# Supplementary problems (posted July 4, updated July 5 3pm)
# REU 2012
Instructor: László Babai  Scribe: Jonathan Gleason

♢ indicates problems that express fundamental facts of linear algebra that you must not miss ("must problems"). ♡ indicates memorable pieces of creative problem solving ("sweet problems").

**Problem 1.** (a) Show that every subgroup of $H \leq (\mathbb{Z}, +)$ is cyclic, i. e., it is of the form $H = d\mathbb{Z}$ for some $d$ (where $d\mathbb{Z} = \{dz \mid z \in \mathbb{Z}\}$).

(b) Use this to show that gcd of integers exists and can be written as a linear combination. (Hint: Notive that given $a, b \in \mathbb{Z}$, the numbers of the form $ax + by$ form a subgroup of $(\mathbb{Z}, +)$.)

♡ **Problem 2.** (a) Recall that an integer $p$ has the *prime property* if $(\forall a, b)($ if $p \mid ab$ then $p \mid a$ or $p \mid b$. Prove that all prime numbers have the prime property. (Use the fact that the gcd is a linear combination.)
(b) Infer the uniqueness of prime factorization from (a).

**Problem 3.** Let $a, b, d \in \mathbb{Z}$. Show that if $d$ is a common divisor of $a$ and $b$ and $d$ can be written as a linear combination of $a$ and $b$ then $|d| = \gcd(a, b)$.

♡ **Problem 4.** Let $k$ be the number of binary digits of $\max(a, b)$ where $a$ and $b$ are positive integers. Show that Euclid's algorithm to find $\gcd(a, b)$ terminates in at most $2k$ rounds. (Each round consist of one application of the Division Theorem.) Give a very simple proof.

**Problem 5.** (a) Define the gcd of polynomials over the field $F$. (b) Prove that the gcd exists and can be expressed as a linear combination with coefficients that are themselves polynomials:
$(\forall f, g \in F[x])(\exists u, v \in F[x])(\gcd(f, g) = uf + vg)$.
(b) Recall that a polynomial $f \in F[x]$ is irreducible over $F$ if its degree is at least 1 and $(\forall g, h \in F[x])($ if $f = gh$ then eithe $g$ or $h$ has degree zero (is a nonzero constant). These polynomials correspond to the prime numbers. Prove that every nonzero polynomial has a unique factorization into irreducible polynomials (unique up to order and scalar multiples). (Hint: copy the ideas for integers above.)

**Problem 6.** The Gauss Lemma (Problems 134 and 135 in the main problem set) is the principal tool for proving irreducibility over the rationals. Prove the Gauss Lemma and use it in the two problems below.

**Problem 7.** (a) Prove that the polynomial $x^4 + 1$ is irreducible over $\mathbb{Q}$.
(b) Factor $x^4 + 1$ into its irreducible factors over $\mathbb{R}$.
(c) Prove that $x^4 + 4$ is reducible over $\mathbb{Q}$.

♡ **Problem 8.** Let $a_1, \ldots, a_k$ be distinct integers. Prove that the following polynomials are irreducible over $\mathbb{Q}$:
(a) $f(x) = \left(\prod_{i=1}^{k}(x - a_i)\right) - 1$
(b) $g(x) = \left(\prod_{i=1}^{k}(x - a_i)\right)^2 + 1$.

♢ **Problem 9.** Let $A, B$ be $n \times n$ matrices over $F$. Prove: $\det(AB) = \det(A)\det(B)$.

**Problem 10.** (a) Find the dimension of $\mathbb{C}$ over $\mathbb{C}$, the dimension of $\mathbb{C}$ over $\mathbb{R}$, and the dimension of $\mathbb{R}$ over $\mathbb{Q}$. (b) Show that the dimension of the space $\mathbb{R}[x]$ of polynomials over $\mathbb{R}$ is countable, (c) Show that the dimension of the space $\mathbb{R}(x)$ of rational functions (equivalence classes of fractions of polynomials) over $\mathbb{R}$ is continuum (and therefore uncountable).

