Math 430
Dr. Songhao Li
Spring 2016

HOMEWORK 1 SOLUTIONS
Due 2/1/16

1. Let $(V, +, \cdot)$ be a vector space over a field $\mathbb{F}$ and let W be a subspace of V. We define the relation $\sim$ on V as follows: for $v_1, v_2 \in V$, we say $v_1 \sim v_2$ if $v_1 - v_2 \in W$. Prove that $\sim$ is an equivalence relation on V.

Proof. Let $x \in V$. Since W is a subspace of V, and in particular is itself a vector space over $\mathbb{F}$, $0 = x - x \in W$, and so $x \sim x$. If $x, y \in V$ such that $x \sim y$, then $x - y \in W$. Again, since W is a vector space over $\mathbb{F}$, $-1_{\mathbb{F}} \cdot (x - y) = y - x \in W$, and so $y \sim x$. If $x, y, z \in V$ such that $x \sim y$ and $y \sim z$, then $x - y, y - z \in W$. Since W is a vector space, $(x - y) + (y - z) = x - z \in W$, and so $x \sim z$. Therefore, $\sim$ is an equivalence relation on V. ∎

Let V/W be the quotient of V by $\sim$ (as a set). Define an addition operation $\oplus$ and multiplication by elements of $\mathbb{F}$ $\otimes$ by $[x] \oplus [y] = [x + y]$ and $\lambda \otimes [x] = [\lambda \cdot x]$ for all $[x], [y] \in V/W$ and $\lambda \in \mathbb{F}$. Prove that $(V/W, \oplus, \otimes)$ is a vector space over $\mathbb{F}$.

Proof. We first show that $\oplus$ and $\otimes$ are well defined operations. Let $[u], [u'], [v], [v'] \in V/W$ such that $[u] = [u']$ and $[v] = [v']$. Then $u \sim u'$ and $v \sim v'$, and so $u - u', v - v' \in W$. Then, since W is a vector space, $(u+v)-(u'+v') = (u-u')+(v-v') \in W$. Then $u+v \sim u'+v'$, and hence $[u] \oplus [v] = [u+v] = [u'+v'] = [u'] \oplus [v']$. That is, $\oplus$ is well defined on V/W. Let $\lambda \in \mathbb{F}$. As before, since $v \sim v'$, $v - v' \in W$. Then, since W is a vector space over $\mathbb{F}$, $\lambda \cdot v - \lambda \cdot v' = \lambda \cdot (v - v') \in W$. Then $\lambda \cdot v \sim \lambda \cdot v'$, and thus $\lambda \otimes [v] = [\lambda \cdot v] = [\lambda \cdot v'] = \lambda \otimes [v']$. Therefore, $\otimes$ is also well defined on V/W.

We now show that $(V/W, \oplus)$ is a commutative group. Since V is a vector space, $x + y \in V$ for all $x, y \in V$, and so $[x] \oplus [y] = [x + y] \in V/W$ for all $[x], [y] \in V/W$, i.e. $\oplus$ is a binary operation on V/W. Since addition $+$ is associative in V, $\oplus$ is associative in V/W:

$[x] \oplus ([y] \oplus [z]) = [x] \oplus [y + z] = [x + (y + z)] = [(x + y) + z] = [x + y] \oplus [z] = ([x] \oplus [y]) \oplus [z]$.

Similarly, $\oplus$ is commutative since $+$ is commutative: $[x] \oplus [y] = [x + y] = [y + x] = [y] \oplus [x]$.

Direct computation shows that the identity element is $[0]$ and $-[x] = [-x]$ for all $[x] \in V/W$:

$[x] \oplus [0] = [x + 0] = [x]$ and $[x] \oplus [-x] = [x + -x] = [0]$. Again, we are assured that $[0], [-x] \in V/W$ since $(V, +)$ is a group.

