.]

   Solution: (i) First, $(0+f)(x) = 0 + f(x) = f(x)$ and $(1 \cdot f)(x) = 1 \cdot f(x) = f(x)$, so 0 and 1 are the additive and multiplicative identities, respectively. Next $((f+g)+h)(x) = f(x)+g(x)+h(x) = (f+(g+h))(x)$ and similarly $((fg)h)(x) = f(x)g(x)h(x) = (f(gh))(x)$ so the operations are associative. The addition is commutative for the same reason: $(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x)$. Finally the function $(-f)(x) := -f(x)$ is clearly the additive inverse to f, and $(f(g+h))(x) = f(x)(g(x)+h(x)) = f(x)g(x) + f(x)h(x) = (fg+fh)(x)$ verifies distributivity.

   (ii) It suffices to note that the constant functions are continuous (as well as differentiable), and sums, differences, and products of continuous (or differentiable) functions are continuous (or differentiable).

   (iii) If R is zero, then $\mathrm{Fun}(X,R) = \{0\}$ as well, which is not an integral domain. Suppose R is nonzero. Let $x_0, x_1 \in X$ be distinct points, and let f, g be functions such that $f(x_0) = 0, f(x_1) = 1, g(x_0) = 1$, and $g(x_1) = 0$. Then $fg = 0$ even though f and g are nonzero.

2. For a ring R, an element $a \in R$ is *nilpotent* if $a^n = 0$ for some $n \geq 1$. Let $\mathrm{nil}(R) \subseteq R$ be the subset of nilpotent elements.

   (i) Let R be a commutative ring. Show that $\mathrm{nil}(R)$ is an ideal. [Hint: Prove that the binomial formula for the expansion of $(x+y)^n$ holds in arbitrary commutative rings.]

   (ii) Give an example of a non-commutative ring where $\mathrm{nil}(R)$ does not form an ideal.

   (iii) Let $x \in R$ be nilpotent (and do not assume R is commutative). Show that $1 + x \in R^\times$.

   (iv) Find all the nilpotent elements in the ring $R = \mathbb{Z}/p^r\mathbb{Z}$ for every prime p and $r \geq 1$. [Optional: extend this to $\mathbb{Z}/n\mathbb{Z}$ for every $n \in \mathbb{Z}$.]

Solution: (i) If x and y commute and $x^m = 0 = y^n$ (for some $m, n \geq 1$), then the binomial theorem shows that $(x+y)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} x^i y^{m+n-1-i}$: for $i \leq m-1$, we have $y^{m+n-1-i} = 0$ and for $i \geq m$ we have $x^i = 0$, so that each term is actually zero. Thus $(x+y)^{m+n-1} = 0$. Since x^m implies $(-x)^m = (-1)^m x^m = 0$, we conclude that $\mathrm{nil}(R)$ is an abelian subgroup of R. Next, for every x with $x^m = 0$, we have $(ax)^m = a^m x^m = 0$. Therefore $\mathrm{nil}(R)$ is an ideal.

(ii) Almost any non-commutative ring will do, for example, $R = M_2(\mathbb{R})$. In here we have $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and so the LHS is a sum of two nilpotent elements whereas the RHS is not nilpotent.

(iii) The geometric series expansion is $1 - x + x^2 - x^3 + \cdots$. Indeed, if $x^n = 0$, then $(1+x)(1 - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1}) = 1$. Similarly $(1 - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1})(1+x) = 1$. Thus $1 + x$ is invertible.

(iv) The nilpotent elements in $\mathbb{Z}/p^r\mathbb{Z}$ are the multiples of p, namely $\overline{kp}$ for $0 \leq k \leq p^{r-1} - 1$. In $\mathbb{Z}/n\mathbb{Z}$, the nilpotent elements are $r \in \mathbb{Z}/n\mathbb{Z}$ such that $p \mid n$ implies $p \mid r$ for all primes p. That is, if $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ for $\alpha_i \geq 1$ integers, then r is nilpotent if and only if $p_1 \cdots p_m \mid r$.

3. Show the following:

   (i) If $a > 0$, then $\mathbb{R}[X]/(X^2 - a) \cong \mathbb{R} \times \mathbb{R}$.

