Topics for the exam – List of definitions, theorems and proofs
(**D** = definition, **T** = theorem, **P** = theorem + proof)

1. **Integers**
   - **D** Number systems ($\mathbb{N}, \mathbb{Z}, \mathbb{Q}$), algebraic and transcendental numbers, well ordered sets, integral and fractional part of real numbers and recursive sequences, rings and fields,
   - **T** Well-ordering principle
   - **P** $\sqrt{2}$ is irrational, concept of mathematical induction (with proof with the well ordering principle), Dirichlet approximation
2. **Euclidean algorithm**
   - **D** divisibility, units, gcd, lcm, linear Diophantine equations
   - **T** Properties of divisibility, division with remainders, numeral systems, Horner's method
   - **P** Existence of gcd, Extended Euclidean algorithm, properties of gcd, solutions of linear Diophantine equations.
3. **Primes**
   - **D** irreducibles and primes
   - **T** Legendre's formula
   - **P** primes = irreducibles in $\mathbb{Z}$, there are infinitely many primes, Fundamental theorem of Number theory
4. **Modular arithmetics**
   - **D** $a \equiv b \pmod{m}$, residue classes, complete and reduced residue systems, Euler's totient function φ, modular inverse
   - **T** Properties of operations with congruences, computing modular powers, linear combinations of complete and reduced residue systems, the canonical form of φ, solution of linear congruences and the number of solutions, $\mathbb{Z}_m$ is a ring and $\mathbb{Z}_p$ is a field
   - **P** Dividing congruences, Euler-Fermat's theorem, Fermat's little theorem, Chinese remainder theorem
5. **Complex numbers**
   - **D** Complex numbers, algebraic and trigonometric form, conjugate, absolute value, roots of unity, multiplicative order and primitive roots
   - **T** The algebraic form is uniqe, $\mathbb{C}$ is a field, operations in algebraic and trigonometric form, properties of conjugate and absolute value, fundamental theorem of Algebra
   - **P** When two trigonometric forms are equivalent, the order of an n-th root of unity divides n, number of primitive n-th roots.
6. **Number theory of polynomials**
   - **D** polynomials over commutative rings, divisibility and gcd of polynomials, irreducible and primitive polynomials
   - **T** $R[x]$ is a commutative ring, in $\mathbb{F}[x]$ the following: division with remainders, existence of gcd, (extended) Euclidean algorithm, irreducibles = primes, conditions for irreducibility of low degree polynomials, fundamental theorem of number theory in $\mathbb{F}[x]$ and in particular in $\mathbb{R}[x]$ and $\mathbb{C}[x]$, decomposition to primitives and units in $\mathbb{Q}[x]$,
   - **P** Proudct of primitive polynomials is primitive, Schönemann-Eisenstein criterion
7. **Roots of polynomials**
   - **D** Connection of roots and linear factors of a polynomial, formal derivatives, cyclotomic polynomials, polynomials in n variables, symmetric polynomials, elementary symmetric polynomials
   - **T** Vieta's formulae, polynomial interpolation
   - **P** Multiple roots and formal derivatives, rational root test, $x^n - 1 = \prod_{d|n} \Phi_d$

8. **Systems of linear equations**

   D systems of linear equations (SLE), matrix and augmented matrix of a SLE, elementary row operations, row echelon form and reduced row echelon form, pivots, free and bounded variables, $\mathcal{R}(A)$, $\mathcal{C}(A)$ and $\mathcal{N}(A)$

   T the number of solutions of a SLE, description of the solutions of a SLE with the help of $\mathcal{R}(A)$, $\mathcal{C}(A)$ and $\mathcal{N}(A)$

   P Gaussian and Gauss-Jordan elmination, connection with the rank of the matrix

9. **Vectorspaces**

   D operations in $\mathbb{F}^n$, vectorspaces, subspaces, affine subspaces, linear combinations, spanned subspaces, linear independence and dependence, generating sets, bases, dimension, coordinate vectors.

   T properties of operations in $\mathbb{F}^n$, equivalent properties of bases

   P "basis = none of the vectors is a linear combination of the others", properties of independent and generating sets, the set of solutions of an SLE forms an affine subspace

10. **Linear maps**

    D Linear maps, kernel, image, (standard) matrix of a linear map

    T Matrix of the rotations of the plane, when a linear map is injective or surjective

    P $\mathrm{Ker}(\varphi)$ and $\mathrm{Im}(\varphi)$ are subspaces, dimension theorem

11. **Matrices**

    D Operations of matrices, rank, inverse, special matrices (diagonal, triangular, permutation, elementary)

    T Properties of operations, connection between the columns of A, B and AB, rank factorization, dyadic decomposition, operations on special matrices

    P Connection of rank and matrix operations, equivalent conditions for a matrix to be invertible

12. **Determinants**

    D the determinant functions, permutations and inversions, the definition of the determinant with entries, cofactors

    T Operations of determinants, multilinearity, determinant of special matrices

    P $\det(AB) = \det(A)\det(B)$, connection between det and rk, the determinant (defined with the entries) satisfies the identities with row operations.