

## 18.700 - Fall 2006 - Solutions to Problem Set 1

### Problem 1.

- (a) Yes. In fact,  $\mathbb{Q}(\sqrt{2})$  contains 0. It is closed under sum and multiplication, because for  $a, b, c, d \in \mathbb{Q}$  the sum  $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$  belongs to  $\mathbb{Q}(\sqrt{2})$  (because  $a + c \in \mathbb{Q}$  and  $b + d \in \mathbb{Q}$ ) and the product  $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$  belongs to  $\mathbb{Q}(\sqrt{2})$  (because  $ac + 2bd \in \mathbb{Q}$  and  $ad + bc \in \mathbb{Q}$ ).

Moreover,  $\mathbb{Q}(\sqrt{2})$  is closed under taking the opposite, because if  $a, b \in \mathbb{Q}$  then the opposite of  $a + b\sqrt{2}$  is  $-a - b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$  (because  $(-a), (-b) \in \mathbb{Q}$ ). Finally,  $\mathbb{Q}(\sqrt{2})$  is closed under taking inverses. In fact, if  $0 \neq a + b\sqrt{2}$  with  $a, b \in \mathbb{Q}$ , then its inverse is

$$\frac{1}{a + b\sqrt{2}} \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \left( \frac{a}{a^2 - 2b^2} \right) - \left( \frac{b}{a^2 - 2b^2} \right) \sqrt{2}$$

which still belongs to  $\mathbb{Q}(\sqrt{2})$  because  $a/(a^2 - 2b^2)$  and  $b/(a^2 - 2b^2)$  are in  $\mathbb{Q}$  (notice that we multiplied and divided by  $a - b\sqrt{2}$ , which is nonzero as  $a + b\sqrt{2} \neq 0$ ).

- (b) A basis is given by  $\mathcal{B} = \{1, \sqrt{2}\}$ . In fact, every element of  $\mathbb{Q}(\sqrt{2})$  can be written as  $a \cdot 1 + b \cdot \sqrt{2}$  by definition, which shows that  $\mathcal{B}$  is set of generators for  $\mathbb{Q}(\sqrt{2})$  over  $\mathbb{Q}$ .

Now, we want to show that 1 and  $\sqrt{2}$  are linearly independent over  $\mathbb{Q}$ , that is we want to show that: if  $a \cdot 1 + b \cdot \sqrt{2} = 0$  with  $a, b \in \mathbb{Q}$ , then  $a = b = 0$ . If  $b \neq 0$ , then  $\sqrt{2} = -a/b \in \mathbb{Q}$  which is clearly a contradiction, because  $\sqrt{2}$  is not a rational number. Hence,  $b = 0$ . As a consequence,  $a \cdot 1 + 0 \cdot \sqrt{2} = 0$  implies  $a = 0$ .

[Proof that  $\sqrt{2}$  is irrational, not needed in the Problem Set.

By contradiction, suppose there exist  $p, q$  positive integers such that  $\sqrt{2} = p/q$ . Then  $q\sqrt{2} = p$  and, squaring both hand-sides,  $2q^2 = p^2$ . Notice that, in their factorization into a product of primes,  $p^2$  contains an even number of factors 2 and  $2q^2$  contains an odd number of factors 2. Because the factorization is unique, this is a contradiction.]

### Problem 2.

- (a) A vector subspace of  $\mathbb{C}^2$  must contain  $\vec{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ . So, if  $k \neq 0$ , then  $V_k$  is not a vector subspace of  $\mathbb{C}^2$ .

