1. Consider the veracity or falsehood of each of the following statements. For bonus, argue for those that you believe are true while providing a counterexample for those that you believe are false.

(1) Every non-constant complex polynomial has a complex root.

(2) Conjugation of complex numbers is a field automorphism of the complex numbers.

(3) Let $x, y \in R$, a finite ring. If $x * y = 1$, then $y * x = 1$ also.

(4) There are exactly four quadratics in $\mathbb{Z}_2[x]$.

(5) If $p(x)$ is a real polynomial, then it either has a real root or there is a quadratic polynomial with real coefficients that divides it.

Solution.

(1) True.
This follows from the Fundamental Theorem of Algebra.

(2) True.
Proof. Let $\overline{a}$ denote the conjugate of the complex number a. We now want to show that

$$f : \mathbb{C} \to \mathbb{C},\ c \mapsto \overline{c}$$

is a ring isomorphism. Let a_1 and a_2 be complex numbers. Since $\overline{a_1 a_2} = \overline{a_1} \cdot \overline{a_2}$, and $\overline{a_1 + a_2} = \overline{a_1} + \overline{a_2}$, it follows that

$$f(a_1 a_2) = f(a_1) f(a_2) \text{ and } f(a_1 + a_2) = f(a_1) + f(a_2),$$

so that f is an homomorpshim. It now remains to show that f is a bijection. The map f must be surjective because $f(\overline{a_1}) = a_1$. Also if $f(a_1) = f(a_2)$, then the real parts of a_1 and a_2 must be equal. Similarly, their imaginary parts must be equal, so that $a_1 = a_2$. That is f is injective and we can conclude that it is a bijection. Thus f is a field automorphism. $\square$

(3) True.
Proof. Let R be a finite ring, and consider $x, y \in R$ such that $x * y = 1$. The map $f : R \to R$, $r \mapsto r * x$ is bijective because for $r_1, r_2 \in R$ with $f(r_1) = f(r_2)$, we have that $r_1 * x = r_2 * x$. We then cancel x on both sides by multiplying each side on the right by y to get $r_1 = r_2$; thus f is injective, and since R is finite, we can conclude that f is also bijective. Thus there exists $r_3 \in R$ such that $r_3 * x = 1$. Mutltiply the preceding equality on the right by y to get $r_3 = y$. $\square$

(4) False.
There are exactly 8 quadratics in $\mathbb{Z}_2[x]$, and they are

$$0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1.$$

(5) If $p(x)$ is 0, then it is trivially true. However, if $p(x)$ is a constant non-zero polynomial then it is not true. We shall now show that the statement is true if $p(x)$ is a non-constant real polynomial.
Proof. Consider the polynomial

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

where each $a_i \in \mathbb{R}$, $a_n \neq 0$, and $n \geq 1$. By the Fundamental Theorem of Algebra, $p(x)$ has a root λ. If λ is real, then we are done. So assume that λ is a non-real complex number. Observe that the conjugate of λ, $\overline{\lambda}$, is also a root of $p(x)$ since

$$\begin{aligned}
p(\overline{\lambda}) &= a_n \overline{\lambda}^n + a_{n-1} \overline{\lambda}^{n-1} + \cdots + a_0 \\
&= a_n \overline{\lambda^n} + a_{n-1} \overline{\lambda^{n-1}} + \cdots + a_0 \\
&= \overline{a_n}\,\overline{\lambda^n} + \overline{a_{n-1}}\,\overline{\lambda^{n-1}} + \cdots + \overline{a_0} && [\overline{a} = a \ \forall a \in \mathbb{R}] \\
&= \overline{a_n \lambda^n} + \overline{a_{n-1} \lambda^{n-1}} + \cdots + \overline{a_0} \\
&= \overline{a_n \lambda^n + a_{n-1} \lambda^{n-1} + \cdots + a_0} \\
&= \overline{0} = 0. && [p(\lambda) = 0]
\end{aligned}$$

