Outline

Fields and field extensions (6.12.14, 6.12.15)
- Degree of a field extension, multiplicativity of degree, transcendental extensions (6.12.16)
- Frobenius endomorphism (6.12.10)
- Algebraic closure: of a finite field? Of $\mathbb{Q}$? Of $\mathbb{R}$?
- Finite subgroup of multiplicative group of a field is cyclic (6.12.5, 6.12.22)
- Automorphisms of $\mathbb{F}_{p^n}$ (6.12.19)

Number theory
- Euler’s function: multiplicativity, as order of $(\mathbb{Z}/n\mathbb{Z})^*$. (6.13.20)
- Solving congruences modulo $n$ by working in the group of units modulo $n$. Euler’s theorem. Check cases. (6.13.8, 6.13.17)

Symmetric/Hermitian matrices (Linear Algebra Overflow)
- Positive (semi-)definiteness
  1. Characterization by eigenvalues (7.9.6)
  2. Characterization by factorization (7.5.34)
  3. Submatrix criterion (“Sylvester’s Criterion”) (∗)
- Sylvester’s law of interia, signature of a quadratic form
- Eigenvalues of a hermitian/symmetric/orthogonal/unitary matrix

Problems

6.12.5 Prove that a finite subgroup of the multiplicative group of a field is cyclic.

6.12.10 Let $F$ be a field of characteristic $p > 0$. If $\alpha$ is a zero of the polynomial $f(x) = x^p - x + 3$ in an extension field of $F$, show that $f(x)$ has $p$ distinct zeros in the field $F(\alpha)$.

6.12.14 Exhibit infinitely many pairwise nonisomorphic quadratic extensions of $\mathbb{Q}$ and show they are pairwise nonisomorphic.

6.12.15 Let $\mathbb{Q}$ be the field of rational numbers. For $\theta$ a real number, let $F_\theta = \mathbb{Q}(\sin \theta)$ and $E_\theta = \mathbb{Q}(\sin \theta/3)$. Show that $E_\theta$ is an extension field of $F_\theta$ and determine all possibilities for $\dim_{F_\theta} E_\theta$. (Use trigonometric identities.)

6.12.16 Show that the field $\mathbb{Q}(t_1, \ldots, t_n)$ of rational functions in $n$ variables over the rational numbers is isomorphic to a subfield of $\mathbb{R}$.

6.12.19 Let $\mathbb{F}$ be a finite field of cardinality $p^n$, with $p$ prime and $n > 0$, and let $G$ be
the group of invertible $2 \times 2$ matrices with coefficients in $F$. (1) Prove that $G$ has order $(p^{2n} - 1)(p^{2n} - p^n)$. (2) Show that any $p$-Sylow subgroup of $G$ is isomorphic to the additive group of $F$.

6.12.22 Let $p$ be a prime and $F_p$ the field of $p$ elements. How many elements of $F_p$ have square roots in $F_p$? Cube roots? (You may separate into cases for $p$.)

6.13.8 Let $n \geq 2$ be an integer such that $2^n + n^2$ is prime. Prove that

$$n \equiv 3 \mod 6.$$ 

6.13.17 Determine the rightmost decimal digit of

$$A = 17^{17^{17}}.$$ 

6.13.20 Let $\phi$ be Euler’s function. Let $a$ and $k$ be two integers, with $a > 1, k > 0$. Prove that $k$ divides $\phi(a^k - 1)$.

7.5.34 Let $A$ and $B$ be real $n \times n$ symmetric matrices with $B$ positive definite. Consider the function defined for $x \neq 0$ by $G(x) = \frac{\langle Ax, x \rangle}{\langle Bx, x \rangle}$.

- Show that $G$ attains its maximum value.
- Show that any maximum point $U$ for $G$ is an eigenvector for a certain matrix related to $A$ and $B$ and show which matrix.

7.9.6 A real symmetric $n \times n$ matrix is called positive semi-definite if $x^tAx \geq 0$ for all $x \in \mathbb{R}^n$. Prove that $A$ is positive semi-definite if and only if $\text{tr} AB \geq 0$ for every real symmetric positive semi-definite $n \times n$ matrix $B$.

(*) “Sylvester’s Criterion”: Given a symmetric matrix $A = (a_{ij})_{1 \leq i, j \leq n} \in M_n(\mathbb{R})$, let $A_k$ denote the upper left submatrix $A_k = (a_{ij})_{1 \leq i, j \leq k}$.

- Prove by induction on $n$ that $A$ is positive definite if and only if $\text{Det}(A_k) > 0$ for $k = 1, \ldots, n$.
- Prove that the analogous statement fails for positive semi-definite matrices. That is, find $n$ and $A \in M_n(\mathbb{R})$ symmetric such that $\text{Det}(A_k) \geq 0$ for all $1 \leq k \leq n$, but $v^tAv < 0$ for some $v \in \mathbb{R}^n$. 