Problem Set Solutions for

Abstract and Linear Algebra

Nandana Madhukara
nandana.madhukara@gmail.com

Contents

1 Week 1

(1)

- Let the one element be n. If we set $n = 0 = 1$, we get a field.
- We know that for any $a \in \mathbb{F}$
$$0 = 0a = 1a = a.$$
Therefore all elements will be 0 which is impossible for a multi element set. Refer to next part for proof of $0a = 0$.
- We know that
$$0a = (0 + 0)a = 0a + 0a.$$
Therefore $0a$ is the additive identity so it is 0.
- Multiplying both sides by b^{-1} we get
$$abb^{-1} = 0b^{-1} \implies a = 0.$$
We can go through the same argument to prove that b can be 0.
- If we add ab to all the things that we must prove equal, by factoring, we can see that all of them will become 0. Therefore they were equal to start with.

(2) Let us assume that 0^{-1} exists. This would mean
$$0 = 00^{-1} = 1.$$
With the assumption that $0 \neq 1$, we get a contradiction.

(3) If we prove that having zero divisors implies having no inverses, we are done. Another way of saying that a field as zero divisors is that
$$ab = 0$$
for $a, b \neq 0$. The reason this is only true if not all elements have inverses is because if all elements did, we could always multiply both sides by the inverse and we could prove that $a = 0$ or $b = 0$.

(5) The reason for this is because addition and multiplication in fields are commutative so the order in which we field ajoin does not matter.

(6) If such a field $\mathbb{F}$ exists, then it is a field ajoin of $\mathbb{R}$ and some complex number z where $\mathbb{R}(z) \subsetneq \mathbb{C}$. Now whatever we do, i will always be an element of the field or else $\mathbb{F}$ would just be $\mathbb{R}$. Therefore
$$\mathbb{R}(i) \subset \mathbb{F}$$
which means that $\mathbb{F}$ will just be $\mathbb{C}$. Therefore we are done.

Another way of think about this is that complex numbers a two dimensional vector space while real numbers are a one dimensional vector space which means that we cannot have any fields between these or else we would have fractional dimensions.

(7) Assume such a field $\mathbb{F}$ exists. It must contain 0 and 1. However, if it contains 1, it must contain all the integers. If it contains all the integers, it must create all the rationals so we have a contradiction.

(8) The reason for this is because in the set

$$\{1, 2, ..., p-1\}$$

all have multiplicative inverses so we have a multiplicative inverses modulo p.

(9) We start with x. Assume that this is reducible. Then we can write

$$x = q(x)t(x)$$

for some polynomials $q(x), t(x) \in \mathbb{F}_2[x]$. Additionally, we know that all the coefficients of $q(x)$ and $t(x)$ are all 1. Now let the degree of $q(x)$ be n and the degree of $t(x)$ be m. This means that the degree of $q(x)t(x)$ is $n+m$. Since $n+m > 1$, because $q(x)$ and $t(x)$ are non-constant, we have a contradiction. We can extend this argument to find that all polynomials of degree 1 are irreducible.

Now we move on to x^2+x+1. Again we assume that it is reducible We can notice that if $n, m > 1$, the degree of $q(x)t(x)$ will be greater than 2. Therefore $n, m = 1$ which means that $q(x), t(x) = x, x+1$ not necessarily in that order. Therefore we have to consider three cases:

$$q(x)t(x) = x \cdot x = x^2,$$

$$q(x)t(x) = x(x+1) = x^2 + x,$$

and

$$q(x)t(x) = (x+1)(x+1) = x^2 + 2x + 1 = x^2 + 1$$

which all don't work so x^2+x+1 is irreducible

2 Week 2

(1) We must first prove that if $H \leq G$, then $gh^{-1} \in H$ for all $g, h \in H$. Since H is a subgroup, $h \in H$ means that $h^{-1} \in H$. Now because of closure, we can see that $gh^{-1} \in H$.