   (ii) Show that $(\mathbb{Z}/3)[X]/(X^2+1)$ is a field with nine elements.

   (iii) Show that, for any $n \geq 1$, then $\mathbb{Z}[i]/(n) \cong (\mathbb{Z}/n)[X]/(X^2+1)$.

   (iv) Show that $\mathbb{Z}[i]/(2) \cong (\mathbb{Z}/2)[X]/(X^2)$. In particular observe that this is not a field.

Solution: (i) Consider the evaluation homomorphism $\varphi = \mathrm{ev}_{(\sqrt{a}, -\sqrt{a})} : \mathbb{R}[x] \to \mathbb{R} \times \mathbb{R}$ sending x to $(\sqrt{a}, -\sqrt{a})$. (Explicitly, $\varphi(\sum_i b_i x^i) = (\sum_i b_i \sqrt{a^i}, \sum_i (-1)^i b_i \sqrt{a^i})$.) Then $\varphi(x^2 - a) = 0$. Also, φ is surjective. Thus we get a surjective homomorphism $\bar{\varphi} : \mathbb{R}[x]/(x^2 - a)\mathbb{R}[x] \to \mathbb{R} \times \mathbb{R}$. Since $\bar{\varphi}$ is actually a surjective linear map of two-dimensional $\mathbb{R}$-vector spaces, it must be injective and hence an isomorphism. [One could also explicitly show that $\ker(\varphi) = (x^2 - a)\mathbb{R}[x]$, using the explicit formula for φ, and then the first isomorphism theorem implies that we get an isomorphism $\mathbb{R}[x]/(x^2 - a)\mathbb{R}[x] \xrightarrow{\sim} \mathbb{R} \times \mathbb{R}$.]

(ii) First of all, we claim that $R := (\mathbb{Z}/3)[x]/(x^2+1)$, as a set, is $\{a + bx + (x^2+1) \mid a, b \in \mathbb{Z}/3\}$, so it has nine elements. To see this, note that by long division, any polynomial f of degree ≥ 2 satisfies $f = (x^2+1)g + h$ for h a polynomial of degree ≤ 1. On the other hand, no two distinct polynomials of degree ≤ 1 can differ by a multiple of x^2+1. Thus we have established the claim and R indeed has nine elements.

We have to show R is a field. It is enough by our theorem from lecture to show it is an integral domain. It is clearly commutative and nonzero, so we just have to show it has no zero divisors. Assume the contrary. Then there exist $f(x), g(x) \in (\mathbb{Z}/3)[x]$, neither of which are multiples of x^2+1, but such that $f(x)g(x)$ was a multiple of x^2+1. In fact, since we already observed all elements in $(\mathbb{Z}/3)[x]/(x^2+1)$ can be written as degree ≤ 1 polynomials, we can assume this for $f(x)$ and $g(x)$. So it suffices to observe that x^2+1 has no linear factors over the field $\mathbb{Z}/3$. Having linear factors is equivalent to having roots. Note that $\overline{1} = \overline{0}^2 + \overline{1} = \overline{1}^2 + \overline{1} = \overline{2} = \overline{2}^2 + \overline{1}$ in $\mathbb{Z}/3$, so there are no roots of x^2+1 in $\mathbb{Z}/3$. Thus it has no linear factors and there do not exist such $f(x)$ and $g(x)$. We conclude that $(\mathbb{Z}/3)[x]/(x^2+1)$ is an integral domain, and therefore a field.

(iii) We have the evaluation homomorphism $\mathrm{ev}_i : \mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}[i]$, the kernel of which is (x^2+1). We can further mod by n to obtain $\varphi : \mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}[i]/(n)$, the kernel of which is then (x^2+1, n). On the other hand we also have the surjective homomorphism $\mathbb{Z}[x] \twoheadrightarrow (\mathbb{Z}/n)[x]/(x^2+1)$, modding by (n, x^2+1). Since they are both surjections with the same kernel, we get that both $\mathbb{Z}[i]/(n)$ and $(\mathbb{Z}/n)[x]/(x^2+1)$ are isomorphic to $\mathbb{Z}[x]/(n, x^2+1)$, hence they are isomorphic.

