1.a parte: gruppi, congruenze e applicazioni.

1 — **Aritmetica modulare.** Le operazioni in Z/n sono ben definite. Z/n possiede n elementi. Z/n è un anello (che cos'è un anello? Esempi: Z, Q, R, C, A[x]). Risoluzione di congruenze lineari. ax = b mod n. Come riconosco gli elementi invertibili in Z/n?

2 — **L'algoritmo euclideo.** Calcolo del MCD con l'algoritmo euclideo. Identità di Bézout. MCD(a, n) = 1 se e solo se [a] è invertibile in Z/n. Z/n è un campo se e solo se n è primo.

3 — **Teorema cinese dei resti.** Gli invertibili modulo n sono chiusi rispetto a prodotto e inverso: sono un gruppo. Esistenza di soluzioni di congruenze lineari. Metodo generale di risoluzione. Sistemi di congruenze lineari: il teorema cinese dei resti.

4 — **Gruppi.** Definizione di gruppo; esempi. Se A è un anello, (A, +) e (A*, .) sono gruppi. Permutazioni e gruppo simmetrico. Concetto di sottogruppo ed esempi. Sottogruppi di Z (rilettura dell'algoritmo euclideo). Omomorfismi di gruppi: definizione ed esempi; nucleo e immagine. Sottogruppi normali.

5 — **Teorema di Lagrange.** Congruenza modulo un sottogruppo. Definizione. E' una relazione di equivalenza. Le classi di equivalenza sono le classi laterali (destre). Un esempio di calcolo dei laterali. Un sottogruppo è normale se e solo se le sue classi laterali destre sono anche classi laterali sinistre. Le classi laterali hanno tutte lo stesso numero di elementi. Ordine di un gruppo. Teorema di Lagrange: l'ordine di un sottogruppo divide l'ordine del gruppo che lo contiene. Gruppi di ordine primo. Piccolo teorema di Fermat. Teorema di Eulero.

6 — **Crittografia RSA.** Calcolo di potenze modulo n. Crittografia a chiave pubblica e sistema RSA.

7 — **Gruppi ciclici, diedrali, simmetrici.** Notazione ciclica per le permutazioni. Segno di una permutazione. Gruppo alterno.

8 — **La relazione di coniugio.** Definizione e proprietà. L'equazione delle classi. Il coniugio nei gruppi abeliani. Gruppi di ordine p^2, dove p è un primo. Gruppi di ordine pq, dove p e q sono primi distinti.
Gruppi diedrali.

9 — **Esercizi.** (Sistemi di congruenze. Calcolo di potenze mod n. Laterali di sottogruppi e normalità di sottogruppi di indice 2. Qualche forma debole del teorema di Cauchy. Buona definizione del prodotto sui laterali di un sottogruppo normale.)

10 — **Congruenze quadratiche.** Proprietà dei residui quadratici modulo un numero primo p. Simbolo di Legendre. Legge di reciprocità quadratica. Per quali valori del primo p gli elementi -1 e 2 sono residui quadratici modulo p? Algoritmo euclideo per il calcolo del simbolo di Legendre.

11 — **L'algoritmo di primalità di Solovay-Strassen.** Simbolo di Jacobi. Algoritmo (più rapido) per il calcolo dei simboli di Legendre e di Jacobi. Algoritmo di Solovay-Strassen.

12 — **Reciprocità quadratica e teorema di Solovay-Strassen.** Dimostrazioni della legge di reciprocità quadratica e del teorema alla base dell'algoritmo di Solovay-Strassen.

2.a parte: algebra lineare e matrici.

13 — **Sistemi di equazioni lineari.** Chiacchiere preliminari a proposito della risoluzione di sistemi di equazioni. Sistemi equivalenti. Esempi di manipolazioni sulle equazioni che trasformano un sistema di equazioni in un sistema equivalente: permutazione delle equazioni, moltiplicazione di (entrambi i membri di) un'equazione per uno scalare non nullo, somma di equazioni membro a membro. Spiegazione dell'idea. Calcolo esplicito in un caso concreto. Esecuzione matriciale del metodo di Gauss in un esempio.