Next we prove that if $gh^{-1} \in H$ for all $g, h \in H$, H is a subgroup of G. We do this by showing that H satisfies all the group axioms. We know that the identity e is in H since $e = hh^-1 \in H$ for $h \in H$. Now for any $h \in H$,

$$h^{-1} = eh^{-1} \in H.$$

Now the final thing we need is closure: for any$x, y \in H$, since $y^{-1} \in H$,

$$xy = x(y^{-1})^{-1} \in H.$$

(2) The subgroups are

$$\{e\}, \langle\sigma\rangle, \langle\rho\rangle, \langle\rho^2\rangle, \langle\sigma,\rho\rangle, \langle\sigma,\rho^2\rangle, \langle\sigma\rho,\rho\rangle, \langle\sigma\rho^2,\rho\rangle, \langle\sigma\rho,\rho^2\rangle$$

(3) Let us define groups $(H, \cdot)$ and $(G, \star)$. Now for any $h \in H$, we know from the homomorphism property that

$$f(h \cdot e_H) = f(h) = f(h) \star f(e_H)$$

so $f(e_H) = e_G$. Using this fact, we see

$$f(h)^{-1} \star f(h) = e_G = f(e_H) = f(h^{-1}) \star f(h)$$

so $f(h)^{-1} = f(h^{-1})$.

(4) Since G' will be an infinite group, it will never be possible to find a homomorphism between G and G'.

(5) First we prove reflexivity. For a group G, a bijection which satisfies the homomorphism property is when we map each element to itself: for any $g_1, g_2 \in G$,

$$f(g_1 g_2) = g_1 g_2 = f(g_1) f(g_2) = g_1 g_2.$$

Now we go on to symmetry. Let us define groups $(G, \cdot)$ and $(H, \star)$. Let f be the bijection which makes $G \cong H$. We know that for any $g_1, g_2 \in G$,

$$f(g_1 \cdot g_2) = f(g_1) \star f(g_2).$$

Now consider f^{-1}. This is a bijection from $H \to G$ and for any $h_1, h_2 \in H$,

$$f^{-1}(h_1 \star h_2) = f^{-1}(f(f^{-1}(h_1) \cdot f^{-1}(h_2))) = f^{-1}(h_1) \cdot f^{-1}(h_2)$$

so it satisfies the homomorphism property.

Finally we prove transitivity. We define groups $(A, \cdot)$, $(B, \star)$, and $(C, *)$. We must prove that if $A \cong B$ and $B \cong C$, then $A \cong C$. If $A \cong C$, there is a bijection f such that for any $a_1, a_2 \in A$,

$$f(a_1 \cdot a_2) = f(a_1) \star f(a_2)$$

and similarly, if $B \cong C$, there is a bijection g so that for any $b_1, b_2 \in B$,

$$g(b_1 \star b_2) = g(b_1) * g(b_2).$$

Now we can see that the composition $h = g \circ h$ works. First of all it is a bijection. Next, we see that for any $a_1, a_2 \in A$,

$$h(a_1 \cdot a_2) = g(f(a_1 \cdot a_2)) = g(f(a_1) \star f(a_2)) = g(f(a_1)) * g(f(a_2)) = h(a_1) * h(a_2).$$

3 Week 3

(1) Consider the group $G = (\mathbb{Z}/p\mathbb{Z})^\times$ which has order $p - 1$. We also know that for any $a \in G$, if the order of g is n, the cyclic group $|\langle g \rangle| = n$. From Lagrange's theorem, since $\langle g \rangle \leq G$, we know that $n \mid p - 1$. Let $p - 1 = kn$. Therefore

$$a^{p-1} \equiv a^{kn} \equiv 1 \bmod p$$

(2) Consider $G = (\mathbb{Z}/n\mathbb{Z})^\times$ which is a subset of $\mathbb{Z}/n\mathbb{Z}$ in which the elements of the subset are the elements of this field that are relatively prime to n. In other words, $|G|$ is the number of integers less than n that are relatively prime to n. Another name for this idea is $\phi(n)$. Now by Lagrange's Theorem, for any $g \in G$ with an order of N, since $\langle g \rangle$ is a subgroup of G,

$$|g| \mid |G| \implies N \mid \phi(n).$$

If $\phi(n) = kN$ for some integer k, we have

$$a^{\phi(n)} \equiv a^{kN} \equiv 1 \bmod n$$

(3) Let G be a group and $H \leq G$. For all $g \in G$, we have

$$gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg$$

so it is a normal subgroup.

(9) To prove that $aH = bH$ or they are disjoint, we first prove that for $h_1, h_2 \in H$, if $ah_1 = bh_2$, then for any $h \in H$, there exists an $h' \in H$ such that $ah = bh'$. Because H is a group, we can write h as $h = h_1h''$ for $h'' \in H$. Therefore

$$ah = ah_1h'' = bh_2h''.$$

Again because H is a group, we see that $h_2h'' \in H$ which means that we can let h' be h_2h'' so we are done.

