# REU APPRENTICE CLASS \#11 

INSTRUCTOR: LÁSZLÓ BABAI<br>SCRIBE: MARKUS KLIEGL

Tuesday, July 12, 2011

## 1. Changing Basis

Definition 1.1. Given two bases $\mathbf{b}=\left(b_{1}, \ldots, b_{n}\right)$ (the old basis) and $\mathbf{b}^{\prime}=\left(b_{1}^{\prime}, \ldots, b_{n}^{\prime}\right)$ (the new basis), define the basis change transformation $\sigma: V \rightarrow V$ by

$$
\sigma\left(b_{i}\right):=b_{i}^{\prime} .
$$

Note that this transformation is invertible (why?). Define also the corresponding matrix

$$
[\sigma]_{\text {old }}:=\left[\left[\sigma\left(b_{1}\right)\right]_{\text {old }}, \ldots,\left[\sigma\left(b_{n}\right)\right]_{\text {old }}\right]=\left[b_{1}^{\prime}, \ldots, b_{n}^{\prime}\right]_{\text {old }}=\mathbf{b}_{\text {old }}^{\prime},
$$

where $[v]_{\text {old }}$ denotes the coordinate vector of $v$ with respect to the old basis. More explicitly, if

$$
v=\sum_{i=1}^{n} \alpha_{i} b_{i}=\sum_{i=1}^{n} \alpha_{i}^{\prime} b_{i}^{\prime},
$$

then

$$
[v]_{\mathrm{old}}=\left(\begin{array}{c}
\alpha_{1} \\
\vdots \\
\alpha_{n}
\end{array}\right), \quad[v]_{\mathrm{new}}=\left(\begin{array}{c}
\alpha_{1}^{\prime} \\
\vdots \\
\alpha_{n}^{\prime}
\end{array}\right)
$$

Theorem 1.2. The coordinates of a vector $v$ with respect to the old and new bases are related by

$$
[v]_{\text {old }}=[\sigma]_{\text {old }} \cdot[v]_{\text {new }} .
$$

Recall that given a linear map $\phi: V \rightarrow W$ and bases $\mathbf{e}$ for $V$ and $\mathbf{f}$ for $W$, respectively, we denote by $[\phi]_{\mathbf{e}, \mathbf{f}}$ the matrix for $\phi$ relative to the bases $\mathbf{e}$ and $\mathbf{f}$. The $j$-th column of this matrix is $\left[\phi\left(e_{j}\right)\right]_{\mathbf{f}}$. Recall further the fundamental relation this notation establishes between matrix multiplication and the action of a linear transformation:

$$
[\phi(v)]_{\mathbf{f}}=[\phi]_{\mathbf{e}, \mathbf{f}} \cdot[v]_{\mathbf{e}} \quad \text { for all } v \in V .
$$

Theorem 1.3. Let $\phi: V \rightarrow W$ be a linear function, and let $\sigma: V \rightarrow V, \mathbf{e} \mapsto \mathbf{e}^{\prime}$ and $\tau: W \rightarrow W, \mathbf{f} \mapsto \mathbf{f}^{\prime}$ be basis change transformations. Writing

$$
\begin{aligned}
A & :=[\phi]_{\mathrm{old}}=[\phi]_{\mathbf{e}, \mathbf{f}}, \\
A^{\prime} & :=[\phi]_{\mathrm{new}}=[\phi]_{\mathbf{e}^{\prime}, \mathbf{f}^{\prime}}, \\
S & :=[\sigma]_{\mathrm{old}}, \\
T & :=[\tau]_{\mathrm{old}},
\end{aligned}
$$

we have

$$
A^{\prime}=T^{-1} A S
$$

That is,

$$
[\phi]_{\text {new }}=[\tau]_{\text {old }}^{-1} \cdot[\phi]_{\text {old }} \cdot[\sigma]_{\text {old }} .
$$

Corollary 1.4. In the special case $V=W$ and $\sigma=\tau$, we have

$$
[\phi]_{\text {new }}=S^{-1} \cdot[\phi]_{\text {old }} \cdot S
$$

In particular, taking $\phi=\sigma$, we find

$$
[\sigma]_{\text {new }}:=S^{-1} S S=S=[\sigma]_{\text {old }} .
$$

Thus,

$$
S=\left[\mathbf{e}^{\prime}\right]_{\mathbf{e}}, \quad S^{-1}=[\mathbf{e}]_{\mathbf{e}^{\prime}} .
$$

Definition 1.5. $A, B \in M_{n}(F)$ are similar if there exist $S, S^{-1} \in M_{n}(F)$ such that $B=S^{-1} A S$. If $A$ and $B$ are similar, we write $A \sim B$.

