Name: Kevin Guillen
Student ID: 1747199

Math 117 - SS2 - HW 1 - August 6th

[1] Confirm that the following form a group. Furthermore, determine which are Abelian.

(a) The cyclic group $\langle g \rangle = \{e, g, g^2, g^3, \ldots, g^{n-1}\}$ of order n is defined to be the collection of powers of g under the restrictions that $g^n = e$ for $e = g^0$ representing the identity element and $g^i = g^j$ if and only if $i = j$.

Proof. Identity: For this e serves as the identity element, and we see that for any $g^j \in \langle g \rangle$ that

$$e + g^j = g^0 + g^j = g^{0+j} = g^j = g^{j+0} = g^j + g^0 = g^j + e$$

Inverses: We see for any $g^j \in \langle g \rangle$ there exists $g^{n-j} \in \langle g \rangle$ such that

$$g^j + g^{n-j} = g^{j+n-j} = g^n = e$$

Associativity: For any $g^i, g^j,$ and $g^k \in \langle g \rangle$, we have,

$$g^i + (g^j + g^k) = g^i + g^{j+k} = g^{i+(j+k)} = g^{(i+j)+k} = g^{i+j} + g^k = (g^i + g^j) + g^k$$

Commutativity: For any $g^i, g^j \in \langle g \rangle$ we see,

$$g^i + g^j = g^{i+j} = g^{j+i} = g^j + g^i$$

Therefore $\langle g \rangle$ is indeed a group and abelian. $\square$

(b) Let $\mathcal{S} = \{a, b\}$ be a collection of two distinct symbols. The *free group* on two generators, denoted by $\text{Free}(\mathcal{S})$, is defined to be the collection of all finite strings that can be formed from the four symbols a, a^{-1}, b, and b^{-1} such that no a appears directly next to an a^{-1} and no b appears directly next to a b^{-1}. This collection comes attached with the operation of concatenation of strings.

Proof. Identity: Since $\text{Free}(\mathcal{S})$ is the collection of all finite strings that can be formed with elements in $\mathcal{S}$. We can take string of length 0 to be our identity e. From here we see for any string $\overline{w} \in \text{Free}(\mathcal{S})$,

$$e + \overline{w} = \overline{w} = \overline{w} + e.$$

Associativity: Let $\overline{w}, \overline{v},$ and $\overline{z}$ be arbitrary strings from $\text{Free}(\mathcal{S})$, we can see,

$$\overline{w} + (\overline{v} + \overline{z}) = \overline{w} + \overline{vz} = \overline{wvz} = \overline{wv} + \overline{z} = (\overline{w} + \overline{v}) + \overline{z}$$

Inverses: Let $\overline{w}$ be a string from $\text{Free}(\mathcal{S})$. The inverse of $\overline{w}$ will simply be the inverse of each character $(a \to a^{-1})$ in reverse order.
$\overline{w}$ is composed of characters, we can write it out as

$$\overline{w} = w_0 w_1 \ldots w_n.$$

Meaning the inverse of $\overline{w}$ will be of the form

$$w_n^{-1}w_{n-1}^{-1}\dots w_0^{-1}.$$

Thus,

$$\begin{aligned}\overline{w}+\overline{w}^{-1} &= w_0w_1\dots w_n + w_n^{-1}w_{n-1}^{-1}\dots w_0^{-1}\\ &= w_0w_1\dots w_nw_n^{-1}w_{n-1}^{-1}\dots w_0^{-1}\\ &= w_0w_1\dots w_{n-1}w_{n-1}^{-1}\dots w_0^{-1}\\ &\vdots\\ &= w_0w_0^{-1}\\ &= e\end{aligned}$$

We know this inverse exists since Free($\mathcal{S}$) is the collection of all finite strings from $\mathcal{S}$ □

[2] Confirm that the following form a field.

