Lecture 3

Invariant Factors

Let \( R \) be a commutative principal ideal ring, for example, \( \mathbb{Z} \) (the usual integers) or \( \mathbb{F}[\lambda] \), the polynomials in indeterminate \( \lambda \) with coefficients in a field \( \mathbb{F} \). We shall work with matrices over \( R \). The applications of matrix theory over \( R \) to number theory usually arise from the case \( R = \mathbb{Z} \), and the applications to control theory from the case \( R = \mathbb{F}(\lambda) \).

Let \( A \) be a matrix over \( R \). Then by elementary unimodular operations on rows and columns \( A \) may be brought to a diagonal form

\[
\text{diag}(s_1, s_2, \ldots)
\]

in which \( s_1|s_2|\ldots \), where \( | \) is the usual symbol for divisibility. The diagonal elements are unique to within multiplication by units, and are called the invariant factors of \( A \). When the invariant factors are written as products of powers of primes, the resulting prime powers are called the elementary divisors of \( A \). Again, they are uniquely determined by \( A \) to within multiplication by units.

The diagonal form \( \text{diag}(s_1, s_2, \ldots) \) is usually called the Smith form of \( A \). It is convenient to allow zero or negative subscripts by setting \( s_i = 1 \) if \( i \leq 0 \). It is also convenient to permit arbitrarily large positive subscripts by setting \( s_i = 0 \) for \( i > \min(m,n) \), when \( A \) is \( m \times n \).

Thus, there exist unimodular matrices \( U \) and \( V \) over \( R \) such that \( B = UAV \) if and only if \( A \) and \( B \) have the same Smith form, that is, the same invariant factors. (H J S Smith, 1861.)

A question of some interest, which has intrigued me since I first learned about invariant factors as an undergraduate, is: how do they change under algebraic operations on matrices? The algebraic operations in mind are the simplest ones possible: addition of matrices, multiplication of matrices, passage to a submatrix.

We do not assume that \( A \) is square. There are considerable advantages to be obtained by including the rectangular case, particularly the capacity to use proof by induction, since it is then possible to move from small matrices to large ones by adding rows.
and/or columns one at a time. Of course, in the rectangular case the main diagonal of diagonalized $A$ may not reach the lower right corner element of $A$.

In undergraduate linear algebra, one usually studies similarity, and there the crucial fact underlying the entire theory is that matrices $A$ and $B$ over a field $\mathcal{F}$ are similar, that is, $B = SAS^{-1}$ for some matrix $S$ with entries in $\mathcal{F}$, if and only if the polynomial matrices $\lambda I - A$ and $\lambda I - B$ have the same invariant factors, that is, the same Smith form when regarded as matrices in $\mathcal{F}(\lambda)$. (Here the matrices must be square.) This theorem appears to go back to Weierstrass. However, when studying invariants for similarity we are forced to restrict attention to square matrices, and this may make induction proofs more difficult to carry through.

A first question is: how do the invariant factors of matrices over $\mathcal{R}$ change if a (rectangular) matrix is augmented by one row? Let

$$B = \begin{pmatrix} A \\ x \end{pmatrix},$$

where $A$ is regarded as having fixed invariant factors, $x$ is a variable single row with entries in $\mathcal{R}$, and we want to know what invariant factors $B$ may have. No generality is lost by taking $A$ diagonal, and then a relatively easy proof shows that the invariant factors of $A$ and $B$ relate by interlacing:

$$s_1(B)ls_1(A)ls_2(B)ls_2(A)l...$$

Moreover, an easy but not quite obvious construction shows that, given invariant factors for $A$, and given invariant factors for $B$, with the interlacing condition satisfied, it is always possible to choose the single row $x$ so that $A$ and $B$ have these prescribed invariant factors.

In slightly different language, this theorem appears in Bourbaki (Commutative Algebra), and I am told the theorem is due to Chatelet, but I have never located the exact reference, in spite of a search of as much of Chatelet's material as I could locate.

Now, one can prolong this theorem, and ask about the effect of multiple row adjunctions (or column adjunctions). The easily obtained result is: if $k$ rows and/or columns are added to $A$ to get $B$, then the relation between the invariant factors of $A$ and $B$ is:
\[ s_i(B) | s_i(A) | s_{i+k}(B), \]

for all \( i \). Moreover, if proposed invariant factors are given for \( A \) and \( B \), satisfying this condition, it always is possible to choose \( A \) and the adjoined rows and columns to get \( B \) so that \( A \) and \( B \) have these prescribed invariant factors.