(iv) Note that in lecture notes there was mentioned a way to do this, $\mathbb{Z}[i]/(2) = \mathbb{Z}[\sqrt{2i}]/(2i)$ since $\sqrt{2i} = 1 + i$ and $(2) = (2i)$, and by the argument there, this is isomorphic to $(\mathbb{Z}/2)[x]/(x^2)$ via the map sending $\sqrt{2i}$ to x. You should give more details to have a complete solution though.

Let us give a more straightforward solution. Consider the map $\varphi : \mathbb{Z}[i] \to (\mathbb{Z}/2)[x]/(x^2)$, $\varphi(a + bi) = \overline{a} + \overline{b}(1 + x)$ (or more precisely, $(\overline{a} + \overline{b}(1 + x)) + (x^2)$). To check this is a homomorphism, note first that it is clearly additive. Using distributivity, the multiplicativity reduces to checking that $\varphi(i^2) = \varphi(-1)$. In other words, $(1 + x)^2 = -1 = 1$ in $\mathbb{Z}/2[x]/(x^2)$, which is true (more precisely, $(1 + x)^2 + (x)^2 = -\overline{1} + (x^2) = 1 + (x^2)$). We claim that the kernel of φ is (2). This is clear because $\overline{a} + \overline{b}(1 + x) = 0$ if and only if $\overline{a} = \overline{b} = 0$ in $\mathbb{Z}/2$, i.e., $a, b \in 2\mathbb{Z}$ and equivalently $a + bi \in (2)$. Now, $(\mathbb{Z}/2)[x]/(x^2)$ is not a field as the element x is nilpotent.

Remark: The map here can also be thought of as being obtained from the evaluation homomorphism $\mathrm{ev}_{1+x}\mathbb{Z}[x] \to (\mathbb{Z}/2)[x]/(x^2)$ sending x to $x + 1$. This homomorphism includes $1 + x^2$ in the kernel so it factors through $\mathbb{Z}[x]/(x^2 + 1) \cong \mathbb{Z}[i]$.

4. Let S be a subset of the nonnegative integers, and let $\mathbb{C}[S]$ be the subset of $\mathbb{C}[X]$ consisting of polynomials $P(X) = \sum_{i=0}^{d} a_i X^i$ such that $a_i = 0$ for $i \notin S$. For which S is $\mathbb{C}[S]$ a subring of $\mathbb{C}[X]$?

   Solution: $\mathbb{C}[S]$ is a subring of $\mathbb{C}[X]$ if and only if S contains zero is closed under addition. Clearly if $\mathbb{C}[S]$ is a subring then it contains 1, so $0 \in S$. Similarly, if a and b are in S and $\mathbb{C}[S]$ is a subring, then x^a and x^b are in $\mathbb{C}[S]$ so x^{a+b} is in $\mathbb{C}[S]$ as well. This implies that $a + b$ lies in S.

   Conversely, one notes that $\mathbb{C}[S]$ is always closed under addition, independently of any conditions on S. Moreover if zero is in S then $1 \in \mathbb{C}[S]$. It thus suffices to show that if S is closed under addition then $\mathbb{C}[S]$ is closed under multiplication; this follows from distributivity.

5. Let F be a field and $f, g \in F[X]$. Prove that there exists $r, q \in F[X]$ such that

$$f = gq + r,$$

   with $\deg r < \deg g$. [This shows that $F[X]$ is a Euclidean domain with Euclidean function $\deg : F[X] \setminus \{0\} \to \mathbb{Z}_{\geq 0}$.]

   Solution: Let $\deg(f) = n$. So

$$f = \sum_{i=0}^{n} a_i X^i,$$

   and $a_n \neq 0$. Similarly, if $\deg g = m$, then

$$g = \sum_{i=0}^{m} b_i X^i,$$

   with $b_m \neq 0$. If $n < m$, we let $q = 0$ and $r = f$, and done.

Otherwise, suppose $n \geq m$, and proceed by induction on n.

We let

$$f_1 = f - a_n b_m^{-1} X^{n-m} g.$$

This is possible since $b_m \neq 0$, and F is a field. Then by construction, the coefficients of X^n cancel out. So $\deg(f_1) < n$.