Since λ is not real, we must have that $\lambda \neq \overline{\lambda}$. Thus the quadratic polynomial $(x-\lambda)(x-\overline{\lambda})$ divides $p(x)$. To complete the proof, we must show that this quadratic polynomial has real coefficients. Now we have that

$$(x-\lambda)(x-\overline{\lambda}) = x^2 - (\lambda + \overline{\lambda})x + \lambda\overline{\lambda} = x^2 - 2 \cdot \mathrm{Re}(\lambda)x + |\lambda|^2,$$

where $\mathrm{Re}(c)$ and $|c|$ denote the real part and magnitude of a complex number c. Thus the quadratic polynomial $(x-\lambda)(x-\overline{\lambda})$ has real coefficients. $\square$

2. **On Complex & Real**.

(1) Find a ring isomorphism (it has to be both additive and multiplicative) between $\mathbb{C}$ and the subring $\mathcal{C} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\} \subseteq \mathcal{M}_2(\mathbb{R})$.

(2) In the notes we gave two descriptions of the quaternions:

$$\mathcal{Q} = \left\{ \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\} \text{ and } \mathcal{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C} \right\}.$$

Find an isomorphism between these two rings (it has to be both additive and multiplicative).

Solution.

(1) We claim that the map

$$f : \mathcal{C} \to \mathbb{C}, \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi$$

is a ring isomorphism.

Proof. Let $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in \mathcal{C}$, so that

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= f\left(\begin{pmatrix} ac-bd & ad+bc \\ -(ac+bd) & ac-bd \end{pmatrix}\right) \\ &= (ac-bd) + (ad+bc)i \\ &= (a+bi)(c+di) \\ &= f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) \end{aligned}$$

and

$$\begin{aligned} f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}+\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= f\left(\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}\right) \\ &= (a+c) + (b+d)i \\ &= (a+bi) + (c+di) \\ &= f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) + f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right). \end{aligned}$$

Hence f is a ring homomorphism. It is clear that f is surjective since if $a_1 + b_1 i \in \mathbb{C}$, then we must have that $f\left(\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}\right) = a_1 + b_1 i$. Now suppose that

$$f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = f\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right).$$

Then we must have that $a + bi = c + di$ so that $a = b$ and $c = d$. That is, f is injective. We can now conclude that f is a ring isomorphism. $\square$

3. Let F be a field and consider the set R of all matrices of the form $\begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}$ where $a, b \in F$. Do the following:

(1) Show R is closed under addition, subtraction and multiplication so it is a subring of $\mathcal{M}_2(F)$, the 2×2 matrices with entries in F.

(2) Find a positive integer n so that if we let the field $F = \mathbb{Z}_n$, then R will be an integral domain.

(3) Find a positive integer n so that if we let the field $F = \mathbb{Z}_n$, then R will **NOT** be an integral domain.

4. Find a positive integer n so that if we let the field $F = \mathbb{Z}_n$, then R will be a field.
5. In any one of the situations 2, 3, or 4, find a unit of order bigger than 2. Just do one.
6. Suppose now that instead of F, we take $a, b \in \mathbb{Z}$, the integers. Prove it is an integral domain.

Bonus. Find $G(R)$, the group of units, in the case when the entries are integers (last situation), and find all elements of finite order in that group.

Solution.