This is for matrices with elements in \( \mathbb{R} \). It would appear that this theorem completely answers all reasonable questions concerning the behaviour of invariant factors. Actually, it's merely a start, and there are a lot more questions.

Here is one. Let \( A \) and \( C \) be square, with \( A \) the leading northwest corner of \( C \), and the call the southeast corner \( B \):

\[ C = \begin{pmatrix} AX \\ YB \end{pmatrix}. \]

The above theorem tells us how the invariant factors of \( A \) and \( C \) relate, permitted free choice of \( X, Y, B \). It likewise tells us how the invariant factors of \( B \) and \( C \) relate, permitted free choice of \( X, Y, A \). However, if one is to fix the invariant factors of \( A, B, C \), and permit free choice only in \( X \) and \( Y \), further conditions are naturally to be expected. Now, here is a surprise: There are no further conditions. So the necessary and sufficient conditions for the existence of complementary principal blocks \( A, B \) in \( C \), with \( A, B, C \) all having prescribed invariant factors, is that the interlacing type conditions of Chatelet's theorem hold for the invariant factors of \( A \) and \( C \), and also hold for the invariant factors of \( B \) and \( C \).

The sufficiency part of the proof now is much more delicate, though. This theorem is due to me.

Often problems involving three matrices are difficult, as we shall see later. Usually necessary conditions can be derived reasonably easily, but sufficiency proofs tend to be hard. It is surprising that this one has such a simple answer, and with a still reasonable (though delicate) sufficiency proof.

Many further types of similar questions, in which certain of \( A, B, X, Y, C \) are prescribed, and the rest to be chosen, have been studied by the very capable group in Portugal and Spain led by G. N. de Oliveira.

A next natural question is about sums. As a logical analogue of the last theorem, we ask about the invariant factors of a matrix when a rank one matrix is added to it:
B = A + X,

where X is a variable rank one matrix, and we want to relate the invariant factors of A and B. Remember that we are still working with matrices over \( \mathbb{R} \). Once again, there is a fairly easy theorem, expressed as two chains of divisibility relations:

\[
s_1(A)l s_2(B)l s_3(A)l s_4(B)l \ldots,
\]

\[
s_1(B)l s_2(A)l s_3(B)l s_4(A)l \ldots.
\]

These are necessary and sufficient conditions for the existence of matrices A, B with prescribed invariant factors such that one of the matrices is the other plus a rank (at most) one matrix.

Now, what can we say when we consider the three parts of a sum? In spite of the relative ease of the theorem above on complementary submatrices in a full matrix, it is to be expected that theorems involving three matrices are more difficult than those involving only two.

Specifically, what can we say about the invariant factors of A, B, C when C = A + B? Of course, the matrices are all now of the same shape. This seems to be a quite hard problem. However, there is something easy that can be proved.

We have

\[
A = U_1 D_A V_1,
\]

where \( U_1 \) and \( V_1 \) are unimodular, and \( D_A \) is the diagonal matrix of invariant factors of A:

\[
D_A = \text{diag}(s_1(A), s_2(A), \ldots).
\]

Also, let \( B = U_2 D_B V_2 \) where \( U_2, V_2 \) are unimodular, and \( D_B \) is diagonal, built from the invariant factors of B.

Now let

\[
D = \text{diag}(s_1(A), s_2(A), \ldots, s_1(B), s_2(B), \ldots)
\]

This matrix has twice as many rows (and twice as many columns) as A and B have. Consider the matrix M given by:
\[ M = \begin{pmatrix} U_1 & U_2 \\ 0 & I \end{pmatrix} \begin{pmatrix} D & A \\ 0 & DB \end{pmatrix} \begin{pmatrix} V_1 & 0 \\ V_2 & I \end{pmatrix} \]

The matrix in the middle is \( D \), and \( M \) has the same invariant factors as \( D \). The leading block in \( M \) is

\[ M_{11} = U_1 D A V_1 + U_2 D B V_2 = C. \]

Thus \( C \) is a principal \( n \times n \) block in a \( 2n \times 2n \) matrix \( M \) having the same invariant factors as \( D \). So Chatelet's divisibility relations connect the invariant factors of \( C \) and \( D \). But \( D \) is diagonal and so its invariant factors can be directly estimated. As a result, we obtain this theorem:

**Theorem.** The invariant factors of \( A, B, \) and \( C = A + B \) satisfy

\[ \gcd(s_i(A), s_j(B)) \mid s_{i+j-1}(C) \]

for all choices of indices \( i \) and \( j \). Here \( \gcd \) means "greatest common divisor".