(a) Let $\mathbb{Z}/p\mathbb{Z}$ for p a prime represent the collection of equivalence classes formed out of the equivalence relation on $\mathbb{Z}$ where $n \sim m$ if $n \equiv m \pmod p$. Addition and multiplication are defined by:

$$[n]+[m]=[n+m] \quad \text{and} \quad [n]\cdot[m]=[n\cdot m]$$

You may assume that $\mathbb{Z}$ has all the standard properties such as associativity, commutativity, etc...

Proof. We know from class that for any integer n, $\mathbb{Z}/n\mathbb{Z}$ will be a commutative ring. All we need to show now is that, when n is prime, every non-zero element in it will have multiplicative inverses.

By definition a prime number, p, will share no common divisors except 1 with another integer n ($n \neq p$). Thus take any non-zero element $n \in \mathbb{Z}/p\mathbb{Z}$. n represents a congruence class of elements which are by definition not multiples of p. Thus, $\gcd(n,p)=1$.

From here we know from elementary number theory that there exists $u, v \in \mathbb{Z}$ such that

$$u\cdot n + v\cdot p = 1.$$

Bringing this into $\mathbb{Z}/p\mathbb{Z}$ we have

$$\begin{aligned}\overline{u}\cdot\overline{n}+\overline{0} &\equiv \overline{1}\\ \overline{u}\cdot\overline{n} &\equiv \overline{1}\end{aligned}$$

That means for any non-zero $n \in \mathbb{Z}/p\mathbb{Z}$, where p is prime, that there exists a $u \in \mathbb{Z}/p\mathbb{Z}$ such that $\overline{u}\cdot\overline{n}=1$. Which means that every non-zero element has a multiplicative inverse. Thus satisfying the criteria to be a field. □

(b) Consider the collection $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$ that comes attached with the binary operations:

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

$$(a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$$

You may assume that $\mathbb{Q}$ has all of the standard properties of a field.

Proof. Associativity: For any $x, y,\ z \in \mathbb{Q}(\sqrt{2})$ we have,

$$\begin{aligned}
x + (y + z) &= (a_1 + b_1\sqrt{2}) + ((a_2 + b_2\sqrt{2}) + (a_3 + b_3\sqrt{2})) \\
&= (a_1 + b_1\sqrt{2}) + (((a_2 + a_3) + (b_2 + b_3)\sqrt{2})) \\
&= (a_1 + (a_2 + a_3)) + (b_1 + (b_2 + b_3))\sqrt{2} && \text{since } \mathbb{Q} \text{ is associative} \\
&= ((a_1 + a_2) + a_3) + ((b_1 + b_2) + b_3)\sqrt{2} \\
&= ((a_1 + a_2) + (b_1 + b_2)\sqrt{2}) + (a_3 + b_3\sqrt{2}) \\
&= ((a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})) + (a_3 + b_3\sqrt{2}) \\
&= (x + y) + z
\end{aligned}$$

we also have,

$$\begin{aligned}
x \cdot (y \cdot z) &= (a_1 + b_1\sqrt{2}) \cdot ((a_2 + b_2\sqrt{2}) \cdot (a_3 + b_3\sqrt{2})) \\
&= (a_1 + b_1\sqrt{2}) \cdot (((a_2 \cdot a_3) + (b_2 \cdot b_3)\sqrt{2})) \\
&= (a_1 \cdot (a_2 \cdot a_3)) + (b_1 \cdot (b_2 \cdot b_3))\sqrt{2} && \text{since } \mathbb{Q} \text{ is associative} \\
&= ((a_1 \cdot a_2) \cdot a_3) + ((b_1 \cdot b_2) \cdot b_3)\sqrt{2} \\
&= ((a_1 \cdot a_2) + (b_1 \cdot b_2)\sqrt{2}) \cdot (a_3 + b_3\sqrt{2}) \\
&= ((a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2})) \cdot (a_3 + b_3\sqrt{2}) \\
&= (x \cdot y) \cdot z
\end{aligned}$$