Exercise 1.6. This is an equivalence relation.
Observation 1.7. $A, B$ describe the same linear transformation with respect to some bases if and only if $A \sim B$.

Exercise 1.8. If $A \sim B$, then $\operatorname{rk}(A)=\operatorname{rk}(B), \operatorname{tr}(A)=\operatorname{tr}(B)$, and $\operatorname{det}(A)=\operatorname{det}(B)$.
This shows that we can define the rank, trace, and determinant of a linear transformation as the corresponding quantity of the matrix that describes our linear transformation in some basis. These concepts are well-defined, i.e., they depend only on the linear transformation and not on the choice if the basis. A major theme in linear algebra is consequently to understand matrices up to equivalence.

Exercise 1.9 (!). For a linear map $\phi: V \rightarrow W$ we define $\operatorname{rk}(\phi):=\operatorname{dim} \operatorname{im}(\phi)$. Let e be a basis of $V$ and f is a basis of $W$. Set $A=[\phi]_{\mathrm{e}, \mathrm{f}}$. Prove:

$$
\operatorname{rk}(A)=\operatorname{rk}(\phi)
$$

In particular, $\operatorname{rk}(A)$ does not depend on the choice of the bases $\mathrm{e}, \mathrm{f}$.
Recall that the rank-nullity theorem asserts

$$
\underbrace{\operatorname{dim}(\operatorname{ker} \phi)}_{\text {nullity }}+\underbrace{\operatorname{dim}(\operatorname{im} \phi)}_{\text {rank }}=\operatorname{dim}(V) .
$$

## 2. Euler's $\varphi$ Function

Definition 2.1. Euler's $\varphi$ function is the function

$$
\varphi(n):=|\{i \mid 1 \leq i \leq n, \operatorname{gcd}(i, n)=1\}| .
$$

Problem 102. Prove that $\varphi(n)$ is equal to the number of primitive $n$-th roots of unity.
Problem 103. Show that for the matrix

$$
D_{n}=(\operatorname{gcd}(i, j))_{1 \leq i, j \leq n}
$$

we have

$$
\operatorname{det}\left(D_{n}\right)=\prod_{i=1}^{n} \varphi(i)
$$

Hint: Find an upper-triangular ( 0,1 )-matrix $Z$ such that

$$
D_{n}=Z^{T}\left(\begin{array}{ccc}
\varphi(1) & & 0 \\
& \ddots & \\
0 & & \varphi(n)
\end{array}\right) Z
$$

## 3. Eigenvalues, Eigenvectors, the Characteristic Polynomial

Definition 3.1. If $\phi: V \rightarrow V$ is a linear transformation, we say $v \in V$ is an eigenvector to the eigenvalue $\lambda \in F$ if $v \neq 0$ and $\phi(v)=\lambda v$.
Definition 3.2. If $A \in M_{n}(F)$, then $v \in F^{n}$ is an eigenvector to eigenvalue $\lambda \in F$ if $v \neq 0$ and $A v=\lambda v$.
Definition 3.3. $v$ is an eigenvector of $\phi$ if $v \neq 0$ and there exists $\lambda \in F$ such that $\phi(v)=\lambda v$. Similarly for matrices.

Definition 3.4. $\lambda \in F$ is an eigenvalue of $\phi$ if there exists $v \neq 0$ such that $\phi(v)=\lambda v$. Similarly for matrices.
Observation 3.5. $v \in V$ is an eigenvector of $\phi: V \rightarrow V$ to eigenvalue $\lambda$ if and only if $[v]_{\mathbf{b}}$ is an eigenvector of $[\phi]_{\mathbf{b}}$.

Exercise 3.6. For any $\lambda \in F$ the set

$$
U_{\lambda}=\left\{x \in F^{n} \mid A x=\lambda x\right\}=\operatorname{ker}(\lambda I-A)
$$

is a linear subspace. The nonzero elements of $U_{\lambda}$ are precisely the eigenvectors of $A$ to eigenvalue $\lambda$. So $\lambda$ is an eigenvalue of $A$ precisely if $\operatorname{dim}\left(U_{\lambda}\right) \geq 1$.
Observation 3.7. By the rank-nullity theorem, we have

$$
\operatorname{dim} U_{\lambda}=n-\operatorname{rk}(\lambda I-A)
$$

Theorem 3.8. The following are equivalent:
(1) $\lambda$ is an eigenvalue of $A \in M_{n}(F)$
(2) $\operatorname{dim} U_{\lambda} \geq 1$
(3) $\operatorname{rk}(\lambda I-A)<n$
(4) $\lambda I-A$ is singular
(5) $\operatorname{det}(\lambda I-A)=0$