14 — **Il metodo di eliminazione di Gauss.** Descrizione dell'algoritmo nel caso generale. Cosa può andare storto? Descrizione precisa della prima parte del procedimento di eliminazione di Gauss. Esecuzione dell'algoritmo su una matrice. Un esempio di sistema senza soluzioni. Il concetto di pivot.
Seconda parte del procedimento di eliminazione: come annullare i coefficienti sopra i pivot.
Un esempio di sistema lineare omogeneo con più di una soluzione. Un esempio di sistema lineare non omogeneo e confronto delle sue soluzioni con quelle del corrispondente sistema lineare omogeneo.
Procedimento automatico di calcolo delle soluzioni: scrivo la matrice dei coefficienti del sistema (includendo i termini noti) ed eseguo il procedimento di eliminazione: se ho un pivot sull'ultima colonna, il sistema non ha soluzioni (è incompatibile); altrimenti porto a secondo membro le variabili relative a colonne senza pivot, e parametrizzo le soluzioni assegnando ad esse valori qualsiasi. In particolare, il sistema dato ha soluzioni se e solo se non ha un pivot sull'ultima colonna

15 — **Campi.** Definizione di campo. Q, R sono campi. Z/p è un campo quando p è un numero primo; i campi finiti hanno p^n elementi. Un campo con 4 elementi.

16 — **I numeri complessi.** Definizione. Somma e prodotto. Esponenziale complessa. Forma polare. Radici dell'unità. Teorema fondamentale dell'algebra.

17 — **Risoluzione di sistemi lineari.** Due casi reali, un caso complesso, un caso in Z/2.

18 — **Piccola introduzione ai problemi lineari.** Calcolo della spesa: è lineare, e la linearità permette di fare il conto a partire da poche informazioni. Struttura di spazio vettoriale di R^n: somma tra vettori e multipli reali. Applicazioni lineari tra R^m e R^n. Interpretazione geometrica di R, R^2, R^3.
Un altro esempio di applicazione lineare: la rotazione in R^2 attorno all'origine di angolo fissato.

Matrice associata ad un'applicazione lineare da R^m a R^n. Significato e uso della matrice. Prodotto righe per colonne.

19 — **Composizione e prodotto righe per colonne.** Un nuovo esempio: l'applicazione identità e la matrice identità. La composizione di applicazioni lineari è ancora lineare. La matrice associata alla composizione si ottiene eseguendo il prodotto righe per colonne. Composizione di rotazioni nel piano e prodotto delle loro matrici: formule di addizione per seno e coseno. Un'applicazione R^m → R^n è lineare se e solo se è descritta da espressioni di primo grado senza termine noto.

20 — **Spazi vettoriali e applicazioni lineari.** Definizione di spazio vettoriale e applicazione lineare tra spazi vettoriali. Prime proprietà immediate delle applicazioni lineari: se $T : V \to W$ è lineare allora $T(0) = 0$ e $T(-v) = -T(v)$ per ogni $v \in V$. Nucleo e immagine di un'applicazione lineare. Un'applicazione lineare è iniettiva se e solo se il suo nucleo contiene solo il vettore nullo.
Sottospazi vettoriali. Il nucleo e l'immagine di un'applicazione lineare V → W sono sottospazi vettoriali (di V e W rispettivamente). Sottospazi vettoriali di R^2 ed R^3 e loro interpretazione geometrica. Applicazione alla risoluzione dei sistemi di equazioni lineari: le soluzioni di un sistema lineare omogeneo costituiscono un sottospazio vettoriale.
Esempio di risoluzione di un sistema di equazioni lineari non omogeneo. Cosa posso dire delle sue soluzioni a priori? Se $T : V \to W$ è lineare, e $w_0 \in W$, allora la differenza di due soluzioni di $T(v) = w_0$ appartiene al nucleo. Più precisamente, se v_0 è una soluzione, allora le soluzioni sono tutte e sole quelle della forma $v_0 + k$, al variare di k nel nucleo di T. Reinterpretazione dell'esempio precedente.