Identity element: Let our additive identity be $0 = 0 + 0\sqrt{2}$, we see for any $(a + b\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$

$$\begin{aligned}
0 + (a + b\sqrt{2}) &= (0 + 0\sqrt{2}) + (a + b\sqrt{2}) \\
&= (0 + a) + (0 + b)\sqrt{2} \\
&= a + b\sqrt{2} \\
&= (a + 0) + (b + 0)\sqrt{2} \\
&= (a + b\sqrt{2}) + (0 + 0\sqrt{2}) \\
&= (a + b\sqrt{2}) + 0
\end{aligned}$$

Let our multiplicative identity be $1 = 1 + 1\sqrt{2}$, we see for any $(a + b\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$,

$$\begin{aligned}
1 \cdot (a + b\sqrt{2}) &= (1 + 1\sqrt{2}) \cdot (a + b\sqrt{2}) \\
&= (1 \cdot a) + (1 \cdot b)\sqrt{2} \\
&= a + b\sqrt{2} \\
&= (a \cdot 1) + (b \cdot 1)\sqrt{2} \\
&= (a + b\sqrt{2}) \cdot (1 + 1\sqrt{2}) \\
&= (a + b\sqrt{2}) \cdot 1
\end{aligned}$$

Inverse element: Since $a, b \in \mathbb{Q}$ for $(a+b\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$ The additive inverse for $(a+b\sqrt{2})$ is simply $((-a)+(-b)\sqrt{2}$ where $-a, -b$ are simply the additive inverses for $a, b \in \mathbb{Q}$ since $\mathbb{Q}$ is a field.

$$(a + b\sqrt{2}) + ((-a) + (-b)\sqrt{2}) = (a - a) + (b - b)\sqrt{2} = 0 + 0\sqrt{2} = 0$$

$$((-a) + (-b)\sqrt{2}) + (a + b\sqrt{2}) = (-a + a) + (-b + b)\sqrt{2} = 0 + 0\sqrt{2} = 0$$

The same reasoning applies for multiplicative inverses in that for any element $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ the multiplicative inverse will simply be $a^{-1} + b^{-1}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ where a^{-1} and b^{-1} are simply a and b's multiplicative inverse in $\mathbb{Q}$ respectively.
Commutativity: Let $x, y \in \mathbb{Q}(\sqrt{2})$, we can see under addition that,

$$\begin{aligned}
x + y &= (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) \\
&= (a_1 + a_2) + (b_1 + b_2)\sqrt{2} && \text{elements in } \mathbb{Q} \text{ are commutative} \\
&= (a_2 + a_1) + (b_2 + b_1)\sqrt{2} \\
&= (a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2}) \\
&= y + x
\end{aligned}$$

We also see under multiplication that,

$$\begin{aligned}
x \cdot y &= (a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) \\
&= (a_1 \cdot a_2) + (b_1 \cdot b_2)\sqrt{2} && \text{elements in } \mathbb{Q} \text{ are commutative} \\
&= (a_2 \cdot a_1) + (b_2 \cdot b_1)\sqrt{2} \\
&= (a_2 + b_2\sqrt{2}) \cdot (a_1 + b_1\sqrt{2}) \\
&= y \cdot x
\end{aligned}$$

Distrubitve Property: We see for $x, y,\ z \in \mathbb{Q}(\sqrt{2})$,

$$\begin{aligned}
x \cdot (y+z) &= (a_1 + b_1(\sqrt{2})) \cdot ((a_2 + b_2(\sqrt{2})) + (a_3 + b_3(\sqrt{2}))) \\
&= (a_1 + b_1(\sqrt{2})) \cdot ((a_2 + a_3) + (b_2 + b_3)\sqrt{2}) \\
&= a_1(a_2 + a_3) + b_1(b_2 + b_3)\sqrt{2} && \text{Distrubition holds in } \mathbb{Q} \\
&= (a_1 a_2 + a_1 a_3) + (b_1 b_2 + b_1 b_3)\sqrt{2} \\
&= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2})(a_3 + b_3\sqrt{2}) \\
&= xy + xz
\end{aligned}$$