Instead  $V_0$ , which is equal to  $\left\{ \begin{pmatrix} z \\ -z \end{pmatrix} \in \mathbb{C}^2 \mid z \in \mathbb{C} \right\}$ , is a vector subspace of  $\mathbb{C}^2$ . In fact,

$V_0$  contains  $\vec{0}$ . Moreover, for every  $z, w \in \mathbb{C}$  the sum  $\begin{pmatrix} z \\ -z \end{pmatrix} + \begin{pmatrix} w \\ -w \end{pmatrix} = \begin{pmatrix} z + w \\ -(z + w) \end{pmatrix}$  still belongs to  $V_0$  (closure under sum). Moreover, for every  $\lambda \in \mathbb{C}$  and  $z \in \mathbb{C}$  the product  $\lambda \cdot \begin{pmatrix} z \\ -z \end{pmatrix} = \begin{pmatrix} \lambda \cdot z \\ -\lambda \cdot z \end{pmatrix}$  belongs to  $V_0$ .

- (b) A basis for  $V_0$  is  $\mathcal{B} = \left\{ \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$ . In fact, every element of  $V_0$  can be written as  $z \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix}$  for some  $z \in \mathbb{C}$ , so that  $\mathcal{B}$  is a set of generators of  $V_0$  over  $\mathbb{C}$ . Moreover, if a set containing only one nonzero vector is always a set of linearly independent vectors. Thus  $\mathcal{B}$  is a basis for  $V_0$  over  $\mathbb{C}$ .

- (c) The same argument of (a) says that  $W_k$  is not a vector subspace of  $\mathbb{C}^2$  over any field for  $k \neq 0$ . About  $W_0$ , notice that  $(i, i)$  belongs to  $W_0$  but  $i \cdot (i, i) = (-1, -1)$  does not. Hence,  $W_0$  is not a vector subspace of  $\mathbb{C}^2$  over  $\mathbb{C}$ .
- (d) The same argument of (a) says that  $W_k$  is not a vector subspace of  $\mathbb{C}^2$  over any field for  $k \neq 0$ . Notice that  $W_0$  contains  $\vec{0}$  and  $W_0$  can be identified to  $\left\{ \begin{pmatrix} z \\ -\bar{z} \end{pmatrix} \in \mathbb{C}^2 \mid z \in \mathbb{C} \right\}$ . Moreover, for every  $z, w \in \mathbb{C}$  the sum  $\begin{pmatrix} z \\ -\bar{z} \end{pmatrix} + \begin{pmatrix} w \\ -\bar{w} \end{pmatrix} = \begin{pmatrix} z+w \\ -(z+w) \end{pmatrix}$  still belongs to  $W_0$ . Finally, for every  $\lambda \in \mathbb{R}$  and  $z \in \mathbb{C}$  the product  $\lambda \cdot \begin{pmatrix} z \\ -\bar{z} \end{pmatrix} = \begin{pmatrix} \lambda \cdot z \\ -\lambda \cdot \bar{z} \end{pmatrix}$  belongs to  $W_0$  because  $\lambda \cdot \bar{z} = \bar{\lambda} \cdot z = \overline{\lambda \cdot z}$  for  $\lambda \in \mathbb{R}$ .

**Problem 3.**

- (a)  $\mathbb{R}[t]_d$  is not a vector subspace of  $\mathbb{R}[t]$  because it does not contain 0 (for which the degree is not defined).

If we consider  $\mathbb{R}[t]_d \cup \{0\}$  (instead of  $\mathbb{R}[t]_d$ ), then it is a vector subspace over  $\mathbb{R}$  if  $d = 0$ . If  $d > 0$ , then  $\mathbb{R}[t]_d \cup \{0\}$  is not a vector subspace, because  $t^d$  and  $1 - t^d$  are polynomials in  $\mathbb{R}[t]$  of degree exactly  $d$  but their sum  $(t^d) + (1 - t^d) = 1$  has degree  $0 \neq d$ , so it does not belong to  $\mathbb{R}[t]_d \cup \{0\}$ .