4 Week 4

(1) Let $g \in G$ have order m. We must prove that for any $d \mid m$, there exists a $g_1 \in G$ where $g_1 \neq 1$ such that $g_1^d = 1$. We can see that

$$g^m = g^{d' \cdot d} = g^{d'^d} = 1.$$

Because of closure, $g^{d'}$ is an element in G so we are done.

(2) Since we know that the order of G is p, by Cauchy's Theorem, there must be an element of order p. Let this element be g. Therefore $\langle g \rangle = G$ so now the bijection f that satisfies the homomorphism property is the function which maps elements of G based on what power of g they are.

(3) Consider groups $(G_1, \star_1)$ and $(G_2, \star_2)$ with identity elements e_1 and e_2, respectively. First we prove that $G_1 \times G_2$ has an identity element. We see this element is (e_1, e_2) because for $g_1 \in G_1$ and $g_2 \in G_2$,

$$(g_1, g_2)(\star_1, \star_2)(e_1, e_2) = (g_1 \star_1 e_1, g_2 \star_2 e_2) = (g_1, g_2).$$

Now similarly, for element $(g_1, g_2) \in G_1 \times G_2$, its inverse is just (g_1^{-1}, g_2^{-1}). Finally the direct product gets its other group properties, closure and associativity, from the fact that G_1 and G_2 are groups.

(4) Since $p = 2$ is the smallest prime we see that

$$\{a\} \cong \mathbb{Z}/2\mathbb{Z}$$

where $\{a\}$ is our one element abelian group.

(6) We use lemma 4.2. Since $\langle g \rangle$ and H are subgroups of G, we can consider them as our A and B and by this lemma we are done.

(11) Consider $G = (\mathbb{Z}/n\mathbb{Z})^\times$ which is a subset of $\mathbb{Z}/n\mathbb{Z}$ in which the elements of the subset are the elements of this field that are relatively prime to n. In other words, $|G|$ is the number of integers less than n that are relatively prime to n. Another name for this idea is $\phi(n)$. Now by Lagrange's Theorem, for any $g \in G$ with an order of N, since $\langle g \rangle$ is a subgroup of G,

$$|g| \mid |G| \implies N \mid \phi(n).$$

If $\phi(n) = kN$ for some integer k, we have

$$a^{\phi(n)} \equiv a^{kN} \equiv 1 \bmod n$$

5 Week 5

(1)

- We know that
$$0 \cdot \mathbf{v} = (0+0) \cdot \mathbf{v} = 0 \cdot \mathbf{v} + 0 \cdot \mathbf{v}.$$
Therefore $0 \times \mathbf{v} = \mathbf{0}$.
- We know that
$$\mathbf{0} = 0 \cdot \mathbf{v} = (1-1) \cdot \mathbf{v} = 1 \cdot \mathbf{v} + (-1) \cdot \mathbf{v} = \mathbf{v} + (-1) \cdot \mathbf{v}.$$
Therefore $(-1) \cdot \mathbf{v}$ must be the inverse $\mathbf{v}$ so we are done.
- We know that
$$a \cdot \mathbf{0} = a \cdot (\mathbf{0} + \mathbf{0}) = a \cdot \mathbf{0} + a \cdot \mathbf{0}.$$
Therefore $a \cdot \mathbf{0} = \mathbf{0}$.
- If a is 0, we are done. If a is non zero, then we multiply both sides of a^{-1} and we are done

(2) The first property is trivial. Now the other properties follow from the fact that fields are associative and distributive.

(3) We prove that $(\mathbb{R}^n, +)$ is a vector space over $\mathbb{R}$ by checking all the scalar multiplication axioms. (We can prove that $(\mathbb{R}^n, +)$ is a vector space over $\mathbb{Q}$ in the same manner as the proof that follows since this set is a subfield of R). Now let $(x_1, x_2, ..., x_n)$ be an element of $(\mathbb{R}^n, +)$. First,

$$1 \cdot (x_1, x_2, ..., x_n) = (1 \cdot x_1, 1 \cdot x_2, ..., 1 \cdot x_n) = (x_1, x_2, ..., x_n).$$

Next for $a, b \in \mathbb{R}$,

$$a \cdot (b \cdot (x_1, x_2, ..., x_n)) = a \cdot (bx_1, bx_2, ..., bx_n) = (abx_1, abx_2, ..., abx_n) = (ab) \cdot (x_1, x_2, ..., x_n).$$

