Math 306, Spring 2012
Homework 5 Solutions

(1) (a) (3 pts) Find a linearly dependent set of three vectors in $\mathbb{R}^3$, but such that any set of two of them is linearly independent.

(b) (5 pts) Let V be a vector space over $\mathbb{C}$. Suppose that $B = \{v_1, v_2, v_3\}$ is a linearly independent subset of V. Prove that the set $B' = \{v_1 + v_2, v_2 + v_3, v_1 + v_3\}$ is a linearly independent subset of V.

Solution:

(a) Take, for example, $\{(1,0,0),(0,1,0),(1,1,0)\}$

(b) Suppose that there are $c_1, c_2, c_2 \in \mathbb{C}$ such that $c_1(v_1 + v_2) + c_2(v_2 + v_3) + c_3(v_1 + v_3) = 0$. Then $(c_1 + c_3)v_1 + (c_1 + c_2)v_2 + (c_2 + c_3)v_3 = 0$. Since $B = \{v_1, v_2, v_3\}$ is linearly independent, we conclude that $c_1 + c_3 = 0$, $c_1 + c_2 = 0$ and $c_2 + c_3 = 0$. Then we can write

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Since the determinant of this 3×3 matrix is 2, it is invertible, so

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

as required.

(2) (5 pts/part) Let K be a field and let K^n be the vector space of n-tuples over K. For all $j \in \{1, \ldots, n\}$, let

$$e_j = (0, \ldots, 0, 1, 0, \ldots, 0, \ldots, 0),$$

where the 1 occurs in the j-th position. Let $f_j = e_1 + \cdots + e_j$ for all $j \in \{1, \ldots, n\}$.

(a) Prove that $B_1 = \{e_1, e_2, \ldots, e_n\}$ is a basis for K^n.

(b) Prove that $B_2 = \{f_1, f_2, \ldots, f_n\}$ is a basis for K^n.

(Hint: you may assume that the familiar result which says that rows or columns of a square matrix are linearly independent iff matrix is invertible extends to matrices over general fields K.)

Solution:

(a) Suppose that there are $a_1, \ldots, a_n \in K$ such that $a_1e_1 + \cdots + a_ne_n = 0$. Then we have $(a_1, a_2, \ldots, a_n) = 0$, so $a_1 = a_2 = \cdots = a_n = 0$. Hence B_1 is linearly independent. To show that B_1 spans K^n, consider $v \in K^n$. Then $v = (v_1, \ldots, v_n)$ for some $v_i \in K$. Therefore $v = v_1e_1 + \cdots + v_ne_n$.

(b) Suppose that there are $a_1, \ldots, a_n \in K$ such that $a_1f_1 + \cdots + a_nf_n = 0$. Then we have

$$(a_1, a_1 + a_2, \ldots, a_1 + a_2 + \cdots + a_n) = 0.$$

Equivalently we can write

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since the determinant of this $n \times n$ matrix A is 1, it is invertible, so it follows that $a_1 = a_2 = \cdots = a_n = 0$. Hence B_2 is linearly independent. One way to show that B_2 spans K_n is to let $B' = B_2 \cup \{v\}$ for some $v = (v_1, \ldots, v_n) \in K^n$ and find $b_1, \ldots, b_n \in K$ such that $v = b_1f_1 + \cdots + b_nf_n$ (this would show that B_2 is a maximal linearly independent set and hence spans the entire space). Equivalently, we want $b_1, \ldots, b_n \in K$

such that

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

We can solve for such b_i by multiplying each side by A^{-1}. Hence B' is linearly dependent, so B_2 is maximal.

(3) (3 pts/part) Find an infinite linearly independent subset of the following vector spaces. No proof is required.
  (a) $\mathbb{R}$ over $\mathbb{Q}$.
  (b) $K(t)$ over K, where K is a field and t is an indeterminate.
  (c) K^S over K, where K is a field and S is an infinite set.

Solution:
  (a) $B = \{\sqrt{p} \colon p \text{ is prime}\}$
  (b) $B = \{t^n \colon n \in \mathbb{Z}_{\geq 0}\}$
  (c) $B = \{f_t \colon t \in S\}$, where $f_t \colon S \to K$ is defined by

$$f_t(s) = \begin{cases} 0 & \text{if} \quad s \neq t, \\ 1 & \text{if} \quad s = t, \end{cases}$$

for all $s \in S$.

