Math 341 - Solutions #1

1. a. \( z = a + bi \neq 0 \) so either \( a \neq 0 \) or \( b \neq 0 \) (or both \( \neq 0 \)). We want to find \( w = c + di \) s.t. \( z \cdot w = (ac - bd) + (bc + ad)i = 1 \).
   This yields the following equations:
   
   1. \( ac - bd = 1 \)
   2. \( bc + ad = 0 \)

   By the second equation, assuming for now that \( a \neq 0 \), we have \( d = -\frac{bc}{a} \). Substituting into the first equation we find

   \[
   \frac{ac + b^2c}{a} = 1 \quad \text{or} \quad \frac{a^2c + b^2c}{a} = c(a^2 + b^2).
   \]

   So since we know \( a^2 + b^2 > 0 \) we have that

   \[
   c = \frac{a}{a^2 + b^2}, \quad d = -\frac{b}{a^2 + b^2}, \quad w = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.
   \]

   Although we assumed earlier that \( a \neq 0 \) we see that these real numbers are defined so long as \( a^2 + b^2 \neq 0 \), which it can not be since at least one of \( a, b \) are non-zero.

b. \( z = a + bi \neq 0 \). As stated in the problem if \( \bar{z} = a - bi \), then \( z \cdot \bar{z} = a^2 + b^2 \neq 0 \). Let \( w = \frac{1}{a^2 + b^2} \bar{z} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \).

   Then \( z \cdot w = z \cdot \frac{1}{a^2 + b^2} \bar{z} = 1 \). So \( w \) is the inverse of \( z \).

c. 1. Find solutions to \( z^3 = 1 \) with \( z \in \mathbb{C} \). I will use the statement of DeMoivre's theorem using exponentials, so that \((e^{i\theta})^n = e^{i(n\theta)} \). If we represent \( z = re^{i\theta} \) with \( r > 0 \), \( 0 \leq \theta < 2\pi \) we see that if \( z^3 = r^3e^{i3\theta} = 1 = 1e^{i0} \), then \( r^3 = 1 \) and \( 3\theta = 0 \) (as angles). So \( r = 1 \) and \( \theta = 0, \frac{2\pi}{3}, \frac{4\pi}{3} \).
2. Find solutions to $z^4 = -1$. Again if we represent $z = r e^{i \theta}$
with $r > 0$ and $0 \leq \theta < 2\pi$ then once again we have
$z^4 = r^4 e^{i (4 \theta)} = -1 = 1 e^{i \pi}$. So $r = 1$ and $4 \theta = \pi$
(as angles). So $\theta = \frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}$.

\[ \begin{array}{ccc|ccc}
1 & 2 & 3 & 4 & 5 & 6 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 2 & 3 & 4 & 5 \\
2 & 2 & 3 & 4 & 5 & 6 \\
3 & 3 & 4 & 5 & 6 & 0 \\
4 & 4 & 5 & 6 & 0 & 1 \\
5 & 5 & 6 & 0 & 1 & 2 \\
6 & 6 & 0 & 1 & 2 & 3 \\
\end{array} \]

\[ \begin{array}{ccc|ccc}
1^1 = 1 & 2^{-1} = 4 & 3^{-1} = 5 & 4^{-1} = 2 & 5^{-1} = 3 & 6^{-1} = 6 \\
\hline
1^1 & 2^1 = 2 & 3^1 = 3 & 4^1 = 4 & 5^1 = 5 & 6^1 = 6 \\
\end{array} \]

b. $2 \cdot 2 = 2^2 = 4$
$c. Claim$: If $p$ is an odd prime then exactly half of the non-zero elements of $\mathbb{F}_p$.

**Fact 1**: $x^2 = (-x)^2$ in $\mathbb{F}_p$ and because $p$ is odd $x \neq -x$.

Because of this the map $f : \mathbb{F}_p \to \mathbb{F}_p$ where $f(x) = x^2$ has the property that $\frac{1}{2}$ of the non-zero elements of $\mathbb{F}_p$ are in the image (equal to $f(x)$ for some $x$).

**Fact 2**: Suppose $x^2 = y^2$. Then $x^2 - y^2 = (x-y)(x+y) = 0$. So
$(x-y) = 0$ meaning $x = y$ or $(x+y) = 0$ meaning $x = -y$.

This means $\frac{1}{2}$ of the non-zero elements of $\mathbb{F}_p$
are in the image.
a. Let $\mathbb{F}$ be a field. Then $\mathbb{F}$ is a vector space over itself using addition and scalar multiplication from the field.

I will write vectors as $(a)$ where $a \in \mathbb{F}$ for clarity.

I will use $[.]$ for parentheses when needed.