Now we consider another element of our abelian group $(y_1, y_2, ..., y_n) \in \mathbb{R}^n$ for axiom (3):

$$a \cdot ((x_1, ..., x_n) + (y_1, ..., y_n)) = (ax_1 + ay_1, ..., ax_n + ay_n) = a \cdot (x_1, ..., x_n) + a \cdot (y_1, ..., y_n).$$

Finally,

$$(a+b) \cdot (x_1, ..., x_n) = (ax_1 + bx_1, .., ax_n + bx_n) = a \cdot (x_1, ..., x_n) + b \cdot (x_1, ..., x_n)$$

Now we when try to do $(\mathbb{R}^n, +)$ over $\mathbb{C}$, our scalar multiplication will not preserve closure so $\mathbb{R}^n$ would not be a vector space.

(5) We first start with $\mathbb{F}[x]$. First we see that $(\mathbb{F}[x], +)$ where $+$ is defined naturally, is an abelian group since the coefficients of $\mathbb{F}[x]$ are elements of a field. Also scalar multiplication preserves closure since again the coefficients are elements of a field. Now the rest of the axioms follow like **(3)**.

6 Week 6

(1) We first prove that if $L : V \to W$ is a linear map, then $L(c\mathbf{u} + \mathbf{v}) = cL(\mathbf{u}) + \mathbf{v}$. From the first property of linear transformations we have $L(c\mathbf{u} + \mathbf{v}) = L(c\mathbf{u}) + L(\mathbf{v})$. Now the second property gives us $L(c\mathbf{u}) + L(\mathbf{v}) = cL(\mathbf{u}) + L(\mathbf{v})$.

Now we prove the opposite direction. We know that $L(c\mathbf{u} + \mathbf{v}) = cL(\mathbf{u}) + \mathbf{v}$. Now we must show that this equation implies the two properties of linear transformations. We can easily see this so we are done.

(2) We can prove this very similarly to **(1)** since all vectors in V are linear combinations of the basis vectors.

(4) Let $V_1 = \{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n\}$. Now we must prove that whenever

$$c_1 L(\mathbf{v}_1) + ...c_n L(\mathbf{v}_n) = \mathbf{0},$$

this implies that $c_1, ..., c_n = 0$. We see that

$$c_1 L(\mathbf{v}_1) + ...c_n L(\mathbf{v}_n) = L(c_1\mathbf{v}_1 + ... + c_n\mathbf{v}_n) = \mathbf{0}.$$

Since V_1 is a set of linearly independent vectors, we are done.

(8) If L satisfies homogeneity, then $L(c\mathbf{v}) = cL(\mathbf{v})$. The only function that satisfies this is a linear function, that is a polynomial of degree 1. Therefore this function also satisfies additivity.

7 Week 7

(2) Consider the Cartesian coordinate system. Each vector in $\mathbb{R}^2$ can represented as a point on the plane. This means are two basis vectors are $(0, 1)$ and $(1, 0)$. First we see that $(0, 1)$ goes to

$$(\cos(\theta), -\sin(\theta)) = (\cos(-\theta), \sin(-\theta))$$

which is a θ radian counterclockwise rotation about the origin $(0, 0)$.

For the second basis vector it will go to

$$(\sin(\theta), \cos(\theta)) = \left(\cos\left(\frac{\pi}{2} - \theta\right), \sin\left(\frac{\pi}{2} - \theta\right)\right)$$

which is also a θ radian counterclockwise rotation about the orgin. Therefore the whole linear transformation is a θ radian counterclockwise rotation.

(3)

(i) Let $\mathbf{v} \in V$ where V is some vector space. Being able to think $\mathbf{v}$ as something else is saying that there is an isomorphism between V and the vector space of the other way we think of $\mathbf{v}$.

(4) This transformation T would just be $T : V \to V$ since

$$T(\mathbf{v}) = T\left(\sum_{i=1}^{n} b_i u_i\right) = \sum_{i=1}^{n} b_i T(u_i) = \sum_{i=1}^{n} b_i w_i \in V.$$

Let this new vector we get be $\mathbf{u}$. Now we prove that we cannot get $T(\mathbf{v}') \neq \mathbf{u}$ for any $\mathbf{v}' \in V$ that is not $\mathbf{v}$.