Finally, we show that $\otimes$ satisfies the required axioms of scalar multiplication in a vector space. Let $\alpha, \beta \in \mathbb{F}$ and $[x], [y] \in V/W$. Then, since $(V, +, \cdot)$ is a vector space over $\mathbb{F}$, we have
$\alpha \otimes [x] = [\alpha \cdot x] \in V/W$, $\alpha \otimes (\beta \otimes [x]) = \alpha \otimes [\beta \cdot x] = [\alpha \cdot (\beta \cdot x)] = [(\alpha\beta) \cdot x] = (\alpha\beta) \otimes [x]$,
$1_{\mathbb{F}} \otimes [x] = [1_{\mathbb{F}} \cdot x] = [x]$, $\alpha \otimes ([x] \oplus [y]) = \alpha \otimes [x+y] = [\alpha \cdot (x+y)] = [\alpha \cdot x + \alpha \cdot y] = [\alpha \cdot x] \oplus [\alpha \cdot y] = (\alpha \otimes [x]) \oplus (\alpha \otimes [y])$, and $(\alpha + \beta) \otimes [x] = [(\alpha + \beta) \cdot x] = [\alpha \cdot x + \beta \cdot x] = [\alpha \cdot x] \oplus [\beta \cdot x] = (\alpha \otimes [x]) \oplus (\beta \otimes [x])$. Therefore, $(V/W, \oplus, \otimes)$ is a vector space over $\mathbb{F}$. ∎

Suppose that the dimension of V over $\mathbb{F}$ is finite. Prove that $\dim_{\mathbb{F}} V/W = \dim_{\mathbb{F}} V - \dim_{\mathbb{F}} W$.

Proof. If $W = V$, then $V/W = \{[0]\}$ since $x - y \in V = W$, i.e. $x \sim y$, for all $x, y \in V$. In this case, $\dim_{\mathbb{F}} V/W = 0$, $\dim_{\mathbb{F}} V = \dim_{\mathbb{F}} W$, and the given equation holds.

In the case that $W \subsetneq V$, we have $\dim_{\mathbb{F}}/W \leq \dim_{\mathbb{F}} V$; in particular, $\dim_{\mathbb{F}} W$ is finite. Let $\{w_1, \ldots, w_m\}$ be a basis for W, and $\{w_1, \ldots, w_m, v_1, \ldots, v_n\}$ be a basis for V, so that $\dim_{\mathbb{F}} W = m$ and $\dim_{\mathbb{F}} V = m + n$. We will show that $\{[v_1], \ldots, [v_n]\}$ is a basis for V/W. Let $[x] \in V/W$. Then $x \in V$, so
$x = \sum\limits_{i=1}^{m} \lambda_i \cdot w_i + \sum\limits_{j=1}^{n} \sigma_j \cdot v_j$ for some $\lambda_i, \sigma_j \in \mathbb{F}$. Since $w_i - 0 = w_i \in W$, we have $w_i \sim 0$ for each i; in fact, $w \sim 0$ if and only if $w \in W$. Then

$$
\begin{aligned}
&= \left[\sum_{i=1}^{m} \lambda_i \cdot w_i + \sum_{j=1}^{n} \sigma_j \cdot v_j\right] \\
&= \left[\sum_{i=1}^{m} \lambda_i \cdot w_i\right] \oplus \left[\sum_{j=1}^{n} \sigma_j \cdot v_j\right] \\
&= \left(\sum_{i=1}^{m} \lambda_i \otimes [w_i]\right) \oplus \left(\sum_{j=1}^{n} \sigma_j \otimes [v_j]\right) \\
&= \left(\sum_{i=1}^{m} \lambda_i \otimes [0]\right) \oplus \left(\sum_{j=1}^{n} \sigma_j \otimes [v_j]\right) \\
&= [0] \oplus \left(\sum_{j=1}^{n} \sigma_j \otimes [v_j]\right) \\
&= \sum_{j=1}^{n} \sigma_j \otimes [v_j]
\end{aligned}
$$

and thus $\{[v_1], \ldots, [v_n]\}$ spans V/W over $\mathbb{F}$.

Suppose $[0] = \sum_{j=1}^{n} \alpha_j \otimes [v_j]$ for some $\alpha_j \in \mathbb{F}$. Then $\left[\sum_{j=1}^{n} \alpha_j \cdot v_j\right] = \sum_{j=1}^{n} \alpha_j \otimes [v_j] = [0]$, i.e. $\sum_{j=1}^{n} \alpha_j \cdot v_j \sim 0$. Then $\sum_{j=1}^{n} \alpha_j \cdot v_j \in W$, and thus $\sum_{j=1}^{n} \alpha_j \cdot v_j = \sum_{i=1}^{m} \beta_i \cdot w_i$ for some $\beta_i \in \mathbb{F}$. Then $\sum_{j=1}^{n} \alpha_j \cdot v_j + \sum_{i=1}^{m} \text{-}\beta_i \cdot w_i = \sum_{j=1}^{n} \alpha_j \cdot v_j - \sum_{i=1}^{m} \beta_i \cdot w_i = 0$. Since $\{w_1, \ldots, w_m, v_1, \ldots, v_n\}$ is a basis for V, we must then have $\alpha_j = 0 = \beta_i$ for all i and all j. Since each α_j is equal to zero, $\{[v_1], \ldots, [v_n]\}$ is linearly independent, and thus is a basis (a linearly independent spanning set). Therefore, $\dim_{\mathbb{F}} V/W = n = (m+n) - m = \dim_{\mathbb{F}} V - \dim_{\mathbb{F}} W$. ■