We can see $\mathbb{Q}(\sqrt{2})$ does indeed form a field. □

[3] The fact that $\mathbb{Z}/p\mathbb{Z}$ (where p is a prime) is a field shows that not quite all the laws of elementary arithmetic hold in fields; in $\mathbb{Z}/2\mathbb{Z}$, for instance, $1+1=0$. Prove that if $\mathbb{F}$ is a field, then either the result of repeatedly adding 1 to itself is always different from 0, or else the first time that it is equal to 0 occurs when the number of summands is a prime. (The *characteristic* of the field $\mathbb{F}$, denoted by $\mathrm{char}(\mathbb{F})$, is defined to be 0 in the first case and the crucial prime in the second.)

Proof. By defintion every field must contain a multiplicative identity 1, and an additive identity 0 such that $1 \neq 0$. If we repeatedly add 1 to itself and never reach 0 then we are done, if not we want to show it will be prime. The reason being is if $\mathrm{char}(\mathbb{F}) = n$, where n is composite. That would mean n has divisors other than 1 and itself, so we can express n as $n = dk$ where $d, k \in \mathbb{Z}$ and $1 < d, k < n$. By defintion of n being the characteristic of the field that means $n \cdot 1 = 0$, but $n = dk$, so therefore $dk \cdot 1 = 0$. But a field has no proper zero divisors as we've shown in class, therefore $d \cdot 1 = 0$ or $k \cdot 1 = 0$ which is a contradiction since n is supposed to be the characteristic of $\mathbb{F}$ and r and s are less than n. Therefore n must be prime if not equal to 0.

□

[4] Let $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$.

(a) If addition and multiplication are defined by:

$$(x, y) + (z, w) = (x + z, y + w) \quad \text{and} \quad (x, y) \cdot (z, w) = (x \cdot z, y \cdot w)$$

does $\mathbb{R}^2$ become a field?

Proof. No. This is because $(1, 0), (0, 1) \in \mathbb{R}^2$, which are non zero but we see their product is the zero element of the field, which can't means it can't be a field since in class we showed a field doesn't have zero divisors.

$$(1, 0) \cdot (0, 1) = (0, 0)$$

□

(b) If addition and multiplication are defined by:

$$(x, y) + (z, w) = (x + z, y + w) \quad \text{and} \quad (x, y) \cdot (z, w) = (x \cdot z - y \cdot w, x \cdot w + y \cdot z)$$

is $\mathbb{R}^2$ a field then?

Proof. Yes this forms a field. For multiplication we see it follows that of values in the $\mathbb{C}$ which we know from class is a field. Since recall,

$$\begin{aligned}(x + iy)(z + iw) &= (xz) + i(xw) + i(yz) - (yw) \\ &= (xz - yw) + i(xw + yz)\end{aligned}$$

In this case those the coeffectients done for the imaginary componenet are is simply the 2nd comonponent in $\mathbb{R}^2$ and the real component of the the complex number lines up with the first comonponent of $\mathbb{R}^2$.

We know $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, we also know $\mathbb{R}$ is an abelian group under addition by definition of being a field. We know from group theory that the direct product of 2 abelian groups is also an abelian group. Therefore $\mathbb{R}^2$ under this defintion of addition and multiplication is indeed a field, more specifically the only way to make $\mathbb{R}^2$ into a field.

□

[5] Show that for any field $\mathbb{F}$ the set $\mathbb{F}^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{F}\}$ forms a vector space over the field $\mathbb{F}$ where addition of vectors is taken componentwise. If $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ for p a prime, how many vectors are there in $\mathbb{F}^n$?