Assume that such a $\mathbf{v}'$ exists. Then if $\mathbf{v}' = \sum_{i=1}^n b_i' u_i$ where $\{b_i\} \neq \{b_i'\}$, through the same process as above we get

$$T(\mathbf{v}') = \sum_{i=1}^n b_i' w_i = \mathbf{u} = T(\mathbf{v}).$$

This means that we can write $\mathbf{u}$ in two different ways through a common basis which is a contradiction because this would contradict the fact that bases are sets of *linearly independent* vectors.

Now this means that T is an injective function which means that it is invertible.

(6) We could express this as

$$\begin{bmatrix} 3 & -5 & 2 \\ -1 & 2 & 2 \\ 2 & -1 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}.$$

Let 3×3 matrix be A, the x, y, and z matrix be $\mathbf{v}$, and the other matrix be $\mathbf{w}$. Now our equation reduces down to

$$A\mathbf{v} = \mathbf{w}$$

where we want to solve for v. Multiplying both sides by A^{-1} gives us

$$A^{-1}A\mathbf{v} = \mathbf{v} = A^{-1}\mathbf{w}.$$

The RHS will result in a 3×1 so we will have unique solutions for x, y, and z.

(10) We can see that

$$\begin{bmatrix} 0 & 1/2 \\ 2 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Since we are raising the matrix to the tenth power, our answer is just the identity matrix.

(11) Let our matrix be a representation of a linear map T. Let the basis of the input vector space be $\{\mathbf{v}_i\}$ and the basis of the output vector space be $\{\mathbf{w}_i\}$. For the sake of contradiction, let us assume that there exists a T^{-1} such that $T(\mathbf{x}) = \mathbf{y}$ iff $T^{-1}(\mathbf{y}) = \mathbf{x}$. We know one element in $\{\mathbf{w}_i\}$ is $\mathbf{0}$ and let $\mathbf{v}_1$ be the basis that maps to this. Therefore $T^{-1}(\mathbf{0}) = \mathbf{v}_1$. However linear maps always map $\mathbf{0}$ to itself since for any linear transformation L, we have $L(\mathbf{0}) = L(\mathbf{0}) + L(\mathbf{0})$. Therefore $\mathbf{v}_1 = \mathbf{0}$. This can not be true since this does not satisfy the linear independence property of bases so we have a contradiction.

8 Week 8

(1) A nice basis for V would be all polynomials of the form

$$\sum_{k=0}^m a_k x^k$$

for some $a_k \in \mathbb{F}$ and $m \leq n$.

(2)

- We see that the set $\bigcup_{n=1}^\infty \mathbb{F}[x]_{\leq n}$ has a polynomial of degree 1, 2, and for any k, it has a polynomial of degree k. By definition this is $\mathbb{F}[x]$ so we are done.

- First we check additivity. For two polynomials $p(x)$ and $q(x)$ let $r(x) = p(x) + q(x)$ so $r(1) = p(1) + q(1)$. Therefore

$$\phi(p(x) + q(x)) = \phi(r(x)) = r(1) = p(1) + q(1) = \phi(p(x)) + \phi(q(x)).$$

Now let

$$p(x) = \sum_{k=0}^{n} a_k x^k.$$

Now we check homogeneity:

$$\phi(cp(x)) = \phi\left(c\sum_{k=0}^{n} a_k x^k\right) = c\sum_{k=0}^{n} a_k = cp(1) = c\phi(p(x))$$

Therefore we are done.

(3) We must show that if a linear combination of all the uncountably many φ_α is $\mathbf{0}$, then all the coefficients are 0. In the linear combination, let the input vector for the functionals be $\mathbf{v} \in V$ where $\mathbf{v}$ is nonzero. Let

$$\mathbf{v} = \sum_{k\in\mathbb{Q}} a_k v_k.$$

Now we can see that

$$\varphi_\alpha(\mathbf{v}) = \sum_{k\in\mathbb{Q}} a_k \varphi_\alpha(v_k) = \sum_{i<\alpha} a_i.$$

Now we assume that the coefficients of the linear combination are nonzero. However since the φ_α's are positive (this is because $\mathbf{v}$ is nonzero) which means that whole linear combination is nonzero. Therfore we have a contradiction so we are done.