(4) (3 pts/part) Compute the degree $[L\colon K]$ for each of the field extensions below, and exhibit a basis for L as a vector space over K if the degree is finite.
  (a) $\mathbb{Q}(\sqrt[3]{5}) \colon \mathbb{Q}$
  (b) $\mathbb{R}(\sqrt[5]{2}) \colon \mathbb{R}$
  (c) $\mathbb{Q}(e^{2\pi i/5}) \colon \mathbb{Q}$
  (d) $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \colon \mathbb{Q}(\sqrt{3})$
  (e) $\mathbb{C} \colon \mathbb{Q}$

Solution:
  (a) The extension has degree 3 with basis $B = \{1, \sqrt[3]{5}, \sqrt[3]{25}\}$.
  (b) The extension has degree 1 with basis $B = \{1\}$.
  (c) The extension has degree 4 with basis $B = \{1, e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}\}$.
  (d) The extension has degree 2 with basis $B = \{1, \sqrt{5}\}$.
  (e) The extension has infinite degree.

(5) Use the Tower Law for the following.
  (a) (5 pts) Prove that, if $L\colon K$ is a field extension with $[L\colon K] = 1$, then $L = K$. (Hint: Show that $K \subseteq L$ and $L \subseteq K$.)
  Remark: We have already used this result in case of simple extensions $K(\alpha)\colon K$ in class. The proof in that case is that if the degree of this extension is 1, then the degree of the monic minimal polynomial over K for α is 1, i.e. the polynomial must be $x - \alpha$, which means that α is in K.
  (b) (3 pts) If $[L\colon K]$ is a prime integer, prove that there are no intermediate fields M strictly between L and K.

Solution:
  (a) Suppose that $[L\colon K] = 1$. Clearly $K \subseteq L$. Let $B = \{e\}$ be a basis of $L\colon K$. We claim that $e \in K$. Indeed, if $\alpha \in K^*$, then $\alpha \in L$, so there is $\beta \in K$ such that $\alpha = \beta e$. Clearly $\beta \neq 0$, so $e = \alpha/\beta$. Therefore $e \in K$. Now for all $\gamma \in L$, there is $\delta \in K$ such that $\gamma = \delta e$, so $\gamma \in K$. Therefore $L \subseteq K$, as required.
  (b) Let $[L\colon K]$ be prime. Suppose that M is a field with $K \subseteq M \subseteq L$. Then by the Tower Law, we have $[L\colon M] = 1$ or $[M\colon K] = 1$. So $L = M$ or $K = M$, so M is not strictly contained between L and K.

(6) (5 pts/part)
  (a) Prove that $B = \{\sqrt{6}, \sqrt{10}\}$ is a linearly independent subset of $\mathbb{R}$ as a vector space over $\mathbb{Q}$.
  (b) Prove that $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})\colon \mathbb{Q}$ has degree 4 and not 8. Exhibit a basis for this extension.

Solution:
  (a) Suppose that there are $a, b \in \mathbb{Q}$ such that $a\sqrt{6} + b\sqrt{10} = 0$. Suppose that $b \neq 0$. Then $a \neq 0$. Without loss of generality, assume that a and b are coprime integers. Then $6a^2 = 10b^2$, i.e. $3a^2 = 5b^2$. Hence $3|5b^2$, so $3|b$. Hence $9|3a^2$, so $3|a^2$. Therefore $3|a$, a contradiction. Therefore $b = 0$, and so $a = 0$. So $B = \{\sqrt{6}, \sqrt{10}\}$ is a linearly independent subset.
  (b) Since $\sqrt{15} = \frac{\sqrt{60}}{2} \in \mathbb{Q}(\sqrt{6}, \sqrt{10})$, it follows that $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10})$. Clearly

$$[\mathbb{Q}(\sqrt{6}, \sqrt{10})\colon \mathbb{Q}] = 4,$$

so we are done.

(7) (3 pts/part) The following statements are all false. Provide a counterexample or a counterproof. Recall that an extension $L\colon K$ is finite if the degree $[L\colon K]$ is finite.
  (a) Every field extension of $\mathbb{R}$ is a finite extension.
  (b) Every field extension of a finite field is a finite extension.
  (c) There is some element of $\mathbb{C}$ that is transcendental over $\mathbb{R}$.
  (d) If K is a field, then every algebraic extension of K is finite.
  (e) For all $n \in \mathbb{Z}_{\geq 2}$, there are no intermediate fields properly between $\mathbb{Q}(\sqrt[n]{2})$ and $\mathbb{Q}$.

Solution:
  (a) If t is an indeterminate, then $\mathbb{R}(t)$ is an infinite extension of $\mathbb{R}$.
  (b) If t is an indeterminate, then $\mathbb{Z}_2(t)$ is an infinite extension of $\mathbb{Z}_2$.
  (c) Note that $[\mathbb{C}\colon \mathbb{R}] = 2$ which is prime. Hence for any $\alpha \in \mathbb{C}$, we have $[\mathbb{R}(\alpha)\colon \mathbb{R}] = 1$ or 2. Therefore α is algebraic over $\mathbb{R}$.
  (d) The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)\colon \mathbb{Q}$ is algebraic but infinite.
  (e) The field $\mathbb{Q}(\sqrt{2})$ is lies properly between $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}$.

