MATH 511B, SOLUTIONS 6

1. Since V is finite dimensional, to prove that L^* is invertible it suffices to prove that L^* is injective. If $L^*w = 0$ then

$$\langle v, w\rangle = \langle L(L^{-1}v), w\rangle = \langle L^{-1}v, L^*w\rangle = \langle L^{-1}v, 0\rangle = 0$$

for all $v \in V$; since the pairing is perfect, it follows that $w = 0$, as desired.

If $v, w \in V$ write $v = Lx$ and $w = L^*y$. Then

$$\begin{aligned} \langle L^{-1}v, w\rangle &= \langle x, L^*y\rangle \\ &= \langle Lx, y\rangle \\ &= \langle v, (L^*)^{-1}w\rangle \end{aligned}$$

and therefore $(L^*)^{-1} = (L^{-1})^*$.

2.

(a) For instance, let $||\cdot||$ be the sup norm on $\mathbb{R}^2$, in which $||(x,y)|| = \max(x,y)$. This is easily checked to be a norm, and the vectors $u = (1,0)$ and $v = (0,1)$ do not satisfy the parallelogram law. (In fact, for those of you familiar with ℓ^p- or L^p-spaces, any ℓ^p- or L^p-space with $p \neq 2$ will do. The example above is the ℓ^∞ norm on $\mathbb{R}^2$.)

(b) By the triangle inequality we have

$$||x|| \leq ||x-y|| + ||y||$$

and also

$$||y|| \leq ||y-x|| + ||x|| = ||x-y|| + ||x||$$

from which it follows that

$$|\ ||x|| - ||y||\ | \leq ||x-y||\,.$$

Putting $x = u + c_n v$ and $y = u + cv$ gives

$$|\ ||u + c_n v|| - ||u + cv||| \leq ||(c_n - c)v|| = |c_n - c| \cdot ||v|| \to 0$$

as $n \to \infty$, whence the claim.

3. We define

$$\langle u, v\rangle = \frac{1}{2}(||u+v||^2 - ||u||^2 - ||v||^2)\,.$$

Then $\langle u, v\rangle = \langle v, u\rangle$ and $\langle u, u\rangle = \frac{1}{2}(||2u||^2 - 2||u||^2) = ||u||^2$. From the latter we see

- $\langle u, u\rangle \neq 0$ if $u \neq 0$, so $\langle\ ,\ \rangle$ is definite;
- the norm satisfies $||u|| = \langle u, u\rangle^{1/2}$, so if $\langle\ ,\ \rangle$ is an inner product, then the norm associated to it is indeed $||\cdot||$.

It remains to check that $\langle\ ,\ \rangle$ is bilinear. Since it is symmetric, it suffices to prove that it is bilinear in the second coordinate. Note that

$$\begin{aligned} 2\langle u,v\rangle &= ||u+v||^2-||u||^2-||v||^2 \\ 2\langle u,w\rangle &= ||u+w||^2-||u||^2-||w||^2 \\ 2\langle u,v+w\rangle &= ||u+v+w||^2-||u||^2-||v+w||^2 \end{aligned}$$

and so additivity will follow if we can prove that

$$||u+v||^2+||u+w||^2+||v+w||^2=||u+v+w||^2+||u||^2+||v||^2+||w||^2\,.$$

Applying the parellogram identity to $u+\frac{v+w}{2},\frac{v+w}{2}$ and to $u+\frac{v+w}{2},\frac{v-w}{2}$ gives

$$\begin{aligned} ||u+v+w||^2+||u||^2 &= 2||u+\frac{v+w}{2}||^2+2||\frac{v+w}{2}||^2 \\ ||u+v||^2+||u-w||^2 &= 2||u+\frac{v+w}{2}||^2+2||\frac{v-w}{2}||^2 \end{aligned}$$

Taking the difference of these equations yields

$$||u+v+w||^2+||u||^2+\frac{1}{2}||v-w||^2=||u+v||^2+||u-w||^2+\frac{1}{2}||v+w||^2$$

and adding $\frac{1}{2}||v+w||^2$ to both sides and applying the parallelogram law to v,w gives the desired identity. This proves additivity.

From repeated applications of additivity it follows that

$$\langle u,nv\rangle=n\langle u,v\rangle$$

for any integer n. Then

$$\langle u,\frac{m}{n}v\rangle=m\langle u,\frac{1}{n}v\rangle=\frac{m}{n}(n\langle u,\frac{1}{n}v\rangle)=\frac{m}{n}\langle u,v\rangle$$

so that $\langle u,cv\rangle=c\langle u,v\rangle$ for any rational number c. Let $\{c_n\}$ be a sequence of rational numbers tending to c. From the definition of $\langle\ ,\ \rangle$ we have

$$c_n\langle u,v\rangle=\langle u,c_nv\rangle=\frac{1}{2}(||u+c_nv||^2-||u||^2-c_n^2||v||^2)\,.$$

By 2(a) the right-hand side tends to $\langle u,cv\rangle$ as $n\to\infty$, whereas the left-hand side tends to $c\langle u,v\rangle$. Therefore $c\langle u,v\rangle=\langle u,cv\rangle$ for all real numbers c, and $\langle\ ,\ \rangle$ is bilinear.

4.

(a) Certainly $(x^m)^n=x^{mn}=e$. Moreover, if r is a positive integer less than n then $mr<mn$, and therefore $(x^m)^r=x^{mr}\neq e$.

(b) Let $r=\operatorname{ord}(y)$. Since $y^{kp}=x^k=e$ we see that r is a divisor of kp. On the other hand, $y^r=e$ implies that $y^{rp}=x^r=e$, and therefore r is a multiple of $k=\operatorname{ord}(x)$. Since p is prime, the only (positive) multiples of k that divide kp are k and kp themselves. Write $k=p\ell$. If we had $y^k=e$ then we would have $x^\ell=y^{p\ell}=y^k=e$; but this is a contradiction, since $\ell<k=\operatorname{ord}(x)$. Therefore $y^k\neq e$ and $\operatorname{ord}(y)=kp$.

5. Let G be a cyclic group with generator a, suppose and $H<G$. If H is the trivial subgroup then H is certainly cyclic. Otherwise there exists a smallest positive integer k such that $a^k\in H$, and $\langle a^k\rangle\subset H$. Suppose that $a^\ell\in H$. (Recall

that every element of H has this form since a is a generator of G.) By division we have $\ell = q \cdot k + r$ where the remainder satisfies $0 \leq r < k$. Then $a^\ell = (a^k)^q a^r$, and since H contains both a^ℓ and a^k, it follows that $a^r \in H$. But k was the smallest positive integer such that $a^k \in H$, and since r is smaller than k it cannot be positive; therefore $r = 0$ and k divides ℓ. This proves the reverse inclusion $H \subset \langle a^k \rangle$, and so $H = \langle a^k \rangle$.