21 — **Nucleo e immagine.** Calcolo del nucleo e dell'immagine di applicazioni lineari. Il concetto di combinazione lineare. L'insieme delle combinazioni lineari degli elementi di un sottoinsieme $X \subset V$ è un sottospazio vettoriale di V ; è il più piccolo sottospazio vettoriale di V che contiene X.
Sottospazio vettoriale generato da un elemento, da due elementi, da nessun elemento. Sottospazio vettoriale generato da una circonferenza in R^2. Il sottospazio vettoriale generato da X può coincidere con il sottospazio vettoriale generato da un sottoinsieme proprio di X.

22 — **Dipendenza e indipendenza lineare.** Se un insieme di vettori contiene 0, allora è linearmente dipendente; se in un insieme di vettori due elementi coincidono, allora è linearmente dipendente.
Un sottoinsieme di un insieme linearmente indipendente è linearmente indipendente (in particolare, l'insieme vuoto è linearmente indipendente). Dei vettori sono linearmente indipendenti se nessuno di essi si scrive come combinazione lineare degli altri.
Se esiste v che si scrive in più di un modo come combinazione lineare di $v1, \ldots, vn$, allora $v1, \ldots, vn$ sono linearmente dipendenti; se esiste v che si scrive in esattamente un modo come combinazione lineare di $v1, \ldots, vn$, allora $v1, \ldots, vn$ sono linearmente indipendenti.
Un'applicazione lineare R^m → R^n con $m > n$ non è mai iniettiva. Un'applicazione lineare R^m → R^n può essere invertibile solo quando $m = n$.

23 — **Riformulazioni della (in)dipendenza lineare.** Come costruire un'applicazione

lineare R^k → V a partire da una da una k-upla di elementi di V. Un insieme di vettori che contiene dei generatori è un insieme di generatori. Alcune osservazioni di teoria. Ogni k-upla di elementi di V induce un'applicazione lineare R^k → V ; questa applicazione è iniettiva se e solo se gli elementi sono linearmente indipendenti, e suriettiva se e solo se gli elementi generano V . Una base di V composta da n elementi induce un'applicazione lineare invertibile R^n → V .
Due basi (finite) di V hanno lo stesso numero di elementi; dimensione di uno spazio vettoriale.
Se v1, . . . , vn ∈ V sono linearmente indipendenti e non generano V , allora è possibile trovare v tale che v1, . . . , vk, v siano ancora linearmente indipendenti.
Ogni insieme linearmente indipendente si completa ad una base.
Un insieme linearmente indipendente che ha la stessa cardinalità di una base è una base.

24 — **Dimensione di spazi vettoriali.**
Se v1, . . . , vn ∈ V sono linearmente dipendenti e generano V , allora è possibile rimuoverne uno in modo che i rimanenti siano ancora generatori di V; da ogni insieme di generatori si estrae una base
Un insieme di generatori che ha la stessa cardinalità di una base è una base.
In uno spazio vettoriale di dimensione n, n vettori sono linearmente indipendenti se e solo se sono generatori. Se U ⊂ V è un sottospazio vettoriale, allora dim U ≤ dim V ; inoltre se dim U = dim V (e V ha dimensione finita) allora U = V . Calcolo rigoroso dei sottospazi vettoriali di R^2 e R^3. Come verificare la lineare indipendenza di vettori in R^n. Calcolo di una base del nucleo di un'applicazione lineare R^5 → R^4.

25 — **Esercizi.** (Risoluzione di esercizi su completamento a basi, estrazione di basi, verifica di lineare indipendenza, ricerca di generatori di sottospazi)

26 — **Dimensione di sottospazi vettoriali.** Le manipolazioni dell'eliminazione di Gauss su una matrice non modificano il sottospazio vettoriale generato dalle sue righe. In una matrice a gradino, le righe non nulle sono linearmente indipendenti. Come determinare una base di un sottospazio vettoriale di R^n dato un insieme di suoi generatori.
La dimensione del sottospazio vettoriale generato dalle righe di una matrice è uguale al numero di pivot della sua riduzione a gradoni, ed è quindi uguale alla dimensione del sottospazio vettoriale generato dalle sue colonne.
Il Teorema di Rouché-Capelli: enunciato e dimostrazione. Esempi.