If $n = m$, then $\deg(f_1) < n = m$. So we can write

$$f = (a_n b_m^{-1} X^{n-m}) g + f_1,$$

and $\deg(f_1) < \deg(f)$. So done. Otherwise, if $n > m$, then as $\deg(f_1) < n$, by induction, we can find r_1, q_1 such that

$$f_1 = g q_1 + r_1,$$

and $\deg(r_1) < \deg g = m$. Then

$$f = a_n b_m^{-1} X^{n-m} g + q_1 g + r_1 = (a_n b_m^{-1} X^{n-m} + q_1) g + r_1.$$

So done.

6. Let R be the ring of continuous functions on the unit interval $[0, 1]$, where addition and multiplication of functions is defined pointwise.

   (i) Show that for any $c \in [0, 1]$, the subset $\{f \in R : f(c) = 0\}$ is a maximal ideal M_c of R.

   (ii) Show that if $b \neq c$, then $M_b \neq M_c$.

   (iii) Show that if M is any maximal ideal of R, then $M = M_c$ for some c.

   (iv) Show that M_c is not generated by the element $f(x) = x - c$ of R. Show further that M_c is not even finitely generated.

   Solution: (i) This subset is the kernel of the homomorphism: $R \to \mathbb{R}$, given by evaluation at c. Since this homomorphism is surjective, we have $R/M_c \cong \mathbb{R}$, so M_c is maximal (since $\mathbb{R}$ is a field.)

   (ii) The function $x - b$ lies in M_b but not M_c.

   (iii) Let M be an ideal of R that is not contained in any M_c. Then for each $c \in [0, 1]$ we have an element f_c of M such that $f_c \notin M_c$. In particular $f_c(c) \neq 0$; since f_c is continuous this means that f_c is nonzero in a neighborhood U_c of c. Since $[0, 1]$ is compact, there exist a finite collection $c_1, \ldots, c_n$ such that $U_{c_1}, \ldots, U_{c_n}$ cover $[0, 1]$. Then $g = f_{c_1}^2 + f_{c_2}^2 + \cdots + f_{c_n}^2$ is an element of M that is strictly positive everywhere on $[0, 1]$, so $\frac{1}{g}$ is continuous on $[0, 1]$ and thus lies in R. In particular g is a unit of R that is contained in M, so M is the unit ideal. Thus any maximal ideal of R is contained in some M_c and therefore equal to that M_c.

   (iv) The function $g(x) = |x - c|^{\frac{1}{2}}$ lies in M_c and is not a multiple of $f(x)$. Indeed, if $g(x) = f(x)h(x)$, then we have $h(x) = |x - c|^{-\frac{1}{2}}$ for $x > c$ and $h(x) = -|x - c|^{-\frac{1}{2}}$ for $x < c$, and this does not extend to a continuous function at $x = c$.

   Further, suppose that $f_1, \ldots, f_n$ generate M_c, and let $g(x) = \max\left(|x - c|, |f_1(x)|, \ldots, |f_n(x)|\right)^{\frac{1}{2}}$. Then for any function h of the form $h_1(x)f_1(x) + \cdots + h_n(x)f_n(x)$ with $h_i \in R$ we have that $\frac{h(x)}{g(x)}$ approaches 0 as x approaches c from the left or right, so that $g(x)$ cannot be in the ideal generated by $f_1, \ldots, f_n$.

7. Let R be a ring, let $f : G \to H$ be a surjective group homomorphism and let $f_* : R[G] \to R[H]$ be the ring homomorphism induced by f. Let $N = \ker(f)$. Show that $\ker(f_*) = (N - 1)$, i.e. the ideal generated by the set $N - 1 = \{x - 1 : x \in N\} \subseteq R[G]$. [Hint: Start by considering the case where H is the trivial group and $f_* : R[G] \to R$.]

   Solution: Since $f_*(n-1) = f_*(n) - 1 = f(n) - 1 = 1 - 1 = 0$, we must have $N - 1 \subseteq \ker(f)$. Since $\ker(f)$ is an ideal, we also have $(N - 1) = R[G] \cdot N \subseteq \ker(f)$.