This is very much like the Weyl inequality for the eigenvalues of a sum of Hermitian matrices (with complex number entries), and the Fan inequality for the singular values of a product of arbitrary (complex) matrices. The Weyl inequality is: Let \( A, B, C = A + B \) be Hermitian matrices with eigenvalues \( \alpha_1 \geq \alpha_2 \geq \alpha_3 \geq \ldots, \beta_1 \geq \beta_2 \geq \beta_3 \geq \ldots, \gamma_1 \geq \gamma_2 \geq \gamma_3 \geq \ldots \). Then

\[ \gamma_{i+j-1} \leq \alpha_i + \beta_j. \]

If we change \( A, B, C = A + B \) to general complex matrices (not necessarily Hermitian), and change eigenvalues to singular values, the same inequality holds (Fan's theorem.) The subscript \( i+j-1 \) is the minimal one for which these theorem(s) hold. Note that in this part of the discussion, we discuss matrices with complex entries, not matrices over \( \mathbb{R} \).

Now, there are many other inequalities for the eigenvalues of a sum of Hermitian matrices. So, one might expect many other inequalities for the invariant factors of a sum of integral matrices. But every other inequality suggested by the Hermitian case turns out to be false for the invariant factor case. However, there is another
fact that is true for the invariant factors of a sum: If \( s_1(A) = 0 \), then
A is the zero matrix, hence \( B \equiv C \pmod{s_1(A)} \), and therefore

\[
\det B = \det C \pmod{s_1(A)}.
\]

So this is an additional condition for a sum of matrices over \( \mathcal{R} \).

Now \( C = A + B \) can be rewritten in two other ways: \( A = C - B \), and \( B = C - A \), and the conditions so far developed must hold in these two other situations.

Thus we have necessary conditions for the invariant factors of a sum of integral matrices, namely, the greatest common divisor and the determinantal congruence conditions. Are they sufficient?

I settled the 2x2 and 3x3 cases. Both are rather intricate calculations. In the 3x3 case we have 21 conditions. Let me explain. Changing the notation, call the invariant factors

\[
a_1a_2a_3, \ b_1b_2b_3, \ c_1c_2c_3.
\]

The 21 conditions are:

\[
(a_1b_1)c_1, \ (a_1b_2)c_2, \ (a_2b_1)c_2, \ (a_1b_3)c_3, \ (a_2b_2)c_3, \ (a_3b_1)c_3,
\]

\[
c_1c_2c_3 = a_1a_2a_3 \pmod{b_1},
\]

together with these conditions in which a, b, and c are cyclically permuted (and a minus sign introduced in the permuted determinantal conditions.) The result I obtained is that these 21 conditions are necessary and sufficient to describe the behaviour of the invariant factors of a sum of matrices over \( \mathcal{R} \).

I started to work on the 4x4 case, but got tired of the problem. So further progress is still awaited.

An accurate description of this problem for the invariant factors of a sum is that it is a hard diophantine problem. We are dealing with the solvability of a large family of polynomial type divisibility conditions, and it is necessary to exhibit a solution, and to compound the difficulty, we work over a ring, not a field.

It would be nice if an abstract formulation of this problem could be found, say in terms of \( \mathcal{R} \) modules. But I know of no such formulation.
Now we turn to the issue of the invariant factors of a product of \( R \) matrices. Here there is a beautiful and most natural abstract formulation, which turns out to be important in control theory and in finite abelian groups. (Special cases of it may be found in the Gohberg, Lancaster, Rodman books, and elsewhere.)

We consider finitely generated modules over the ring \( R \). Recall that a module is just a vector space in which the scalars come from a ring, not a field. Finitely generated means there is a finite number of elements whose linear combinations fill out the module.