27 — **Il determinante.** Area di un parallelogramma nel piano, linearità e determinante di matrici 2 × 2. Defizione assiomatica della funzione determinante: è separatamente lineare nelle righe, è alternante nelle righe, assume il valore 1 sulla matrice identità. Una funzione che soddisfi tali proprietà è calcolabile attraverso il procedimento di eliminazione di Gauss, ed è pertanto univocamente determinata. Determinante di matrici diagonali. Determinante di matrici triangolari.
Espressione esplicita del determinante di matrici 2 × 2 e 3 × 3. Espressione generale come sommatoria sulle permutazioni. Varie definizioni del segno di una permutazione. Permutazioni pari e permutazioni dispari.

28 — **Proprietà del determinante.** Il determinante di una matrice è uguale al determinante della sua trasposta. Il determinante è separatamente lineare e

alternante anche nelle colonne della matrice. Una matrice quadrata ha righe linearmente indipendenti se e solo se ha colonne linearmente indipendenti se e solo se ha determinante non nullo. Sviluppo di Laplace: perché funziona? Le colonne di una matrice, nella cui posizione si trovano i pivot al termine del procedimento di eliminazione, sono linearmente indipendenti; le altre sono loro combinazione lineare.

29 — **Matrice inversa.** Due modi per calcolare l'inversa di una matrice. Esempi. Il metodo di Cramer per la risoluzione di sistemi quadrati. Esempi

30 — **Il teorema degli orlati.** Richiami: in una matrice quadrata, il determinante è diverso da 0 se e solo se le righe sono linearmente indipendenti se e solo se le colonne sono linearmente indipendenti; il rango di una matrice coincide sia con la dimensione del sottospazio generato dalle sue righe che con la dimensione del sottospazio generato dalle sue colonne; se ad un insieme di vettori linearmente indipendenti aggiungo un ulteriore vettore, ottengo un insieme linearmente indipendente se e solo se l'ultimo vettore non è combinazione lineare degli altri. Alcune osservazioni: in una matrice $h \times k$, con $h \leq k$, la presenza di un minore $h \times h$ non nullo implica la lineare indipendenza delle h righe; di conseguenza, la presenza di un minore $h \times h$ non nullo in una matrice garantisce la lineare indipendenza delle h righe che attraversano il minore.
Se in una matrice $(h+1)\times k$, con $h < k$, ho un minore $h\times h$ non nullo che è orlato solo da minori
$(h+1)\times(h+1)$ nulli, allora le colonne che non attraversano il minore di ordine h sono combinazione lineare delle colonne che lo attraversano, e quindi il rango della matrice è h; in particolare la riga che non attraversa il minore di ordine h è combinazione lineare delle h righe che lo attraversano. Di conseguenza, la presenza in una matrice di un minore $h \times h$ non nullo orlato da soli minori
$(h+1)\times(h+1)$ nulli garantisce che ciascuna delle righe che non attraversano il minore di ordine h è combinazione lineare delle righe che lo attraversano; in particolare, la matrice ha rango h.
Calcolo del rango di matrici attraverso il metodo dell'orlato. Compatibilità di sistemi di equazioni lineari.

31 — **Esercizi.** (Risoluzione di un sistema con il metodo di Cramer. Calcolo del rango di una matrice con il teorema degli orlati. Risoluzione di un sistema dipendente da parametri con il teorema degli orlati.)

32 — **Esercizi di tipo geometrico.** (Equazioni parametriche e cartesiane di sottospazi. Sottospazi affini. Equazione di retta per due punti, piano per tre punti. Intersezione di due sottospazi affini. Somma e intersezione di sottospazi vettoriali).

33 — **Basi e coordinate.** Coordinate in una base. L'applicazione che associa a ciascun vettore le sue coordinate rispetto ad una base fissata è lineare e invertibile. Esempio di applicazione che calcola le coordinate rispetto ad una base di R^n. Traduzione di coordinate da una base ad un'altra. L'applicazione che traduce le coordinate da una base ad un'altra è lineare e invertibile. Esempi di calcolo dell'applicazione che traduce le coordinate da una base ad un'altra base di R^n. Matrice associata ad un'applicazione lineare $T : V \to W$ una volta fissate una base di V e una base di W. Nel caso di un'applicazione $R^m \to R^n$, una volta scelte le basi canoniche di entrambi gli spazi vettoriali, la matrice associata coincide con quella

finora utilizzata.
Uso della matrice associata ad un'applicazione. Matrice associata all'identità. Composizione di applicazioni lineari e prodotto righe per colonne. Risoluzione di un esercizio.