1. **Proof.** Let $A = \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}, B = \begin{pmatrix} c & d \\ -d & c-d \end{pmatrix} \in R$. Then we have that

$$A + B = \begin{pmatrix} a+c & b+d \\ -(b+d) & (a+c)-(b+d) \end{pmatrix}$$
$$AB = \begin{pmatrix} ac-bd & ad+bc-bd \\ -(ad+bc-bd) & ac-ad-bc \end{pmatrix}, \text{ and}$$
$$-A = \begin{pmatrix} -a & -b \\ b & b-a \end{pmatrix},$$

so that R is closed under addition, multiplication, and negation. The set R clearly contains the identity (by letting $a = 1$ and $b = 0$). Thus R is a subring of $\mathcal{M}_2(F)$. Note that R is also closed under subtraction since it is closed under addition and negation. □

2. Claim that R is an integral domain if $F = \mathbb{Z}_2$.
Proof. Suppose that $AB = 0$ where

$$A = \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix} \text{ and } B = \begin{pmatrix} c & d \\ -d & c-d \end{pmatrix} \in R.$$

Then we must have that $\det(A)\det(B) = 0$. Since F is an integral domain, we can assume without loss that $\det(A) = 0$. That is, $a^2 + b^2 - ab = 0$. Since $F = \mathbb{Z}_2$, we observe that of the four choices for a and b, $\det(A) = 0$ if and only if $a = b = 0$ if and only if $A = 0$. Thus R is an integral domain if $F = \mathbb{Z}_2$. □

3. Now let $F = \mathbb{Z}_3$. Notice that although

$$\begin{pmatrix} 1 & 2 \\ -2 & -1 \end{pmatrix} \neq 0, \text{ we have that } \begin{pmatrix} 1 & 2 \\ -2 & -1 \end{pmatrix}^2 = 0,$$

so that R is not an integral domain if $F = \mathbb{Z}_3$.

4. Let $F = \mathbb{Z}_2$. Then the elements of R are

$$A = 0, B = 1, C = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and } D = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

By inspection we can see that R is commutative under multiplication. Also we have that $B^{-1} = B$, $C^{-1} = D$, so that R is a field if $F = \mathbb{Z}_2$.

(5) From (4), we have that $|C| = 3$.

(6) We shall follow the same line of thought as we did in (2). So to show that R is an integral domain, it suffices to show that the equation $a^2 + b^2 - ab = 0$ has only the trivial solution in $\mathbb{Z}$. Since

$$a^2 + b^2 - ab = \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4},$$

it is clear that $a^2 + b^2 - ab$ is positive if a or b is nonzero; hence we must have that $a = b = 0$, so that R is an integral domain.

4. Consider the set R of matrices of the form $\frac{1}{2}\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$, $a, b \in \mathbb{Z}, a \equiv b \bmod 2$.

(1) Show $I_2 \in R$.

(2) Show R is closed under addition, negation and multiplication so it is a subring of $\mathcal{M}_2(\mathbb{Q})$.

(3) Compute the characteristic polynomial of any such matrix, and observe it is monic with integer coefficients.

(4) Show there are infinitely many units in R.

Bonus. Find $\mathbb{I}(R)$, the group of units of R.

Solution.

(1) Setting $a = 2$ and $b = 0$ will show us that R has the identity.

(2) Let $A = \frac{1}{2}\begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$ and $B = \frac{1}{2}\begin{pmatrix} c & d \\ 5d & c \end{pmatrix} \in R$. Then it follows that

$$A + B = \frac{1}{2}\begin{pmatrix} a + c & b + d \\ 5(b + d) & a + c \end{pmatrix}$$

$$AB = \frac{1}{2}\begin{pmatrix} \dfrac{ac + 5bd}{2} & \dfrac{ad + bc}{2} \\[2ex] 5\dfrac{ad + bc}{2} & \dfrac{ac + 5bd}{2} \end{pmatrix}, \text{ and}$$

$$-A = \frac{1}{2}\begin{pmatrix} -a & -b \\ -5b & -a \end{pmatrix}.$$

By membership in R, we must have that $a \equiv b \bmod 2$ and $c \equiv d \bmod 2$. Thus $a + c \equiv b + d \bmod 2$. Also ac and bd must have the same parity, and so must ad and bc. This says that $ac + 5bd$ and $ad + bc$ are both even. Thus we must have that

$$\frac{ac + 5bd}{2} \equiv \frac{ad + bc}{2} \bmod 2.$$