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 $\mathrm{Free}(\mathcal{S})$, 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 $\mathrm{Free}(\mathcal{S})$ 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 $\overline{w} \in \mathrm{Free}(\mathcal{S})$,

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

Associativity: Let $\overline{w}, \overline{v},$ and $\overline{z}$ be arbitrary strings from $\mathrm{Free}(\mathcal{S})$, 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 $\mathrm{Free}(\mathcal{S})$. 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 $\mathcal{S}$ $\square$

[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...

(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.

[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 char($\mathbb{F}$), is defined to be 0 in the first case and the crucial prime in the second.)

[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?

(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?

[5] Show that for any field $\mathbb{F}$ the set $\mathbb{F}^n = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in \mathbb{F}\}$ 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 $\mathbb{F}^n$?

[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 $\mathbb{F}[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_0, a_1, \dots, a_n \in \mathbb{F}\}$ 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.

(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.

[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 $y(x) = \alpha$?