34 — **Applicazioni lineari e matrici.** Matrice associata ad un'applicazione lineare in basi diverse: come passare da una scelta ad un'altra.
Il problema della diagonalizzazione di un endomorfismo. Esempi. Gergo: autovalori e autovettori. Una base diagonalizza un endomorfismo se e solo se è composta da suoi autovettori. Una strategia: scelgo elementi linearmente indipendenti da ciascun autospazio, li metto insieme, e cerco di ottenere una base.

35 — **Diagonalizzabilità di endomorfismi lineari.** Molteplicità algebrica e geometrica di autovalori. Alcune prime proprietà. Polinomio caratteristico e suo grado.
La molteplicità geometrica di un autovalore è sempre minore o uguale alla sua molteplicità algebrica. Un endomorfismo è diagonalizzabile solo se la somma delle molteplicità geometriche dei suoi autovalori è uguale alla dimensione n dello spazio su cui agisce: questo accade esattamente quando gli autovalori, contati con la loro molteplicità, sono n e ciascuna molteplicità geometrica coincide con la corrispondente molteplicità algebrica. Un esempio di non diagonalizzabilità.

36 — **Criteri di diagonalizzabilità.** Esempi. Dimostrazione che se la somma di elementi scelti in autospazi distinti è nulla, allora tutti gli elementi sono nulli.
Se la somma delle molteplicità geometriche degli autovalori di $T : V \to V$ coincide con $\dim V$, allora T è diagonalizzabile.

37 — **Applicazioni.** Page-rank? Rotazioni e quaternioni? Numeri di Fibonacci?

———————————————

Qui terminano gli argomenti coperti nel corso che ho tenuto l'anno accademico passato. Avrei piacere di aggiungere qualche altra applicazione, che però richiede strumenti più "metrici".

3.a parte: prodotti scalari e proprietà metriche.

38 — **Prodotti scalari e strutture euclidee.** Prodotti scalari. Decomposizione di Fourier. Ortonormalizzazione di Gram-Schmidt. Applicazione: ogni endomorfismo di uno spazio vettoriale complesso di dimensione finita ha matrice triangolare superiore in una base ortonormale opportuna.

39 — **Teorema spettrale.** Due endomorfismi che commutano si triangolarizzano nella stessa base. Se V è uno spazio euclideo complesso di dimensione finita, e $T : V \to V$ commuta con la sua aggiunta, allora T si diagonalizza in una base ortonormale. Esempi: applicazioni simmetriche (hermitiane), antisimmetriche (antihermitiane), ortogonali (unitarie). Decomposizione per autovalori singolari.

40 — **Applicazioni.** Algoritmi di compressione. Algoritmi efficienti di moltiplicazione di numeri grandi.

1.st part: groups, congruences and applications.

1 — Modular arithmetic. Operations in Z/n are well defined. Z/n has cardinality n. Z/n is a ring (what is a ring? Examples: Z, Q, R, C, A[x]). Solving linear congruences. ax = b mod n. How do I tell whether an element of Z/n is invertible?

2 — Euclidean algorithm. Computing GCD with the Euclidean algorithm. Bézout's identity. GCD(a, n) = 1 iff [a] is invertible in Z/n. Z/n is a field iff n is prime.

3 — Chinese remainder theorem. Invertible elements mod n are closed under product and taking inverse: they constitute a group. Existence of solutions of linear congruences. General solution method. Systems of linear congruences: the Chinese remainder theorem.

4 — Groups. Definition of group; examples. If A is a ring, then (A, +) and (A*, .) are groups. Permutations and symmetric groups. The concept of subgroup; examples. Subgroups of Z (using the Euclidean algorithm). Group homomorphisms: definition and examples; kernel and image. Normal subgroups.