Part 1 Section 4 Exercises

29. Show that if G is a finite group with identity e and with an even number of elements, then there exists $a \neq e$ in G such that $a * a = e$.

Proof. First, note that $a * a = e$ if and only if $a = a^{\text{-}1}$. Let $G_1 = G \setminus \{e\}$, and let $x_1 \in G_1$. If $x_1 = x_1^{\text{-}1}$, then we are done. Otherwise, set $G_2 = G_1 \setminus \{x_1, x_1^{\text{-}1}\}$ and let $x_2 \in G_2$. Continuing similarly, we will either find an element x_i such that $x_i = x_i^{\text{-}1}$ or else, since $|G|$ is even, we will arrive at the singleton set G_I, where $I = \frac{|G|}{2}$. Supposing that none of the x_i satisfy $x_i = x_i^{\text{-}1}$, let $G_I = \{a\}$. Since $a \in G$ and G is a group, $a^{\text{-}1} \in G$. However, since $x_i \neq a \neq x_i^{\text{-}1}$ for all i, we have $x_i \neq a^{\text{-}1} \neq x_i^{\text{-}1}$ by the cancellation law. Therefore, since $a \neq e$ implies $a^{\text{-}1} \neq e^{\text{-}1} = e$, we must have $a^{\text{-}1} = a$. ■

32. Show that every group G with identity e and such that $x * x = e$ for all $x \in G$ is abelian.

Proof. Since $x * x = e$, $x = x^{\text{-}1}$ for all $x \in G$. Let $a, b \in G$. Then, by Corollary 4.18,
$a * b = a^{\text{-}1} * b^{\text{-}1} = (b * a)^{\text{-}1} = b * a$. Therefore, $(G, *)$ is commutative. ■

41. Let G be a group and let g be one fixed element of G. Show that the map i_g, such that $i_g(x) = gxg^{\text{-}1}$ for $x \in G$, is an isomorphism of G with itself.

Proof. Suppose $x, y \in G$ such that $i_g(x) = i_g(y)$. Then $gxg^{\text{-}1} = gyg^{\text{-}1}$. By the left cancellation law, we must then have $xg^{\text{-}1} = yg^{\text{-}1}$; the right cancellation law then shows that $x = y$, and so i_g is injective.

Let $t \in G$. Then, since G is a group, $g^{\text{-}1}tg \in G$ and $i_g(g^{\text{-}1}tg) = g(g^{\text{-}1}tg)g^{\text{-}1} = (gg^{\text{-}1})t(gg^{\text{-}1}) = ete = t$, and so i_g is surjective.

Since $i_g(xy) = gxyg^{\text{-}1} = gxeyg^{\text{-}1} = gx(g^{\text{-}1}g)yg^{\text{-}1} = (gxg^{\text{-}1})(gyg^{\text{-}1}) = i_g(x)i_g(y)$, i_g is a group homomorphism. Therefore, i_g is a group isomorphism from G to itself (i.e. i_g is a group automorphism of G). ■

Part 1 Section 5 Exercises

22. Describe all the elements in the cyclic subgroup of $GL(2, \mathbb{R})$ generated by $\begin{bmatrix} 0 & \text{-1} \\ \text{-1} & 0 \end{bmatrix}$.

Solution: Since $\begin{bmatrix} 0 & \text{-1} \\ \text{-1} & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, we have $\left\langle \begin{bmatrix} 0 & \text{-1} \\ \text{-1} & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 0 & \text{-1} \\ \text{-1} & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$

■

43. Show that if H and K are subgroups of an abelian group G, then $\{hk \mid h \in H, k \in K\}$ is also a subgroup of G.