Let us state the last equivalence as a separate theorem to emphasize it; for that is how we usually detect eigenvalues.
Theorem 3.9. $\lambda$ is an eigenvalue of $A$ if and only if $\operatorname{det}(\lambda I-A)=0$.
Definition 3.10. $f_{A}(t)=\operatorname{det}(t I-A)$ is called the characteristic polynomial of $A$.
Observation 3.11. $\lambda$ is an eigenvalue of $A$ if and only if $f_{A}(\lambda)=0$.
Observation 3.12. If $A \in M_{n}(F)$, then $f_{A}$ is a polynomial in $t$ of degree $n$. So we may write

$$
f_{A}(t)=a_{n} t^{n}+a_{n-1} t^{n-1}+\cdots+a_{0}
$$

From the definition of $f_{A}$, one may easily compute $a_{n}=1$, $a_{n-1}=-\operatorname{tr}(A)$, and $a_{0}=(-1)^{n} \operatorname{det}(A)$.
Theorem 3.13. Over $\mathbb{C}$, we may factor

$$
\begin{equation*}
f_{A}(t)=\left(t-\lambda_{1}\right) \cdots\left(t-\lambda_{n}\right) \tag{1}
\end{equation*}
$$

where $\lambda_{1}, \ldots, \lambda_{n}$ are the eigenvalues of $A$ (not necessarily distinct here). It follows that

$$
\operatorname{tr}(A)=\sum_{i=1}^{n} \lambda_{i}
$$

and

$$
\operatorname{det}(A)=\prod_{i=1}^{n} \lambda_{i}
$$

Definition 3.14. The algebraic mulitplicity of an eigenvalue $\lambda$ is the number of times the factor $(t-\lambda)$ occurs in the factorization (1).

Definition 3.15. The geometric multiplicity of an eigenvalue $\lambda$ is $\operatorname{dim} U_{\lambda}=n-\operatorname{rk}(\lambda I-A)$. This is the number of linearly independent eigenvectors to eigenvalue $\lambda$.

Problem 104. For all $A \in M_{n}(\mathbb{C})$ and for all $\lambda \in \mathbb{C}$, we have

$$
\text { algebraic multiplicity of } \lambda \geq \text { geometric multiplicity of } \lambda \text {. }
$$

Problem 105. If $A \sim B$, then $f_{A}(t)=f_{B}(t)$.
Problem 106. The converse to Problem 105 is false. Hint: Find $A, B$ such that $\operatorname{rk}(A) \neq \operatorname{rk}(B)$ but $f_{A}(t)=f_{B}(t)$.
Problem 107. (a) Consider the matrices

$$
A=\left(\begin{array}{ll}
2 & 7 \\
0 & 3
\end{array}\right), \quad B=\left(\begin{array}{ll}
2 & 0 \\
0 & 3
\end{array}\right)
$$

Note that their characteristic polynomials are equal. (Why?) Are these two matrices similar?
(b) Same question for the matrices

$$
A=\left(\begin{array}{ll}
2 & 7 \\
0 & 2
\end{array}\right), \quad B=\left(\begin{array}{ll}
2 & 0 \\
0 & 2
\end{array}\right)
$$

Definition 3.16. A matrix $A$ is diagonalizable if $A$ is similar to a diagonal matrix, that is, there exist $S, S^{-1}$ such that $S^{-1} A S$ is diagonal.

Definition 3.17. An eigenbasis for $\phi$ is a basis consisting of eigenvectors of $\phi$.
Exercise 3.18. The matrix $[\phi]_{\mathbf{b}}$ is diagonal if and only if $\mathbf{b}$ is an eigenbasis for the linear transformation $\phi$.
Theorem 3.19. (a) $[\phi]_{\mathbf{b}}$ is diagonalizable if and only if there exists an eigenbasis for $\phi$.
(b) $A \in M_{n}(F)$ is diagonalizable if and only if there exists an eigenbasis for $A$.

Problem 108. Prove that $\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$ is not diagonalizable.
Problem 109. Over $\mathbb{C}$, a matrix $A$ is diagonalizable if and only if for all eigenvalues $\lambda$ of $A$, we have alg.mult. $(\lambda)=$ geom.mult. $(\lambda)$.