5 — Lagrange's theorem. Congruence modulo a subgroup: definition; it is an equivalence relation; equivalence classes are the right cosets. Computing cosets in an example. A subgroup is normal iff its right cosets are also left cosets. Cosets have the same cardinality. Order of a group. Lagrange's theorem: the order of a subgroup divides the order of the group it is contained in. Groups of prime order. Fermat's little theorem. Euler's theorem.

6 — RSA encryption. Computing powers modulo n. Public key cryptography and RSA.

7 — Cyclic, dihedral, symmetric groups. Notation for cyclic permutations. Sign of a permutation. Alternating group.

8 — The conjugation relation. Definition and properties. Conjugacy class equation. Conjugacy classes in Abelian groups. Groups of order p^2, where p is a prime. Groups of order pq, where p and q are distinct primes. Dihedral groups.

9 — Exercises. (Systems of congruences. Calculation of powers mod n. Cosets of subgroups and normal subgroups of index 2. Some weak forms of Cauchy's theorem. Good definition of the product on cosets of a normal subgroup.)

10 — Quadratic congruences. Properties of quadratic residues modulo a prime number p. Legendre symbol. Law of quadratic reciprocity. For which values of the prime p are -1 and 2 quadratic residues modulo p? Euclidean algorithm for calculating the Legendre symbol.

11 — The Solovay-Strassen primality algorithm. Jacobi symbol. A (faster) algorithm

for the calculation of Legendre and Jacobi symbols. Solovay-Strassen algorithm.

12 — Quadratic reciprocity and Solovay-Strassen theorem. Proof of the law of quadratic reciprocity and of the statement underlying the Solovay-Strassen theorem.

2.nd part: linear algebra and matrices.

13 — Systems of Linear Equations. A few preliminary words about the resolution of systems of equations. Equivalent systems. Examples of the algebraic manipulations that transform a system of equations in an equivalent system: permutation of equations, multiplication of (both members of) an equation by a non-zero scalar, adding equations. Explicit calculation in a specific case. Matrix form of the Gauss method in an example.

14 — Gauss elimination method. Description of the algorithm in the general case. What can go wrong? Precise description of the first part of the Gauss elimination process. Applying the algorithm on a matrix. An example of a system without solutions. The concept of pivot.
Second part of the elimination process: how to cancel the coefficients above pivots. An example of a homogeneous linear system with more than one solution. An example of a inhomogeneous linear system, and comparison of its solutions with those of the corresponding homogeneous linear system.
Computation of solutions: write the matrix of coefficients of the system (including the known terms) and apply the elimination procedure: when there is a pivot on the last column, the system has no solutions; otherwise move all variables relative to columns without pivot to the right-hand side, and parametrize solutions assigning arbitrary values to such variables. In particular, the system has solutions if and only if it does not have a pivot on the last column.

15 — Fields. Definition. Q, R are fields. Z/p is a field when p is a prime number; finite fields have p^n elements. A field with 4 elements.

16 — Complex numbers. Definition. Sum and product. Complex exponential. Polar Form. Roots of 1. Fundamental Theorem of Algebra.

17 — Solving linear systems. Two real examples, a complex example, an example in Z/2.

18 — Short introduction to linear problems. Grocery shopping: expense is linear, and linearity allows to compute total expence from limited information. Structure of the real vector space R^n: sum of vectors and scalar multiples. Linear maps between R^m and R^n. Geometric Interpretation of R, R^2, R^3.
Another example of linear map: a rotation around the origin by a fixed angle in the real plane.
Matrix associated to a linear map from R^m to R^n. Meaning and use of matrices. Multiplying matrices rows by columns.

19 — Composition and product rows by columns. A new example: the identity map and the identity matrix. The composition of linear maps is still linear. Composing linear maps corresponds to multiplying matrices rows by columns. Composition of

rotations in the plane and the product of their matrices: addition formulas for sine and cosine functions. A map R^m → R^n is linear if and only if it is described by first degree expressions without constant term.