(8) (5 pts/part)
  (a) Suppose that $[L\colon K]$ is a prime number. Prove that $L\colon K$ is a simple extension, i.e. there is $\alpha \in L$ such that $L = K(\alpha)$. (Hint: Look at an earlier problem.)
  (b) Let $L\colon K$ be a finite extension, and let p be an irreducible polynomial in $K[x]$ with $\deg p \geq 2$. Prove by contradiction that, if $\deg p$ and $[L\colon K]$ are coprime, then p has no zeros in L. (Hint: If $\alpha \in L$ is a root of p, then consider the field $K(\alpha)$.)

Solution:
  (a) Suppose that $[L\colon K] = p$ is prime and let $\alpha \in L \backslash K$. Then $[K(\alpha)\colon K]$ divides $[L\colon K]$, so $[K(\alpha)\colon K] = 1$ or p. Since $K(\alpha) \neq K$, it follows that $[K(\alpha)\colon K] = p$ and so $[L\colon K(\alpha)] = 1$. Therefore $L = K(\alpha)$ and L is a simple extension of K.
  (b) Suppose that $\alpha \in L$ is a root of p. Then $[K(\alpha)\colon K]$ divides $[L\colon K]$. But $[K(\alpha)\colon K] = \deg p$, so $\deg p$ divides $[L\colon K]$. Since these numbers are assumed to be coprime, it follows that $\deg p = 1$, a contradiction.

(9) (5 pts/part) We say that a rational number a is a *square* in $\mathbb{Q}$ if there is $b \in \mathbb{Q}$ such that $b^2 = a$. Let $m, n \in \mathbb{Q}$ be non-squares. Prove the following.
  (a) If mn is a square in $\mathbb{Q}$, then $[\mathbb{Q}(\sqrt{m}, \sqrt{n})\colon \mathbb{Q}] = 2$.
  (b) If mn is a non-square in $\mathbb{Q}$, we have $[\mathbb{Q}(\sqrt{m}, \sqrt{n})\colon \mathbb{Q}] = 4$.

Solution:

(a) Suppose that m and n are nonsquares in $\mathbb{Q}$ and suppose that $mn = a^2$ for some $a \in \mathbb{Q}$. Notice that neither m nor n is zero, so we can write $n = \frac{a^2}{m}$, or $\sqrt{n} = \pm\frac{a}{\sqrt{m}}$. Therefore $\sqrt{n} \in \mathbb{Q}(\sqrt{m})$, so

$$[\mathbb{Q}(\sqrt{m}, \sqrt{n})\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt{m})\colon \mathbb{Q}] = 2.$$

(b) Suppose that mn is a nonsquare, and suppose on the contrary that $[\mathbb{Q}(\sqrt{m}, \sqrt{n})\colon \mathbb{Q}] = 2$. Since $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = (\mathbb{Q}(\sqrt{m}))(\sqrt{n})$, it follows that

$$[\mathbb{Q}(\sqrt{m}, \sqrt{n})\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt{m}, \sqrt{n})\colon \mathbb{Q}(\sqrt{m})][\mathbb{Q}(\sqrt{m})\colon \mathbb{Q}].$$

Since $[\mathbb{Q}(\sqrt{m})\colon \mathbb{Q}] = 2$, it follows that $[\mathbb{Q}(\sqrt{m}, \sqrt{n})\colon \mathbb{Q}(\sqrt{m})] = 1$, so $\sqrt{n} \in \mathbb{Q}(\sqrt{m})$, i.e. $\sqrt{n} = a + b\sqrt{m}$ for some $a, b \in \mathbb{Q}$. Therefore $a^2 = (\sqrt{n} - b\sqrt{m})^2 = n + bm^2 - 2b\sqrt{mn}$. Therefore mn is a square in $\mathbb{Q}$, a contradiction.

(10) (5 pts) Suppose that $M\colon L\colon K$ is a tower of field extensions and let $\alpha \in M$ be algebraic over L. Assume that $[K(\alpha)\colon K]$ and $[L\colon K]$ are relatively prime. Prove that the minimum polynomial m_α^L of α over L actually has its coefficients in K.

Solution: Let $m = \deg m_\alpha^K = [K(\alpha)\colon K]$ and $n = [L\colon K]$ and $m' = \deg m_\alpha^L = [L(\alpha)\colon L]$. The hypotheses give $(m, n) = 1$. We certainly know that $m' \le m$ and $m_\alpha^L | m_\alpha^K$. Hence $[L(\alpha)\colon K] = m'n \le mn$. However it is clear that both m and n divide $[L(\alpha)\colon K]$, and since they are relatively prime we must have $mn = [L(\alpha)\colon K]$. In particular $m = m'$ and therefore $m_\alpha^L = m_\alpha^K$, so m_α^L is really a polynomial with coefficients in K.