One learns in introductory algebra that such a module \( M \) is a direct sum of cyclic modules. This means: there are independent elements such that every element is an \( R \) linear combination of these independent elements. The linear combination giving a specific element is unique, but the scalar multiplier on a basis element isn't since there may be torsion: we may have \( rm = 0 \) for a ring element \( r \) and a module element \( m \) without \( r \) being zero. Indeed, this is the most important case. So, one defines the order ideals of the cyclic submodules: these are ideals in \( R \) annihilating the generators of the independent cyclic direct summands.

The basis theorem now says that it is possible to decompose the module \( M \) as a direct sum of cyclic modules such that the order ideals of the individual direct summands form a divisibility chain. Then take a generator for each of the order ideals. These generators are called the invariant factors of the module.

Thus \( M = \langle m_1 \rangle \oplus \langle m_2 \rangle \oplus \ldots \), where the elements of \( R \) annihilating \( m_1 \) are all multiples of an element \( s_1 \), the elements of \( R \) annihilating \( m_2 \) are all multiples of an element \( s_2 \), etc., and \( s_1 | s_2 | \ldots \).

The symbol \( \langle m_1 \rangle \) denotes the cyclic module generated by \( m_1 \), that is, all linear combinations of \( m_1 \) by elements of \( R \).

Now a basic (and still reasonably elementary fact) is that there exist nonsingular \( R \) matrices \( A, B, C = AB \) with prescribed invariant factors if and only if there exist \( R \) modules \( A, B, C \), with \( A \) a submodule of \( C \) and \( B = C/A \), with \( A, B, \) and \( C \) having the same prescribed invariant factors as the matrices \( A, B, \) and \( C = AB \).

Furthermore, a basic fact about modules over principal ideal domains is that the modules decompose as direct sums of \( p \) modules, where \( p \) ranges over the primes in \( R \). This is the module theoretic version of the Sylow theorems of group theory, and especially of the Sylow theorems for finite abelian groups. This decomposition applies to all parts \( A, B, \) and \( C \) in \( B = C/A \). Therefore the module theoretic study of \( B = C/A \) reduces to the case of \( p \) modules, where \( p \)
is a prime. For matrices, $A, B, C = AB$ this means that we study elementary divisors for each fixed prime $p$, and not invariant factors.

We are therefore interested in a torsion $p$ module $C$, where $p$ is a prime, containing a submodule $A$ with quotient $B = C/A$. Torsion means that any element of $C$ is annihilated by some power of $p$. In this situation we wish to study the relationship between the invariant factors of $C$, of $A$, and of the quotient $B = C/A$. The connection between the module invariants of these three $p$-modules was first raised by the group theorist P. Hall in the 1950's, who gave one lecture on it at a Banff conference, but published nothing on it. The one lecture revealed a connection with the algebra of symmetric polynomials. Definitive results were obtained by T. Klein. I now describe Klein's results.

First, introduce new notation. Since $C$ is a $p$ module, the invariant factors of all of $A$, $B$, $C$ are powers of $p$, so let them be

for $A$: $p^{\alpha_1}, p^{\alpha_2}, ..., p^{\alpha_n}, \alpha_1 \geq \alpha_2 \geq ... \geq \alpha_n \geq 0$,

for $B$: $p^{\beta_1}, p^{\beta_2}, ..., p^{\beta_n}, \beta_1 \geq \beta_2 \geq ... \geq \beta_n \geq 0$,

for $C$: $p^{\gamma_1}, p^{\gamma_2}, ..., p^{\gamma_n}, \gamma_1 \geq \gamma_2 \geq ... \geq \gamma_n \geq 0$.

Then Klein's theorem is that the module, submodule, and quotient module exist with these prescribed invariant factors if and only if the exponents satisfy the following very combinatorial conditions:

There exists a tableau (a rectangular matrix) of numbers $\sigma_{ij}$,

$$
\begin{pmatrix}
\sigma_{01} & \sigma_{02} & ... & \sigma_{0n} \\
\sigma_{11} & \sigma_{12} & ... & \sigma_{1n} \\
. & . & . & . \\
\sigma_{r1} & \sigma_{r2} & ... & \sigma_{rn}
\end{pmatrix}
$$

in which the entries are nonnegative integers meeting certain conditions:

(i) Each row is weakly decreasing when read from left to right.
(ii) Each column is weakly increasing when read from top to bottom.

(iii) The top row is $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$.

(iv) The bottom row is $\gamma = (\gamma_1, \gamma_2, ..., \gamma_n)$.