(10) Let the origin be the center of our equilateral triangle. Then the vertices are

$$(r, 0)$$

$$(r\cos(2\pi/3), r\cos(2\pi/3)) = \left(-\frac{r}{2}, \frac{r\sqrt{3}}{2}\right)$$

and

$$(r\cos(4\pi/3), r\cos(4\pi/3)) = \left(-\frac{r}{2}, -\frac{r\sqrt{3}}{2}\right)$$

where r is the circumradius of the triangle. Now we find the dual of this triangle. Now let us find the dual of the convex hull

$$S = \left\{(r, 0), \left(-\frac{r}{2}, \frac{r\sqrt{3}}{2}\right), \left(-\frac{r}{2}, -\frac{r\sqrt{3}}{2}\right)\right\}.$$

We are looking for all functionals $\varphi(s) \le 1$ for $s \in S$. We can consider the bases $\{(1,0),(0,1)\}$ of $\mathbb{R}^2$. Let

$$\varphi((1,0)) = a$$

$$\varphi((0,1)) = b.$$

This means that

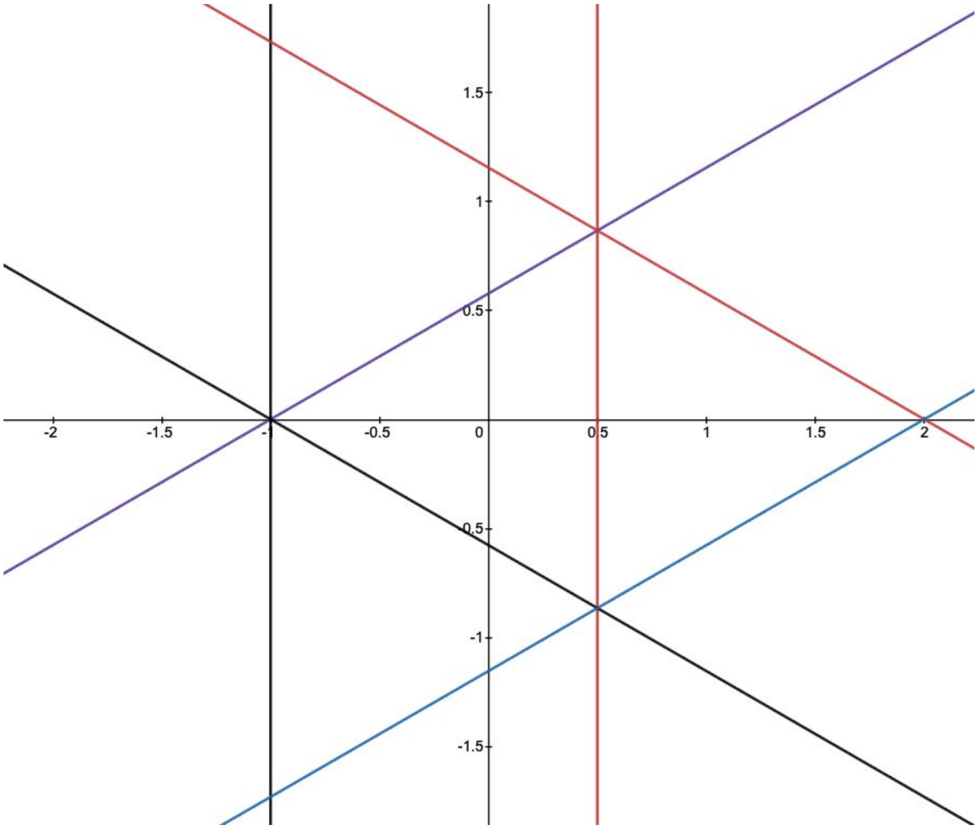
$$\varphi((r,0)) = ar \leq 1.$$

Similarly,

$$\varphi\left(\left(-\frac{r}{2}, \frac{r\sqrt{3}}{2}\right)\right) = -\frac{ar}{2} + \frac{br\sqrt{3}}{2} \leq 1$$

$$\varphi\left(\left(-\frac{r}{2}, -\frac{r\sqrt{3}}{2}\right)\right) = -\frac{ar}{2} - \frac{br\sqrt{3}}{2} \leq 1.$$

We can see that the dual in on the edges of the original equilateral triangle when $r = 2$. (Refer to the image below).



(12) Let us choose the bases $\{(0,0,1),(0,1,0),(1,0,0)\}$. Now all the faces will go to vertices of the dual. These points will be the midpoint of the faces of the cube because of our choice of our bases. Connecting these points gives us an octohedran.