20 — Vector spaces and linear maps. Definition of vector space and linear map between vector spaces. First properties of linear maps: if T: V → W is linear then T (0) = 0 and T (-v) = -T (v) for each v ∈ V. Kernel and image of a linear map. A linear map is injective if and only if its kernel contains only the zero vector.
Subspaces. The kernel and the image of a linear map V → W are subspaces (of V and W, respectively). Subspaces of R^2 and R^3 and geometric interpretation.
Application to solving systems of linear equations: the solutions of a homogeneous linear system form a vector subspace.
Example of solving an inhomogeneous system of linear equations. What can one say about its solutions? If T: V → W is linear, and w_0 ∈ W, then the difference of two solutions of T (v) = w_0 belongs to the kernel. More precisely, if V_0 is a solution, then the solutions are exactly those of the form V_0 + k, where k lies in the kernel of T.

21 — Kernel and image. Computing kernel and image of linear maps.
The concept of linear combination. The set of linear combinations of elements lying in a subset X⊂V is a subspace of V; it is the smallest subspace of V containing X.
Subspace generated by an element, two elements, by any number of elements.
Subspace generated by a circumference in R^2. The vector subspace generated by X may coincide with the vector subspace generated by a proper subset of X.

22 — Linear dependence and independence. If a set of vectors contains 0, then it is linearly dependent; if in a set of vectors two elements coincide, then it is linearly dependent.
A subset of a linearly independent set is linearly independent (in particular, the empty set is linearly independent). Some vectors are linearly independent if none of them can be written as a linear combination of the others.
If there exists v that can be written in more than one way as a linear combination of v1,. . . , vn, then v1. . . , vn are linearly dependent; if there exists v that can be written in exactly one way as linear combination of v1,. . . , vn, then v1. . . , vn are linearly independent.
A linear map R^m → R^n with m>n is never injective. A linear map R^m → R^n can only be invertible when m = n.

23 — Reformulations of linear (in)dependence. How to build a linear map R^k → V starting from a from a k-tuple of elements of V. A set of vectors that contains a set of generators is a set of generators. Each k-tuple of elements of V induces a linear map R^k → V; this application is injective if and only if the elements are linearly independent, and surjective if and only if the elements generate V. A basis of V which consists of n elements induces a linear application invertible R^n → V.
Two (finite) bases of V have the same number of elements; dimension of a vector space.
If v1. . . , vn ∈ V are linearly independent and do not generate V, then it is possible to find v such that v1,. . . , vk, v is still linearly independent. Every linearly independent set can be completed to a basis.
A linearly independent set that has the same cardinality of a (finite) basis is a basis.

24 — Dimension of vector spaces.
If v1. . . , vn $\in$ V are linearly dependent and generate V, then it is possible to remove one of them in such a way that the remaining are still V generators; a basis can be extracted from every set of generators. A set of generators that has the same cardinality of a basis is a basis.
In a vector space of dimension n, n vectors are linearly independent if and only if they are generators. If U $\subset$ V is a vector subspace, then dim U $\leq$ dim V; also if dim U = dim V (and V is finite dimensional) then U = V. Rigorous computation of vector subspaces of R^2 and R^3. Verifying linear (in)dependence of vectors in R^n. Computing a basis of the kernel of a linear map R^5 $\to$ R^4.

25 — Exercises. (Solving exercises on completion to bases, basis extraction, linear independence, generators of subspaces).

26 — Dimension of subspaces. The Gauss elimination procedure on a matrix does not change the vector subspace generated by its rows. If a matrix is in echelon form, non-zero rows are linearly independent. How to compute a basis of a vector subspace of R^n from a set of generators.
The dimension of the vector subspace generated by the rows of a matrix is equal to the number of pivot of its echelon reduction, and is therefore equal to the dimension of the vector subspace generated by its columns.
The Rouché-Capelli theorem: statement and proof. Examples.

27 — The determinant. Area of a parallelogram in the plane, linearity and determinant of matrices 2 $\times$ 2. Axiomatic definition of the determinant function: it is separately linear and alternating in the rows, takes the value 1 on the identity matrix. A function that satisfies these properties can be calculated by performing Gauss elimination procedure, and is therefore uniquely determined. Determinant of diagonal matrices. Determinant of (upper) triangular matrices.
Explicit expression of the determinant of 2x2 and 3x3 matrices. General expression as a sum over permutations. Different definitions of the sign of a permutation. Even and odd permutations.