\textbf{Axioms:} Let $(a), (b), (c) \in \mathbb{V}, a, b \in \mathbb{F}$

- **Associativity of $+$:**
  \[ [(a) + (b)] + (c) = (a + b) + (c) = (a + [b] + c) = (a + [b + c]) \]
  \[ = (a) + ([b] + c) = (a) + ([b] + (c)) \]

- **Commutativity of $+$:**
  \[ (a) + (b) = (a + b) = (b + a) = (b) + (a) \]

- **Existence of a zero vector:**
  Consider the vector $(O)$ where $O$ is the additive identity in $\mathbb{F}$.
  \[ (O) + (a) = (O + a) = (a) \]

- **Existence of additive inverses:**
  Since $a \in \mathbb{F}$ and $\mathbb{F}$ is a field \exists $-a \in \mathbb{F}$ s.t. $a + [-a] = 0$.
  \[ \text{So} \quad (a) + (-a) = (a + [-a]) = (O) \]

- **Associativity of Scalar Mult.:**
  \[ \alpha \cdot \beta \cdot (a) = \alpha \cdot (\beta a) = (\alpha \cdot [\beta a]) = (\alpha \cdot \beta \cdot (a)) \]
  \[ = ([\alpha \cdot \beta] \cdot a) \]

- **Scalar Mult. Identity:**
  \[ 1 \cdot (a) = (1 \cdot a) = (a) \]

- **Distributivity 1:**
  \[ \alpha \cdot [(a) + (b)] = \alpha \cdot (a + b) = \alpha \cdot [a + b] = (\alpha a + \alpha b) = (\alpha a + \alpha b) \]
  \[ = \alpha \cdot (a) + \alpha \cdot (b) \]

- **Distributivity 2:**
  \[ [(\alpha + \beta) \cdot a] = (\alpha + \beta) \cdot a = (\alpha a + \beta a) = (\alpha a) + (\beta a) = \alpha \cdot (a) + \beta \cdot (a) \]

\*$\*$: These inequalities follow because $\mathbb{F}$ is a field.
b. \( \mathbb{F}_p^2 = \{ (a, b) \mid a, b \in \mathbb{F}_p \} \) is a vector space over \( \mathbb{F}_p \).

**Axioms**: Let \((a, b), (c, d), (e, f) \in \mathbb{F}_p^2 ; \quad \alpha, \beta \in \mathbb{F}_p \)

- **Assoc of +**:
  
  \[
  [(a, b) + (c, d)] + (e, f) = (a + c, b + d) + (e, f) = [(a + c) + e, (b + d) + f] = (a + [c + e], b + [d + f])
  \]
  
  \[
  = (a + [c + e], b + [d + f]) = (a, b) + [(c, d) + (e, f)]
  \]

- **Comm of +**:

  \[
  (a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b)
  \]

- **Existence of 0**:

  \[
  (a, b) + (0, 0) = (a + 0, b + 0) = (a, b)
  \]

- **Additive inverses**:

  \[
  (a, b) + (-a, -b) = (a + [-a], b + [-b]) = (0, 0)
  \]

- **Assoc of Scalar multi.**:

  \[
  \alpha \cdot [(p, (a, b))] = \alpha \cdot (pa, pb) = (\alpha [pa], \alpha [pb]) = [\alpha p, \alpha (a, b)] = [\alpha p, (a, b)]
  \]

- **Multiplicative Identity**:

  \[
  1 \cdot (a, b) = (1 \cdot a, 1 \cdot b) = (a, b)
  \]

- **Distributivity 1**:

  \[
  \alpha \cdot [(a, b) + (c, d)] = \alpha \cdot (a + c, b + d) = (\alpha [a + c], \alpha [b + d]) = (\alpha a + \alpha c, \alpha b + \alpha d) = (\alpha a, \alpha b) + (\alpha c, \alpha d)
  \]

- **Distributivity 2**:

  \[
  [(\alpha + \beta) \cdot (a, b)] = [(\alpha + \beta) \cdot a, (\alpha + \beta) \cdot b] = (\alpha a + \beta a, \alpha b + \beta b) = (\alpha a, \alpha b) + (\beta a, \beta b) = \alpha \cdot (a, b) + \beta \cdot (a, b)
  \]

\*: Equal Signs marked by \( \wedge \) hold because \( \mathbb{F}_p \) is a field.

All others hold by the rules of addition and scalar multiplication in \( \mathbb{F}_p^2 \).
\[ \vec{u} = (1, 2) \]

0 \cdot \vec{u} = (0, 0)

1 \cdot \vec{u} = (1, 2)

2 \cdot \vec{u} = (2, 4)

3 \cdot \vec{u} = (3, 6)

4 \cdot \vec{u} = (4, 8)

5 \cdot \vec{u} = (5, 10)

6 \cdot \vec{u} = (6, 12)