9 Week 9

(1)

- Let $z = a + bi$. Then $\overline{\overline{z}} = \overline{a - bi} = a + bi = z$.
- We have

$$\overline{\sum_{k=1}^{n} z_k} = \overline{\sum_{k=1}^{n} \mathrm{Re}(z_k) + \mathrm{Im}(z_k) \cdot i} = \sum_{k=1}^{n} \mathrm{Re}(z_k) - i \sum_{k=1}^{n} \mathrm{Im}(z_k) = \sum_{k=1}^{n} \overline{z_k}$$

- Let $z = a + bi$ and $w = c + di$. We have $(a - bi)(c - di) = ac - bd - (bc + ad)i = \overline{z \cdot w}$

(2) For fields the inner product is the dot product. However we see for finite fields this does not work so we are done.

(3) We define the inner product as

$$\langle \mathbf{v}, \mathbf{w} \rangle = \langle (v_1, v_2, v_3), (w_1, w_2, w_3) \rangle = v_1 w_1 + v_2 w_2 + v_3 w_3.$$

We can see that the bases $(2, 0, 0)$, $(0, 2, 0)$, $(0, 0, 2)$ is our answer.

(4) We start with the first property. We must prove that

$$a_1 \mathbf{w}_1 + a_2 \mathbf{w}_2 + \cdots + a_k \mathbf{w}_k = \mathbf{0}$$

implies that $a_1, a_2, ..., a_k = 0$. Take some orthonormal vector w_j. Now we take the inner product of both sides of our equation:

$$a_j = \langle \mathbf{0}, \mathbf{w}_j \rangle = \langle \mathbf{w}_j, \mathbf{w}_j \rangle + \langle -\mathbf{w}_j + \mathbf{w}_j \rangle = 1 - 1 = 0.$$

We can do this for any vector in our set so we are done.

(5) The first property follows from the fact that inner products have positive definiteness. For the next property we have

$$\begin{aligned}
\left\| \frac{\mathbf{v}}{\|\mathbf{v}\|} \right\| &= \left\| \frac{1}{\sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}} \cdot \mathbf{v} \right\| \\
&= \sqrt{\left\langle \frac{1}{\sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}} \cdot \mathbf{v}, \frac{1}{\sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}} \cdot \mathbf{v} \right\rangle} \\
&= \sqrt{\frac{1}{\sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}} \cdot \left\langle \mathbf{v}, \frac{1}{\sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}} \cdot \mathbf{v} \right\rangle} \\
&= \sqrt{\frac{1}{\sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}} \cdot \frac{1}{\sqrt{\langle \mathbf{v}, \mathbf{v} \rangle}} \cdot \overline{\langle \mathbf{v}, \mathbf{v} \rangle}} \\
&= \sqrt{\frac{1}{\langle \mathbf{v}, \mathbf{v} \rangle} \cdot \langle \mathbf{v}, \mathbf{v} \rangle} \\
&= 1
\end{aligned}$$

Now for the last property we have

$$\begin{aligned}
\|\alpha \mathbf{v}\| &= \sqrt{\langle \alpha \mathbf{v}, \alpha \mathbf{v} \rangle} \\
&= \sqrt{\alpha \langle \mathbf{v}, \alpha \mathbf{v} \rangle} \\
&= \sqrt{\alpha \cdot \alpha \cdot \overline{\langle \mathbf{v}, \mathbf{v} \rangle}} \\
&= |\alpha| \cdot \|\mathbf{v}\|
\end{aligned}$$

10 Week 10

(5) We do induction on the degree of p. The base case is when the degree is 1. When this happens, $p(x)$ factors as $x - r_1$ so $p(A) = A - r_1 I_n$.

Now we go on to the inductive case. Let $q(x) = (x - r_1)(x - r_2) \cdots (x - r_k)$. Now we assume that

$$q(B) = (B - r_1 I_k) \cdots (B - r_k I_k)$$

for a $k \times k$ matrix B. Now we must prove our claim for a degree $k + 1$ polynomial $p(x) = (x - r_1)(x - r_2) \cdots (x - r_{k+1}) = (x - r_{k+1})q(x)$. Now from Proposition 10.1, we have, for a $k + 1 \times k + 1$ matrix A,

$$p(A) = (A - r_{k+1} I_{k+1})q(A) = (A - r_1 I_{k+1}) \cdots (A - r_{k+1} I_{k+1})$$

so we are done.