(v) When read down a column the entries remain constant or increase in steps of 1 only.

(vi) Draw a vertical line down the array separating a pair of columns, and for each row compute its increase over the previous row to the right of the vertical line. Call this the partial increase over the previous row. It depends on placing of the vertical line, and for a given placing, becomes a function of each row. The requirement is that the partial increase always weakly decrease upon moving to a lower row.

(vii) The number of times the total increase of one row over the previous row equals $t$ is exactly $\beta_t - \beta_{t+1}$, for each $t$.

This intricately combinatorial requirement describes the allowable invariant factors of a product of integral matrices. The connection with symmetric polynomials is that the same combinatorial scheme arises when a product of two Schur functions is written as a linear combination of Schur functions. (A Schur function is a certain kind of symmetric polynomial.)

The Klein conditions suffer from a great defect that any number theorist immediately notices: They are not divisibility relations. In terms of matrices $C = AB$, one expects that an invariant factor of $A$ times an invariant factor from $B$ should divide (or be divisible by) an invariant factor of $C$. For example, here is a valid divisibility relation:

If the invariant factors of $A$, $B$, $C = AB$ are $a_1|a_2|...$, $b_1|b_2|...$, $c_1|c_2|...$, then

$$a_i b_j \mid c_{i+j-1}.$$ 

This kind of divisibility relation is not apparent in Klein's conditions.

It is possible to derive divisibility conditions, however. For this description we need another tableau.
Let three sequences $a, b, c$ of nonnegative integers be given
(Note: the $a_i, b_i, c_i$ are now integers, not invariant factors):

$$a = (a_1, ..., a_s) \quad (0 \leq a_1 \leq ... \leq a_s),$$

$$b = (b_1, ..., b_s) \quad (0 \leq b_1 \leq ... \leq b_s),$$

$$c = (c_1, ..., c_s) \quad (0 \leq c_1 \leq ... \leq c_s),$$

be given. Use these numbers to specify a pattern for a skew-tableau,
as follows. The case $s = 6$ is displayed:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>$a_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$a_5$</td>
<td>$R_{65}$</td>
</tr>
<tr>
<td></td>
<td>$a_4$</td>
<td>$R_{64}$ $R_{54}$</td>
</tr>
<tr>
<td></td>
<td>$a_3$</td>
<td>$R_{63}$ $R_{53}$ $R_{43}$</td>
</tr>
<tr>
<td></td>
<td>$a_2$</td>
<td>$R_{62}$ $R_{52}$ $R_{42}$ $R_{32}$</td>
</tr>
<tr>
<td></td>
<td>$a_1$</td>
<td>$R_{61}$ $R_{51}$ $R_{41}$ $R_{31}$ $R_{21}$ $R_{11}$</td>
</tr>
</tbody>
</table>

The numbers inside each box are its length. Note the pattern. The
total lengths of the rows are to be $c_6, c_5, c_4, c_3, c_2, c_1$. Moreover, the
sum of the slant box sizes gives the $b$'s:

$$b_6 = R_{66} + R_{65} + R_{64} + R_{63} + R_{62} + R_{61},$$

$$b_5 = R_{55} + R_{54} + R_{53} + R_{52} + R_{51},$$

$$b_4 = R_{44} + R_{43} + R_{42} + R_{41},$$

$$b_3 = R_{33} + R_{32} + R_{31},$$

$$b_2 = R_{22} + R_{21},$$

$$b_1 = R_{11}.$$  

Moreover, there is to be huge amounts of majorization in this display:

$$R_{66} \geq R_{55} \geq R_{44} \geq ... \text{ etc}$$

$$R_{66} + R_{65} \geq R_{55} + R_{54} \geq R_{44} + R_{43} \geq ... \text{ etc}$$
\[ r_{66} + r_{65} + r_{64} \geq r_{55} + r_{54} + r_{53} \geq r_{44} + r_{43} + r_{42} \ldots \text{ etc} \]

etc.

Let us say that the integer sequences \( a, b, c \) admit a skew tableau if nonnegative integers \( r_{ij} \) exist to fulfill these combinatorial constraints. So the test for the admissibility of \( a, b, c \) is implicit: one must test for the solvability for the \( r_{ij} \).

