REU APPRENTICE CLASS #9

INSTRUCTOR: LÁSZLÓ BABAI
SCRIBE: MICHAEL SMITH

Friday, July 8, 2011

1. Field Extensions

Definition 1.1. A subset $F \subseteq H$ of a field H is a *subfield* if it is a field under the operations of H, i.e., if F is closed under sums, products, negation, nonzero reciprocals, and includes the multiplicative identity element "1."

If F is a subfield of H then H is an *extension field* of F. In this case, H is a vector space over F; we call the dimension of this vectorspace the *degree* of this extension and denote it by $[H : F] = \dim_F H$. If $[H : F]$ is finite, this is a *finite extension*.

Problem 74. The only finite extensions of $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$.

Problem 75. Find a field extension F of $\mathbb{Q}$ with $[F : \mathbb{Q}] = 10$.

Problem 76. Suppose $K \subseteq L \subseteq H$ are field extensions. Prove that $[H : K] = [H : L] \cdot [L : K]$.

Definition 1.2. Suppose $F \subseteq H$ is a field extension, and $\alpha \in H$. We say that α is *algebraic* over F if there is an $f \in F[x]$, $f \neq 0$, such that $f(\alpha) = 0$.

Definition 1.3. If $\alpha \in \mathbb{C}$, and α is algebraic over $\mathbb{Q}$, we say that α is an *algebraic number.*

Exercise 1.4. $\sqrt{2} + \sqrt{3}$ is algebraic.

Problem 77. The algebraic numbers form a field.

Definition 1.5. A polynomial $f \in F[x]$ is *irreducible* over F if $\deg f \geq 1$ and f cannot be factored into polynomials (in $F[x]$) of smaller degree.

Theorem 1.6 (Division Theorem)**.** *For all $a, b \in \mathbb{Z}$, $b \neq 0$, there exist $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$ and $a = bq + r$.*

Theorem 1.7 (Division Theorem for Polynomials)**.** *For all $f, g \in F[x]$, $g \neq 0$, there exist $q, r \in F[x]$ such that $\deg r < \deg g$ and $f = gq + r$.*

Corollary 1.8. *For all $f \in F[x]$ and $\alpha \in F$, there exists $q \in F[x]$ such $f(x) = (x - \alpha)q(x) + f(\alpha)$.*

Proof: apply the Division Theorem with $g = x - \alpha$. Then r must be a constant. Setteing $x = \alpha$ we find that this constant is $f(\alpha)$ because $f(\alpha) = (\alpha - \alpha)q + r = r$.

Corollary 1.9. *$f(\alpha) = 0$ if and only if $x - \alpha \mid f$.*

Corollary 1.10. *If $\alpha_1, \ldots, \alpha_n$ are distinct roots of f, then $f(x) = (x - \alpha_1) \ldots (x - \alpha_n)s(x)$ for some $s \in F[x]$.*

Corollary 1.11. *If a polynomial has degree $n \geq 0$, it cannot have more than n distinct roots.*

Corollary 1.12. *If $f, g \in F[x]$ with $\deg f, \deg g \leq n$, and there are $n + 1$ distinct elements $\alpha_0, \ldots, \alpha_n$ of F with $f(\alpha_i) = g(\alpha_i)$ for $i = 0, \ldots, n$, then $f = g$.*

Corollary 1.13. *If F is infinite, and f, g are two polynomials over F for which the corresponding functions $\tilde{f}, \tilde{g} \colon F \to F$ agree, then $f = g$.*

Definition 1.14. If α is algebraic over F, the *minimal polynomial* of α is the nonzero monic $g \in F[x]$ of smallest degree such that $g(\alpha) = 0$. Denote this polynomial by $m_\alpha(x)$.

Theorem 1.15. *For all $f \in F[x]$, $f(\alpha) = 0$ if and only if $m_\alpha \mid f$.*

Corollary 1.16. *Minimal polynomials are unique.*

Problem 78. If α is algebraic over F, the minimal polynomial is irreducible over F.

Definition 1.17. If α is algebraic over F, define $\deg_F(\alpha) = \deg(m_\alpha)$.

Definition 1.18. Suppose $F \subseteq H$ is a field extension, and $\alpha \in H$. $F(\alpha)$ denotes the smallest subfield of H containing F and α.

Problem 79. $F(\alpha)$ exists and is unique. (Lemma: Any intersection of subfields is a subfield.)

Notation 1.19. We write $F[\alpha]$ for the set $\{f(\alpha) \mid f \in F[x]\}$.

Problem 80. If α is algebraic, then $F(\alpha) = F[\alpha]$, and $[F(\alpha) : F] = \deg_F(\alpha)$.

Problem 81. Corollary: If H is a finite extension of F, then every $\alpha \in H$ is algebraic, and if $\alpha \in H$, then $\deg_F(\alpha) \mid [H : F]$.