- (b) In order to be a vector subspace,  $E_k$  must contain the zero vector  $\vec{0}$ , which is the zero polynomial in our case. The zero polynomial belongs to  $E_k$  if and only if  $k = 0$ . So  $E_k$  is not a vector subspace if  $k \neq 0$ . Instead,  $E_0$  is an  $\mathbb{R}$ -vector subspace of  $\mathbb{R}[t]$ . In fact, if  $p, q \in E_0$ , then  $(p + q)(2) = p(2) + q(2) = 0$  and so  $p + q \in E_0$ . Moreover, if  $\lambda \in \mathbb{R}$  and  $p \in E_0$ , then  $(\lambda \cdot p)(2) = \lambda \cdot (p(2)) = \lambda \cdot 0 = 0$  and so  $\lambda \cdot p \in E_0$ .

- (c) We have seen during the first lecture that  $\mathbb{R}[t]_{\leq d}$  is a vector subspace of  $\mathbb{R}[t]$ .  $E_0$  also is a vector subspace of  $\mathbb{R}[t]$ . Their intersection is a vector subspace of  $\mathbb{R}[t]$ . In fact, for every  $p, q \in E_0 \cap \mathbb{R}[t]_{\leq d}$   $p + q$  belongs to both  $E_0$  and  $\mathbb{R}[t]_{\leq d}$  and so to their intersection. The zero polynomial also belongs to  $E_0 \cap \mathbb{R}[t]_{\leq d}$ . Moreover, if  $\lambda \in \mathbb{R}$  and  $p \in E_0 \cap \mathbb{R}[t]_{\leq d}$ , then  $\lambda \cdot p \in E_0 \cap \mathbb{R}[t]_{\leq d}$ .

[Notice that the same argument shows that: if  $V$  is a vector space over a field  $F$  and  $W_1, W_2 \subset V$  are two vector subspace of  $V$  over  $F$ , then their intersection  $W_1 \cap W_2$  is a vector subspace of  $V$  over  $F$ .]

A basis of  $E_0 \cap \mathbb{R}[t]_{\leq 2}$  is  $\mathcal{B} = \{t - 2, (t - 2)^2\}$ . First, notice that  $\mathcal{B}$  is a subset of  $E_0 \cap \mathbb{R}[t]_{\leq 2}$ . Clearly,  $\mathcal{B}$  is a set of linearly independent vectors. In fact, if  $a, b \in \mathbb{R}$  and  $a(t - 2) + b(t - 2)^2 = 0$  ( $= 0$  means: equal to the zero polynomial!), then  $bt^2 + (a - 4b)t + (4b - 2a) = 0$ . As a polynomial is the zero polynomial if and only if all its coefficients are zero, then we need  $a = b = 0$ .

To show that  $\mathcal{B}$  is a set of generators for  $E_0 \cap \mathbb{R}[t]_{\leq 2}$  over  $\mathbb{R}$ , let  $p(t) = at^2 + bt + c \in E_0 \cap \mathbb{R}[t]_{\leq 2}$ . Notice that  $t^2 = (t - 2)^2 + 4t - 4 = (t - 2)^2 + 4(t - 2) + 4$  and  $t = (t - 2) + 2$ , so that  $p(t) = at^2 + bt + c = a[(t - 2)^2 + 4(t - 2) + 4] + b[(t - 2) + 2] + c = a(t - 2)^2 + (4a + b)(t - 2) + (4a + 2b + c)$ . The condition  $p(2) = 0$  forces  $4a + 2b + c = 0$ , so that  $p(t)$  is a linear combination of  $(t - 2)^2$  and  $(t - 2)$ .

- (d) A basis of  $E_0$  is  $\mathcal{B} = \{(t - 2)^n \in E_0 \mid n \text{ positive integer}\}$ .  
*Linear independence:* By contradiction, suppose  $a_d(t - 2)^d + a_{d-1}(t - 2)^{d-1} + \dots + a_1(t - 2) = 0$  ( $= 0$  means: is the zero polynomial!) with  $a_d \neq 0$ . Then  $a_d(t - 2)^d + a_{d-1}(t - 2)^{d-1} + \dots +$

$a_1(t-2) = a_d t^d + (\text{lower order terms})$ , which clearly cannot be the zero polynomial!