♡ **Problem 11.** A $(0,1)$-matrix is a matrix of which every entry is 0 or 1. Let $A$ be a $k \times n$ $(0,1)$-matrix with distinct columns. Prove that $\mathrm{rk}(A) \geq \log_2(n)$. Prove this statement over *every field*. (In class this was proved over $\mathbb{F}_2$ and as a consequence over all fields of characteristic 0 or 2. Prove it over $\mathbb{F}_3$. The log remains to base 2 regardless of the field.)

♡ **Problem 12.** Let $A = (a_{ij})$ be a $k \times n$ matrix of rank $r$ over the field $F$. Consider the $k \times n$ matrix $B = (a_{ij}^2)$ (we square every entry of $A$). Prove: $\mathrm{rk}(B) \leq r(r+1)/2$.

♢ **Problem 13.** Let $F$ be a field, let $V = F^n$, and let $e_k \in V$ be the vector with a 1 in the $k^{\text{th}}$ component and 0s elsewhere. Let $f : \overbrace{V \times \cdots \times V}^{\text{n times}} \to F$ be an alternating multilinear function such that $f(e_1, \ldots, e_n) = 1$. Show that $f = \det$.

**Problem 14.** (a) Show that the volume of a parallelepiped defined by three vectors in $\mathbb{R}^3$ with integer coordinates is an integer. (b) Show that the area of a parallelogram defined by two vectors in $\mathbb{R}^3$ with integer coordinates is not necessaily an integer but is the square root of an integer. (c) Generalize these statements to $k$-dimensional parellelepipeds in $\mathbb{R}^n$.

**Problem 15.** Let $A$ be an $n \times n$ matrix such that $A_{ij} = \gcd(i,j)$. Show that $A$ is non-singular.

♢ **Problem 16.** (Modular equation) Let $U, V \leq W$. Let $U + V := \{u + v \mid u \in U, v \in V\}$. Show that

$$\dim(U \cap V) + \dim(U + V) = \dim(U) + \dim(V)\,.$$

♢ **Problem 17.** Let $A, B$ be matrices of appropriate dimensions over $F$.
(a) Show that $\mathrm{rk}(A + B) \leq \mathrm{rk}(A) + \mathrm{rk}(B)$.
(b) Show that $\mathrm{rk}(AB) \leq \max(\mathrm{rk}(A), \mathrm{rk}(B))$.

**Problem 18.** (a) Show that a matrix has rank $\leq 1$ exactly if it is the product of a column matrix by a row matrix. (b) Let $A$ be a $k \times n$ matrix. (b1) Show that $\mathrm{rk}(A) \leq r$ iff $A$ is the sum of $r$ matrices of rank $\leq 1$. (b2) Show that $\mathrm{rk}(A) \leq r$ iff there exists a $k \times r$ matrix $B$ and an $r \times n$ matrix $C$ such that $A = BC$. (b)

♡ **Problem 19.** (Rank versus mod 2 rank) Let $H_n$ be a $2^n \times 2^n$ $(0,1)$-matrix whose rows and columns are labeled by subsets of an $n$-element set $X$. For $A, B \subseteq X$, define $H_{A,B} = |A \cap B| \pmod 2$. Show that $\mathrm{rk}_{\mathbb{F}_2}(H) = n$ while $\mathrm{rk}_{\mathbb{Q}}(H) = 2^n - 1$.

♢ **Problem 20.** Let $V$ and $W$ be vector spaces over the same field $F$. Let $\{b_1, \ldots, b_m\}$ be a basis for $V$ and let $w_1, \ldots, w_m \in W$ be arbitrary vectors. Show that there exists a unique linear map $\varphi : V \to W$ such that $(\forall i)(\varphi(b_i) = w_i)$.

♢ **Problem 21.** (Rank-Nullity Theorem) Let $V$ and $W$ be vector spaces and let $\varphi : V \to W$ be linear. Show that $\dim(V) = \dim(\ker(\varphi)) + \mathrm{rk}(\varphi)$. (Recall that $\mathrm{rk}(\varphi)$ is defined as the dimension of $\mathrm{Im}(\varphi)$.)