Proof. To answer the 2nd question. There will be p^n vectors. This is because $\mathbb{Z}/p\mathbb{Z}$ contains p elements, and $\mathbb{F}^n$ are $n-$tuple elements. Meaning each component there are p choices, and there are n components, therefore p^n vectors. □

[6] Consider the $\mathbb{C}$-vector space $\mathbb{C}^3$. For each of the following determine whether the subsets form a vector subspace:

(a) $U_1 = \{(z_1, z_2, z_3) \in \mathbb{C}^3 \mid z_1 \in \mathbb{R}\}$

(b) $U_2 = \{(z_1, z_2, z_3) \in \mathbb{C}^3 \mid z_1 = 0\}$

(c) $U_3 = \{(z_1, z_2, z_3) \in \mathbb{C}^3 \mid z_1 = 0 \text{ or } z_2 = 0\}$

(d) $U_4 = \{(z_1, z_2, z_3) \in \mathbb{C}^3 \mid z_1 + z_2 = 0\}$

(e) $U_5 = \{(z_1, z_2, z_3) \in \mathbb{C}^3 \mid z_1 + z_2 = 1\}$

[7] (a) Under what conditions on the scalar $\xi \in \mathbb{C}$ are the vectors $(1+\xi, 1-\xi)$ and $(1-\xi, 1+\xi)$ in $\mathbb{C}^2$ (over the field $\mathbb{C}$) linearly dependent?

(b) Under what conditions on the scalar $\xi \in \mathbb{R}$ are the vectors $(\xi, 1, 0)$, $(1, \xi, 1)$, and $(0, 1, \xi)$ in $\mathbb{R}^3$ (over the field $\mathbb{R}$) linearly dependent?

(c) What is the answer for (b) for $\mathbb{Q}^3$ (over the field $\mathbb{Q}$) in place of $\mathbb{R}^3$ (over the field $\mathbb{R}$).

[8] For any field $\mathbb{F}$ let $\mathbb{F}[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_0, a_1, \ldots, a_n \in \mathbb{F}\}$ where $x^i = x^j$ if and only if $i = j$.

(a) If the addition of polynomials is given by the standard procedure of combining like powers of x show that $\mathbb{F}[x]$ forms a vector space over $\mathbb{F}$.

(b) A polynomial $p(x) \in \mathbb{F}[x]$ is called *even* if $p(-x) = p(x)$ and *odd* if $p(-x) = -p(x)$ identically in x. Let $\mathcal{E}$ and $\mathcal{O}$ represent the subsets of $\mathbb{F}[x]$ that consist of strictly even and odd polynomials, respectively. Show that $\mathcal{E}$ and $\mathcal{O}$ form vector subspaces of $\mathbb{F}[x]$.

(c) Show that $\mathbb{F}[x] = \mathcal{E} \oplus \mathcal{O}$. You may assume that $\text{char}(\mathbb{F}) \neq 2$.

[9] (a) Show that if both U and W are three-dimensional vector subspaces of a five-dimensional $\mathbb{F}$-vector space V, then U and W are not disjoint.

Proof. Since by defition every vector space contains a zero vector, every subspace of a vector space will contain the zero vector. Which means every subspace therefore contains at least one subspace and that is the subspace containing only the zero vector. Thus if U and W are three-deimensional vector subspaces of a five-dimensional $\mathbb{F}$-vector space V. Since U and W are subspaces of the same vector space V, then they share the same zero vector. Thus,

$$U \cap W \neq \emptyset$$

□

(b) Show that if U and W are finite-dimensional vector subspaces of a $\mathbb{F}$-vector space V, then:

$$\dim(U) + \dim(W) = \dim(U + W) + \dim(U \cap W)$$

This is the analogue of the *Inclusion-Exclusion Principle* for sets adapted to vector spaces. In a certain sense the dimension for vector spaces plays the same role cardinality has with respect to sets.