   We now claim that $(N - 1) = \ker(f)$. Suppose $r \in \ker(f)$. Write $r = \sum_{i=1}^{n} a_i g_i$ for some $a_i \in R$ and $g_i \in G$ distinct. Note that $f(r) = \sum_{i=1}^{n} a_i f(g_i) = 0 \in R[H]$. Let $\{f(g_1), \cdots, f(g_n)\} = \{h_1, \cdots, h_m\}$ for $h_i \in H$ distinct. Pick $\widetilde{h}_i \in G$ such that $f(\widetilde{h}_i) = h_i$. Then we have:

$$f(r) = \sum_{i=1}^{n} a_i f(g_i) = \sum_{i=1}^{m} \left(\sum_{g_j \in \widetilde{h}_i N} a_j \right) h_i.$$

   In particular, since $f(r) = 0$ and the h_i are distinct, this implies that $\sum_{g_j \in \widetilde{h}_i N} a_j = 0$ for all $1 \le i \le m$. For each $g_j \in \widetilde{h}_i N$, we can write $g_j = \widetilde{h}_i n_j$ for some $n_j \in N$. Hence we have:

$$r = \sum_{i=1}^{n} a_i g_i = \sum_{i=1}^{m} \left(\sum_{g_j \in \widetilde{h}_i N} a_j \right) g_j = \sum_{i=1}^{m} \left(\sum_{g_j \in \widetilde{h}_i N} a_j \right) \widetilde{h}_i (n_j - 1) \in (N - 1).$$

8. For each commutative ring R and ideal $I \subseteq R$ below, determine (with proof) whether or not I is prime and whether or not I is maximal. [You may assume any results from the course.]

   (i) $R = \mathbb{Z}$, $I = (6)$.

   (ii) $R = \mathbb{Z}$, $I = (8, 12)$.

   (iii) $R = \mathbb{Z}[X]$, $I = (X + 1)$.

   (iv) $R = \mathbb{R}[X]$, $I = (X^2 - 5)$.

   (v) $R = \mathbb{C}[X]$, $I = (X^2 + 3, X^3 - 1)$.

   (vi) $R = (\mathbb{Z}/13\mathbb{Z})[X]$, $I = (X^2 + 1)$.

   (vii) $R = \mathbb{Q}[X, Y, Z]$, $I = (X - Y^2)$.

   Solution: (i) Not prime or maximal since 6 is composite, so $\mathbb{Z}/6\mathbb{Z}$ has zero divisors ($\overline{2} \cdot \overline{3} = 0$).

   (ii) The ideal so generated is (4), and as in (a), this is not prime (or maximal): $4 = 2 \cdot 2$.

   (iii) This is prime, since $\mathbb{Z}[x]/(x + 1) \cong \mathbb{Z}$ (after all $(x + 1)$ is the kernel of the evaluation at -1 homomorphism $\mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}$), and $\mathbb{Z}$ is an integral domain. But it is not maximal since $\mathbb{Z}$ is not a field.

   (iv) This is not prime (or maximal) since $x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$ in $\mathbb{R}[x]$ so $x^2 - 5$ is not irreducible (hence there are zero divisors in $\mathbb{R}[x]/(x^2 - 5)$.

   (v) The ideal is the unit ideal, since $x^2 + 3$ and $x^3 - 1$ have no common roots. The unit ideal however is not prime or maximal (by definition).

   (vi) This is not prime (or maximal) since $x^2 + 1 = (x - 5)(x + 5)$ (as $-\overline{25} = \overline{1}$ modulo 13), so the quotient R/I has zero divisors.

   (vii) This is prime (since $X - Y^2$ is obviously irreducible as it is degree one in X, and $\mathbb{Q}[X, Y, Z]$ is a UFD hence every irreducible is prime and therefore generates a prime ideal). It is not maximal though since it is properly contained in (X, Y, Z) which is maximal.

For a more elementary solution, let $\psi : \mathbb{Q}[X,Y,Z] \twoheadrightarrow \mathbb{Q}[Y,Z]$ be the map sending $X \mapsto Y^2$. We claim that $\ker(\psi) = (X - Y^2)$. Since $\mathbb{Q}[Y,Z]$ is an integral domain but not a field, this would imply that $(X - Y^2)$ is prime but not maximal. To show this, first note that $f(X - Y^2) = 0$ and so $(X - Y^2) \subseteq \ker(\psi)$. In the other direction, we would like to use the Euclidean algorithm. However, $\mathbb{Q}[X,Y,Z]$ is not even a principal ideal domain (this is a good exercise). However, it is possible to show that every $f \in \mathbb{Q}[X,Y,Z]$ can be written in the form $f = q(X - Y^2) + r$ for some $q, r \in \mathbb{Q}[Y,Z]$ by explicit long division. If $f \in \ker(\psi)$, then $r = 0$ and so $f = q(X - Y^2) \in \ker(\psi)$ as required.