Proof. Let $HK = \{hk \mid h \in H, k \in K\}$; since $e \in H, K$, we must have $e = ee \in HK$. In particular, HK is nonempty. Let $hk, h'k' \in HK$. Then, since G is an abelian group, $(hk)(h'k') = h(kh')k' = h(h'k)k' = (hh')(kk')$. Since $h, h' \in H$ and H is a (sub)group, $hh' \in H$. Similarly, $kk' \in K$. Thus, $(hk)(h'k') = (hh')(kk') \in HK$, and so the induced operation is a binary operation on HK. Since G is abelian, $(hk)^{\text{-}1} = k^{\text{-}1}h^{\text{-}1} = h^{\text{-}1}k^{\text{-}1}$. Since H and K are groups, $h^{\text{-}1} \in H$ and $k^{\text{-}1} \in K$, and so $(hk)^{\text{-}1} = h^{\text{-}1}k^{\text{-}1} \in HK$. Therefore, HK is a subgroup of G. ■

51. Let G be a group and let a be one fixed element of G. Show that $C_G(a) = \{x \in G \mid xa = ax\}$ is a subgroup of G.

Proof. Since $ea = a = ae$, $e \in C_G(a)$; in particular, $C_G(a)$ is nonempty. Let $x, y \in C_G(a)$, so that $xa = ax$ and $ya = ay$. Then, $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$, i.e. $xy \in C_G(a)$, and so the induced operation is a binary operation on $C_G(a)$. Since $xa = ax$, we have
$x^{\text{-}1}a = (x^{\text{-}1}a)e = (x^{\text{-}1}a)(xx^{\text{-}1}) = x^{\text{-}1}(ax)x^{\text{-}1} = x^{\text{-}1}(xa)x^{\text{-}1} = (x^{\text{-}1}x)(ax^{\text{-}1}) = e(ax^{\text{-}1}) = ax^{\text{-}1}$,
i.e. $x^{\text{-}1} \in C_G(a)$. Therefore, $C_G(a)$ is a subgroup of G. ■

52. Generalizing Exercise 51, let S be any subset of a group G.

i) Show that $C_G(S) = \{x \in G \mid xs = sx \ \forall s \in S\}$ is a subgroup of G.

ii) Show that the center of G, denoted $Z(G) = C_G(G)$, is an abelian subgroup of G.

Proof.

i) Let $S \subseteq G$. Since $es = s = se$ for all $s \in S$, $e \in C_G(S)$, and so $C_G(S)$ is nonempty. Let $x, y \in C_G(S)$, and let $s \in S$. Then $xs = sx$ and $ys = sy$. Thus, as in Exercise 51, $(xy)s = s(xy)$. Since $s \in S$ is arbitrary, $xy \in C_G(S)$, and so the induced operation is a binary operation on $C_G(S)$. As in Exercise 51, since $xs = sx$, $x^{-1}s = sx^{-1}$ for all $s \in S$, and so $x^{-1} \in C_G(S)$. Therefore, $C_G(S)$ is a subgroup of G.

ii) All that remains to be shown is commutativity. Let $a, b \in Z(G)$. Then, since $b \in G$ and $a \in Z(G)$, $ab = ba$ by definition of $Z(G) = C_G(G)$. Therefore, $Z(G)$ is an abelian subgroup of G. ■

53. Let H be a subgroup of a group G. For $a, b \in G$, let $a \sim b$ if and only if $ab^{-1} \in H$. Show that $\sim$ is an equivalence relation on G.

Proof. Let $x \in G$. Then, since $H \leq G$, $xx^{-1} = e \in H$, i.e. $x \sim x$. Suppose $y \in G$ such that $x \sim y$. Then $xy^{-1} \in H$. Since H is a subgroup, $yx^{-1} = (xy^{-1})^{-1} \in H$. Then $y \sim x$. Suppose $z \in G$ such that $y \sim z$. Then $xy^{-1}, yz^{-1} \in H$. Since $H \leq G$, H is a group, and so $xz^{-1} = xez^{-1} = x(y^{-1}y)z^{-1} = (xy^{-1})(yz^{-1}) \in H$, and so $x \sim z$. Therefore, $\sim$ is an equivalence relation on G. ■

57. Show that a group with no proper nontrivial subgroups is cyclic.

Proof. We will show the contrapositive. Suppose that G is not cyclic. Then G is not the trivial group, and so there is some $x \neq e$ in G. The, since G is not cyclic, $\{e\} \lneq \langle x \rangle \lneq G$, i.e. $\langle x \rangle$ is a proper nontrivial subgroup of G. ■