**Problem 22.** (a) For what primes $p$ do there exist isotropic vectors in $\mathbb{F}_p^2$?
(b) Show that for every $p$, there exist isotropic vectors in $\mathbb{F}_p^4$.
(c) Show that for every $p$, there exist isotropic vectors in $\mathbb{F}_p^3$.

♡ **Problem 23.** Recall that a subspace $W \leq F^n$ is *totally isotropic* if $(\forall u, v \in W)(u\dot{v} = 0)$ where the dot denotes the standard dot product. We have seen that in this case, $\dim(W) \leq \lfloor n/2 \rfloor$. Prove: all maximal isotropic subspaces of $\mathbb{F}_2^n$ have dimension $\lfloor n/2 \rfloor$. In other words, all maximal Eventown club systems are maximum.

**Problem 24.** Let $A$ and $B$ be $k \times n$ matrices. Show: if $Ax = Bx$ for all $x \in F^n$ then $A = B$.

♢ **Problem 25.** (Computing a linear map from coordinates) Let $V$ and $W$ be vector spaces and let $\varphi : V \to W$ be linear. Let $\underline{e} = (e_1, \ldots, e_n)$ be a basis of $V$ and $\underline{f} = (f_1, \ldots, f_k)$ a basis of $W$. Let $v \in V$ be expressed as $v = \sum_{i=1}^{n} \alpha_i e_i$; the $\alpha_i$ are the coordinates of $v$ with respect to the basis $\underline{e}$. We write $[v]_{\underline{e}}$ for the column vector $(\alpha_1, \ldots, \alpha_n)^T$. Similarly for $w \in W$ we write $[w]_{\underline{f}}$ for the column vector consisting of the coordinates of $w$ with respect to the basis $\underline{f}$. Finally we write $[\varphi]_{\underline{e},\underline{f}}$ for the $k \times n$ matrix whose $j$th column is $[\varphi(e_j)]_{\underline{f}}$.

Prove that for every $v \in V$ we have

$$[\varphi(v)]_{\underline{f}} = [\varphi]_{\underline{e},\underline{f}} [v]_{\underline{e}}.$$

**Problem 26.** Let $A$ be a $k \times n$ matrix. When does $A$ have a left inverse? A right inverse? Express your answer in terms of the rank of $A$.

♡ **Problem 27.** Consider the "Fibonacci space" of sequences $(a_0, a_1, \ldots)$ of real numbers satisfying $a_{n+2} = a_{n+1} + a_n$.
(a) Prove that this is a vector space of dimension 2; find a natural basis.
(b) Consider the linear transformation on the Fibonacci space that shifts all sequences to the left by 1 (it drops $a_0$) (the *shift operator*). Find the matrix of this transformation in terms of your natural basis.
(c) Compute the $n$th power of this matrix. (Hint: What is the $n$th power of the shift operator?)
(d) Find the eigenvectors and eigenvalues of the shift operator.
(e) Represent the Fibonacci sequence as a linear combination of two eigenvectors. This gives a striking explicit formula for the Fibonacci numbers.

**Problem 28.** Find the eigenvalues and the eigenvectors of the rotation matrix

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

over the complex numbers.

**Problem 29.** In the space of real functions, consider the subspace $V$ spanned by $\cos x$ and $\sin x$. For $\theta \in \mathbb{R}$, define $T_\theta : V \to V$ by $(T_\theta(f))(x) = f(x - \theta)$ (shift by $\theta$). Show that $T_\theta$ is a linear transformation. Find the matrix representation of $T_\theta$ in terms of the basis $(\cos x, \sin x)$. (You will get a familiar matrix.)

**Problem 30.** When is zero an eigenvalue of the square matrix $A$? Your answer should be "When $A$ is [blank]"; fill in the blank with one word.