*Generation:* We want to show that every polynomial  $p(t)$  such that  $p(2) = 0$  can be written as a linear combination of elements in  $\mathcal{B}$ . We proceed by induction on the degree  $d$  of  $p(t)$ .

The assertion is clearly true for  $d = 0, 1$ . Assume that the assertion holds for all polynomials of degree less than  $d$ : we want to show that it holds for polynomials of degree  $d$ .

Let  $p(t) \in E_0$  be a polynomial of degree  $d$ . Then  $p(t) = a_d t^d + q(t)$ , where  $q(t)$  is a polynomial of degree less than  $d$ . We can rewrite  $p(t) = a_d(t-2)^d + r(t)$ , where  $r(t) = a_d t^d - a_d(t-2)^d + q(t)$  is a polynomial of degree less than  $d$ . Moreover,  $r(t) = p(t) - a_d(t-2)^d$  so that  $r(2) = 0$ . Hence,  $r(t)$  belongs to  $E_0$ . By induction,  $r(t)$  can be written as a linear combination of elements in  $\mathcal{B}$ . As  $p(t) = a_d(t-2)^d + r(t)$ , the polynomial  $p(t)$  can be written as a linear combination of elements in  $\mathcal{B}$  too.

**Problem 4.** (5 points: 2+3)

- (a) The maximum number of nonzero vectors in  $(\mathbb{Z}/3\mathbb{Z})^2 = (\mathbb{Z}/3)^2$  is 4. For example,

$$\begin{pmatrix} \bar{1} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} \\ \bar{2} \end{pmatrix}$$

**Proof of maximality**

Consider a subset  $\mathcal{B} \subset (\mathbb{Z}/3)^2$  containing at least five distinct vectors  $v_1, v_2, v_3, v_4, v_5$ . Assume that none of the  $v_i$  is zero. Then the **ten** vectors

$$v_1, v_2, v_3, v_4, v_5, \bar{2} \cdot v_1, \bar{2} \cdot v_2, \bar{2} \cdot v_3, \bar{2} \cdot v_4, \bar{2} \cdot v_5$$

are all nonzero, because  $v_i \neq \bar{0}$  for  $i = 1, \dots, 5$  and  $\bar{2} \neq \bar{0}$ . Moreover  $\bar{2} \cdot v_i = \bar{2} \cdot v_j \implies \bar{2} \cdot \bar{2} \cdot v_i = \bar{2} \cdot \bar{2} \cdot v_j \implies \bar{1} \cdot v_i = \bar{1} \cdot v_j$  and so  $i = j$ .

But  $(\mathbb{Z}/3)^2$  contains only 8 nonzero vectors. So there must be  $i, j$  such that  $v_i = \bar{2}v_j$ . Thus,  $v_i$  and  $v_j$  are proportional.

- (b) The vector space  $(\mathbb{Z}/p)^n$  has  $p^n$  elements, so the number of nonzero vectors is exactly  $p^n - 1$ . Fix a nonzero vector  $v \in (\mathbb{Z}/p)^n$ . The nonzero vectors of  $(\mathbb{Z}/p)^n$  proportional to  $v$  are clearly  $\bar{1} \cdot v, \bar{2} \cdot v, \dots, \overline{(p-1)} \cdot v$ , which are all distinct (otherwise we would have  $\bar{a} \cdot v = \bar{b} \cdot v$ , that is  $\overline{(a-b)} \cdot v = \bar{0}$ , which is impossible because  $\overline{a-b} \neq 0$  and  $v \neq \bar{0}$ ). Hence, every *class* contains exactly  $p - 1$  nonzero vectors. Thus, the set of nonzero vectors (which has  $p^n - 1$  elements) is made of classes of  $p - 1$  elements each. This means that there are exactly

$$\frac{p^n - 1}{p - 1} = 1 + p + p^2 + \dots + p^{n-1}$$

classes. A set of nonzero vectors that are pairwise linearly independent can be obtained by choosing a vector in each class.