9. (i) Show that every finite integral domain is a field.

   (ii) Let R be a commutative ring. Show that an ideal $I \subseteq R$ is prime if and only if R/I is an integral domain. Deduce that every maximal ideal is a prime ideal.

Solution: (i) Let $a \in R$ be non-zero, and consider the ring homomorphism

$$a \cdot - : R \to R, \quad b \mapsto a \cdot b$$

We want to show this is injective. For this, it suffices to show the kernel is trivial. If $r \in \ker(a \cdot -)$, then $a \cdot r = 0$. So $r = 0$ since R is an integral domain. So the kernel is trivial.

Since R is finite, $a \cdot -$ must also be surjective. In particular, there is an element $b \in R$ such that $a \cdot b = 1_R$. So a has an inverse. Since a was arbitrary, R is a field.

(ii) Let I be prime. Let $a + I, b + I \in R/I$, and suppose $(a + I)(b + I) = 0_{R/I}$. By definition, $(a + I)(b + I) = ab + I$. So we must have $ab \in I$. As I is prime, either $a \in I$ or $b \in I$. So $a + I = 0_{R/I}$ or $b + I = 0_{R/I}$. So R/I is an integral domain.

Conversely, suppose R/I is an integral domain. Let $a, b \in R$ be such that $ab \in I$. Then $(a + I)(b + I) = ab + I = 0_{R/I} \in R/I$. Since R/I is an integral domain, either $a + I = 0_{R/I}$ or $b + I = 0_{R/i}$, i.e. $a \in I$ or $b \in I$. So I is a prime ideal.

Finally note that $I \subseteq R$ is maximal implies R/I is a field implies R/I is an integral domain implies I is prime.

10. Show that $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{2}]$ are Euclidean domains.

Solution: $\mathbb{Z}[\sqrt{-2}]$: We claim that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain with function $\phi(z) = |z|^2$. First note that $\phi(zw) \geq \phi(z)$ for all $w \neq 0$. Now observe that $\mathbb{Z}[\sqrt{-2}] \subseteq \mathbb{C}$ splits $\mathbb{C}$ into a lattice of $1 \times \sqrt{2}$ squares which have diagonal length $\sqrt{1^2 + (\sqrt{2})^2} = \sqrt{3}$. Hence, for all $z \in \mathbb{C}$, there exists $q \in \mathbb{Z}[\sqrt{-2}]$ such that $|z - q| \leq \sqrt{3}/2 < 1$.

Given $a, b \in \mathbb{Z}[\sqrt{-2}]$ with $b \neq 0$, taking $z = a/b$ in the above implies that there exists $q \in \mathbb{Z}[\sqrt{-3}]$ such that $|a/b - q| < 1$, i.e. that $|a - bq|^2 < |b|^2$. Let $r = a - bq \in \mathbb{Z}[\sqrt{-2}]$. Then $a = bq + r$ and $\phi(r) < \phi(b)$ as required.

$\mathbb{Z}[\sqrt{2}]$: We claim that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain with function $\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_{\geq 0}$, $a + b\sqrt{2} \mapsto |a^2 - 2b^2|$. Since $\phi(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2})$, it follows that ϕ is multiplicative and so satisfies $\phi(zw) \geq \phi(z)$ for $w \neq 0$.

The proof is now identical to the case $\mathbb{Z}[\sqrt{-2}]$ except that we use that $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt{2}]$ (which is a field) and we draw elements $a + b\sqrt{2}$ as coordinates (a, b).

$^+$11. Show that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a principal ideal domain but not a Euclidean domain.

Solution not provided. You may continue to work on this throughout the term and contact me to discuss ideas and/or hand in a solution. Remember that this problem is optional and may be significantly more challenging than the other problems.