**Problem 31.** Let $\varphi : V \to V$ be a linear transformation. Let $v_1, \ldots v_k$ be eigenvectors of $\varphi$ corresponding to distinct eigenvalues. Prove: $v_1, \ldots v_k$ are linearly independent.

**Problem 32.** Let $F$ be any field. (a) Let $V$ be an $n$-dimensional vector space over $F$. Find a linear transformation $\varphi : V \to V$ such that $\varphi^n = 0$ but $\varphi^{n-1} \neq 0$.
(b) Find an $n \times n$ matrix over $F$ such that $A^n = 0$ but $A^{n-1} \neq 0$.
(c) Suppose $\varphi^n = 0$. Prove: the only eigenvalue of $\varphi$ is 0.

**Problem 33.** (a) Prove that every matrix has at least one eigenvector over $\mathbb{C}$.
(b) Find an $n \times n$ $(0,1)$-matrix $A$ such that $A$ does not have two linearly independent eigenvectors over $\mathbb{C}$.

$\diamondsuit$ **Problem 34.** Recall that the *characteristic polynomial* of an $n \times n$ matrix $A$ is $f_A(t) = \det(tI - A)$ where $I$ is the identity matrix. Write $f_A(t)$ as $t^n + a_{n-1}t^{n-1} + \cdots + a_0$. Prove: (a) $a_{n-1} = -\operatorname{tr}(A)$; (b) $a_0 = (-1)^n \det(A)$.

(c) A $k \times k$ symmetric minor of $A$ is the determinant of a $k \times k$ submatrix that is positioned symmetrically about the diagonal, i. e., the same set of column and row indexes determine the submatrix. Note that the number of $k \times k$ symmetric submatrices is $\binom{n}{k}$. Prove: $(-1)^k a_{n-k}$ is the sum of the $k \times k$ symmetric minors.

**Problem 35.** Recall that a complex number is *algebraic* if it is a root of a nonzero polynomial with integer coefficients. Prove that each of the following numbers is algebraic:
(a) $\sqrt{2} + \sqrt{3}$; (b) $\sqrt{2} + \sqrt[3]{2}$.

**Problem 36.** (Field extensions) Let $F \subset G \subset H$ be fields. Prove:

$$\dim_F H = (\dim_F G)(\dim_G H).$$

**Problem 37.** Let $\alpha \in \mathbb{C}$. Let $\mathbb{Q}[\alpha]$ denote the set of numbers of the form $f(\alpha)$ for all polynomials $f \in \mathbb{Q}[x]$. Prove: $\alpha$ is algebraic if and only if $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha]$ is finite if and only if $\mathbb{Q}[\alpha]$ is a field.

**Problem 38.** (Field of algebraic numbers) (a) Prove that the algebraic numbers form a field. (b) Prove that the field of algebraic numbers is algebraically closed.

**Problem 39.** Prove: if $A$ is an $n \times n$ matrix over $F$ then there exists a nonzero polynomial $f \in f[x]$ such that $f(A) = 0$. (Do not use any major theorem; your proof should take no more than a couple of lines. Use the First Miracle of linear algebra.)

$\diamondsuit$ **Problem 40.** (Change of basis) Let $\varphi : V \to W$ be a linear map. Fix an "old basis" $\underline{e}$ and a "new basis" $\underline{e}'$ in $V$ and similarly an old basis $\underline{f}$ and a new basis $\underline{f}'$ in $W$. Let $A$ be the matrix of $\varphi$ with respect to the old bases, and $A'$ the matrix of $\varphi$ with respect to the new bases. Let $S$ denote the correspoinding base change matrices: $S = [\sigma]_{\underline{e}}$ where $\sigma : V \to V$ is defined by $\sigma(e_j) = e'_j$. Define $\tau : W \to W$ and $T = [\tau]_{\underline{f}}$ analogously. Prove:

$$A' = T^{-1}AS\,.$$

Hint: Prove: for all $x \in F^n$ (where $n = \dim V$) we have $A'x = T^{-1}ASx$.