28 — Properties of the determinant. The determinant of a matrix is equal to the determinant of its transpose. The determinant is separately linear and alternating also with respect to the columns of the matrix. A square matrix has linearly independent rows if and only if it has linearly independent columns if and only if it has non-zero determinant. Laplace expansion: why does it work? The columns of a matrix corresponding to pivots at the end of the Gauss elimination procedure are linearly independent; the others can be expressed as their linear combinations.

29 — Inverse matrix. Two ways to compute the inverse of a matrix. Examples. The Cramer method for solving square systems of equations. Examples.

30 — Kronecker's theorem on rank and minors. A square matrix has 0 determinant iff the rows are linearly independent iff the columns are linearly independent; the rank of a matrix coincides with both the dimension of the subspace generated by its rows and with the dimension of the subspace generated by its columns;by adding a vector to a set of linearly independent vectors, one obtains a linearly independent set iff the

last vector is not a linear combination of the others.
Starting observations: in an h×k matrix, with h ≤ k, the presence of a non-zero h×h minor implies linear independence of the h rows; consequently, the presence of a non-zero h×h minor in a matrix guarantees the linear independence of the h rows through the minor. If in a (h + 1) × k matrix, with h <k, a non-zero h×h minor can be extended only to vanishing (h+1)x(h+1) minors, then the columns that do not intersect the hxh minor are linear combination of the columns that pass through it, and then the rank of the matrix is h; in particular the rows that do not intersect the hxh minor are linear combinations of the h rows that cross it. As a consequence, the presence in a matrix of a non-zero h×h minor that can be extended only to vanishing (h+1)x(h+1) minors ensures that each of the rows that do not cross the hxh minor is a linear combination of the rows that pass through it; in particular, the matrix has rank h.
Calculation of the rank matrices through Kronecker's theorem. Compatibility of systems of linear equations.

31 — Exercises. (Solving a system of linear equations with Cramer's method. Calculating the rank of a matrix with Kronecker's theorem. Solving a paramenter dependent system of linear equations.)

32 — Use of linear concepts in geometry. (Parametric and Cartesian equations of subspaces. Affine subspaces. Equation of a straight line passing through two points, of a plane through three points. Intersection of two affine subspaces. Sum and intersection of subspaces).

33 — Bases and coordinates. Coordinates with respect to a given basis. The map associating each vector with its coordinates in a fixed base is linear and invertible. Example of a map calculating coordinates with respect to a basis of R^n.
"Translating" coordinates from one basis to another. The maps that converts coordinates from one basis to another one is linear and invertible. Computing maps that translate coordinates from one basis to another basis of R^n.
Matrix associated to a linear map T: V → W with respect to given bases of V and of W. Special cases.
Use of the matrix associated with a linear map. Matrix associated with identity map. Composition of linear applications and multiplication row by column. Explicit examples.

34 — Linear maps and matrices. Matrix associated to a linear map in different bases: how to pass from one choice to another.
The problem of diagonalization of endomorphisms. Examples. Jargon: eigenvalues and eigenvectors. A basis diagonalizes an endomorphism if and only if it consists of its eigenvalues. A strategy: choose linearly independent elements from each eigenspace, put them together, and try to get a basis.

35 — Diagonalizability of linear endomorphisms. Algebraic and geometric multiplicity of eigenvalues. Some basic properties. Characteristic polynomial and its degree.
The geometric multiplicity of an eigenvalue is always less than or equal than its algebraic multiplicity. An endomorphism is diagonalizable only if the sum of the geometric multiplicity of its eigenvalues equals the dimension of the vector space it acts on: this happens exactly when the eigenvalues, counted with their multiplicity,

are n and each geometric multiplicity coincides with the corresponding algebraic multiplicity. A non-diagonalizable example.

36 — Diagonazability criteria. Examples. Proof that the sum of eigenspaces is direct. If the sum of the geometric multiplicity of the eigenvalues of $T: V \to V$ coincides with dim V, then T is diagonalizable.