Problem 82 (Doubling the cube: The Delian Problem)**.** $\sqrt[3]{2}$ cannot be constructed by straightedge and compass.

2. Determinants

Notation 2.1. We write $M_n(F)$ for the space $F^{n\times n}$ of $n \times n$ square matrices over F. Recall that S_n is the group of all permutations of the set $[n] = \{1, \dots, n\}$.

Definition 2.2. The *determinant* of a matrix $A = (a_{ij}) \in M_n(F)$ is

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Observation 2.3. The determinant of a diagonal (or upper triangular) matrix is the product of the entries on the diagonal.

Problem 83. $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$

Observation 2.4 (Properties of the Determinant)**.**

- $\det(A^T) = \det A$.
- If any column of A is zero, $\det A = 0$.
- Denote the matrix obtained by permuting the columns of the matrix A by the permutation π by A^π. Then $\det(A^\pi) = \operatorname{sgn}(\pi) \det A$.
- If two columns of A are equal, then $\det A = 0$.

Problem 84. Prove (over an arbitrary field, including fields of characteristic 2) that if two columns of A are equal, then $\det A = 0$.

Definition 2.5. Let $A \in M_n(F)$, $i \neq j$, and $\lambda \in F$. Writing the columns of A as

$$A = \left[a_1, \dots, a_n\right]$$

the matrix

$$A' = \left[a_1, \dots, a_{i-1}, a_i - \lambda a_j, a_{i+1}, \cdots, a_n\right]$$

is obtained from A by an *elementary column operation.*

Theorem 2.6. *If A' is obtained from A by an elementary column operation, then* $\det A = \det A'$.

Theorem 2.7. *The determinant of A is zero if and only if the columns of A are linearly dependent.*

Theorem 2.8. *Let $A \in M_n(F)$. Then* $\operatorname{rk}(A) = n$ *if and only if* $\det A \neq 0$.

Problem 85. Theorem: Let A be an $n \times m$ matrix. Prove: $\operatorname{rk}(A)$ is the largest r such that A has an $r \times r$ submatrix with nonzero determinant.

Definition 2.9. We say that $A \in M_n(F)$ is *nonsingular* if $\det A \neq 0$, and *singular* if $\det A = 0$.

Definition 2.10. Let $A \in F^{k\times n}$. We say that $B \in F^{n\times k}$ is a *right inverse* of A if $AB = I_k$, and a *left inverse* of A if $BA = I_n$.

Problem 86. Let $A \in F^{k\times n}$. Show that A has a right inverse if and only if A has full row-rank, i.e., $\mathrm{rk}(A) = k$. Similarly, show that A has a left inverse if and only if A has full column rank, i.e., $\mathrm{rk}(A) = n$.

Observation 2.11. If $A \in M_n(F)$ has a right inverse B and a left inverse C, then $B = C$.

Problem 87. If $k \neq n$, $|F| = \infty$, and A has a right inverse, then A has infinitely many right inverses.

Corollary 2.12. *If $A \in M_n(F)$ has a right inverse, this right inverse is unique.*

Theorem 2.13. *For a square matrix $A \in M_n(F)$, the following are equivalent:*

- *A is nonsingular.*
- $\det A \neq 0$.
- $\mathrm{rk}\, A = n$.
- *The columns of A are linearly independent.*
- *The columns of A span F^n.*
- *The rows of A are linearly independent.*
- *The rows of A span F^n.*
- *A has a right inverse.*
- *A has a left inverse.*
- *A has a two-sided inverse.*
- *The nullity of A is zero.*
- *The system of homogenous equations $Ax = 0$ has only the trivial solution.*
- *For all $b \in F^n$, the system $Ax = b$ has a solution.*
- *For all $b \in F^n$, the system $Ax = b$ has a unique solution.*
- *For all $b \in F^n$, the system $Ax = b$ has at most one solution.*

Problem 88. Give a simple explicit formula for

$$\det \begin{pmatrix} a & b & b & \dots & b & b & b \\ b & a & b & \dots & b & b & b \\ b & b & a & \dots & b & b & b \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ b & b & b & \dots & a & b & b \\ b & b & b & \dots & b & a & b \\ b & b & b & \dots & b & b & a \end{pmatrix}.$$

The resulting expression should be completely factored.

Problem 89. Let $x_1, \dots, x_n \in F$, and define the Vandermonde matrix

$$V(x_1, \dots, x_n) = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix}.$$

Show that

$$\det V(x_1, \dots, x_n) = \prod_{i<j} (x_j - x_i)$$

Problem 90. What is

$$\det \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ -1 & 1 & 1 & \dots & 0 & 0 & 0 \\ 0 & -1 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 & 0 \\ 0 & 0 & 0 & \dots & -1 & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & -1 & 1 \end{pmatrix} \quad ?$$