Proof. U and W are finite dimensional, so we have $\dim(U \cap W) = n$. Meaning our basis can be expressed as the set of vectors

$$\{v_1, v_2, \ldots, v_n\}$$

This set the basis for $U \cap W$. Meaning this set is linearly independent in U and in W. Which means this set of vectors is a subset to the basis for U and W. Giving us the basis for U as,

$$\{v_1, v_2, \ldots, v_n, u_1, \ldots u_i\}$$

And the basis for W as,

$$\{v_1, v_2, \ldots, v_n, w_1, \ldots, w_j\}$$

This implies $\dim(U) = n + i$ and $\dim(W) = n + j$.

Now our goal is to show the union of $\mathcal{B}_U$ and $\mathcal{B}_W$ serves as a basis for $U + W$.

For any $v \in V$ we know this vector is simply $v = u + w$ for $u \in U$ and $w \in W$. We also know u and w can be expressed as a linear combination of the vectors in it's basis for coeffectients in $\mathbb{F}$. Therefore we have,

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \dots \alpha_n v_n + \beta_1 u_1 + \dots \beta_i u_i + \gamma_1 v_1 + \dots \gamma_n v_n + \delta w_1 + \cdots + \delta_j w_j$$

$$v = (\alpha_1 + \gamma_1) v_1 + \cdots + (\alpha_n + \gamma_n) v_n + \beta_1 u_1 + \dots \beta_i u_i + \delta_1 w_1 + \dots \delta_j w_j$$

Therefore the union of $\mathcal{B}_U$ and $\mathcal{B}_W$ spans the whole vector space of $U + W$

Now we want to show these vectors are linearly independent,

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n + \beta_1 u_1 + \dots \beta_i u_i + \delta_1 w_1 + \cdots + \delta_j w_j = 0$$

$$\delta_1 w_1 + \cdots + \delta_j w_j = -(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n + \beta_1 u_1 + \dots \beta_i u_i)$$

Which means $\delta_1 w_1 + \cdots + \delta_j w_j$ is a vector in the span of $\mathcal{B}_U$, therefore $\delta_1 w_1 + \cdots + \delta_j w_j \in U$. Remeber though that $\{w_1, \dots, w_j\}$ is the basis for W, and thus $\delta_1 w_1 + \cdots + \delta_j w_j$ is in W as well, since it is in both W and U it must also be in their intersection. That means our set of vectors $\{v_1, v_2, \dots, v_n\}$ can be used to express $\delta_1 w_1 + \cdots + \delta_j w_j$,

$$\delta_1 w_1 + \cdots + \delta_j w_j = \beta_1 v_1 + \dots \beta_n v_n$$

$$\beta_1 v_1 + \dots \beta_n v_n - (\delta_1 w_1 + \cdots + \delta_j w_j) = 0$$

Recall though the set of vectors $\{v_1, v_2, \dots, v_n, w_1, \dots, w_j\}$ is linearly independent, so the only way to satisfy this is if all δ_i and β_i are equal to 0. The same reasoning applies to

$$\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n + \delta_1 w_1 + \cdots + \delta_j w_j$$

in that all coeffectients will have to be 0 to satisfy the equation. Making the above vectors linearly independent. Therefore,

$$\{v_1, v_2, \dots, v_n, u_1, \dots u_i, w_1, \dots, w_j\}$$

are linearly independent. Meaning it satisfies all the criteria to be a basis for $U + W$.

We see though that $\dim(U + W) = n + i + j$. Recall though that $\dim(U) = n + i$ and $\dim(W) = n + j$ and $\dim(U \cap W) = n$.

$$\dim(U) + \dim(W) = n + i + n + j = 2n + i + j$$

$$\dim(U + W) + \dim(U \cap W) = n + i + j + n = 2n + i + j$$

Therefore $\dim(U) + \dim(W) = \dim(U + W) + \dim(U \cap W)$ as desired.

$\square$

[10] Let V be a finite-dimensional $\mathbb{F}$-vector space with dual V^*. If $y \in V^*$ is non-zero and $\alpha \in \mathbb{F}$ is arbitrary, does there necessarily exist a vector $x \in V$ such that $[x, y] = \alpha$, or equivalently $y(x) = \alpha$?