Now the theorem is this: Let three strictly increasing sequences of positive integers be given:

\[
\begin{align*}
    i &= (i_1, \ldots, i_s), \quad i_1 < \ldots < i_s \\
    j &= (j_1, \ldots, j_s), \quad j_1 < \ldots < j_s, \\
    k &= (k_1, \ldots, k_s), \quad k_1 < \ldots < k_s.
\end{align*}
\]

Then: If the numbers

\[
\begin{align*}
    a_1 &= i_1 - 1, \ldots, a_s = i_s - s, \\
    b_1 &= j_1 - 1, \ldots, b_s = j_s - s, \\
    c_1 &= k_1 - 1, \ldots, c_s = k_s - s
\end{align*}
\]

are admissible, the integer exponents giving the invariant factors of \( A, B, C = AB \) satisfy this family of inequalities:

\[
s_{i_1}(A) \cdots s_{i_s}(A) s_{j_1}(B) \cdots s_{j_s}(B) | s_{k_1}(C) \cdots s_{k_s}(C)
\]

(The symbol \( s \) is unfortunately used here in two meanings: as an invariant factor, and as an integer subscript.) There is equality here when the integer subscript \( s = n \) (for \( n \times n \) matrices.) I have very recently been told by I. Zaballa that he has proved the converse part of the assertion just given: That is, if proposed numbers are given for the invariant factors of \( A, B, C = AB \) satisfying all these divisibility relations, with equality when \( s = n \), then \( n \times n \) matrices \( A, B, C = AB \) in fact exist having these invariant factors. It has long been known that
a purely combinatorial argument was needed to establish this, and this argument is: to show that if the integer inequalities corresponding to these divisibility relations are all satisfied, then the tableau conditions in Klein's theorem are also satisfied, and so the modules $A, B, C$ exist with $B = C / A$ (and therefore so do the matrices $A, B, C = AB$.)

The formulas just discussed surely are divisibility relations, but the allowable indices $i_1, ..., k_s$ in them are defined implicitly, one has to check whether a given set of linear equalities and inequalities has a nonnegative has a nonnegative integer solution $r_{ij}$.

There is one easy case in which the test for the allowability of the integer indices is easily verified:

$$k_1 = i_1 + j_1 - 1, \ k_2 = i_2 + j_2 - 2, ..., \ k_s = i_s + j_s - s.$$  

I call the divisibility inequality corresponding to these subscripts the standard inequality. It contains two noteworthy special cases:

For $s = 1$,

$$s_i(A) s_j(B) \mid s_{i+j-1}(C).$$

This is the Weyl inequality, but for invariant factors.

For $j_1 = 1, j_2 = 2, ..., j_s = s$,

$$s_{i_1}(A) \cdots s_{i_j}(A) s_1(B) \cdots s_s(B) \mid s_{i_1}(C) \cdots s_{i_s}(C).$$

These are the Lidskii-Siegel inequalities for invariant factors. Please excuse the awkward use of $s$ both as a symbol for an invariant factor and as an integer subscript.

We want to put these divisibility relations into a better form. Now, no one appears to know a really good form, but there is a recursive description.

Define by induction on $L$ as to when sequences

$$F = (f_1, ..., f_L), \ G = (g_1, ..., g_L), \ H = (h_1, ..., h_L)$$
are consistent. (Components are strictly increasing integers in \([1,n]\).)
For \(L = 1\),

\[ f_1 + g_1 = h_1 + 1. \]

Continue by induction. Let

\[ P = (p_1, \ldots, p_k), \quad Q = (q_1, \ldots, q_k), \quad R = (r_1, \ldots, r_k) \]

be consistent sequences for \(k < L\), with strictly increasing components in \([1,L]\). Then we require of \(F, G, H\) that

\[ \sum_{t=1}^{k} f_{pt} + \sum_{t=1}^{k} g_{qt} \leq \sum_{t=1}^{k} h_{rt} + \frac{k(k+1)}{2} \]

and

\[ f_1 + \ldots + f_L + g_1 + \ldots + g_L = h_1 + \ldots + h_L + \frac{L(L+1)}{2}. \]

Now we have this apparently true statement: The rules for consistency precisely describe the the admissible sequences in the divisibility relations. I did part of its proof some years ago, and it appears to be contained in B. V. Lidskii's announced solution concerning the spectrum of a sum of Hermitian matrices. I have recently have been reexamining my proof, with the intent of relating it to an algorithmic procedure in Young Tableaux combinatorics called the Littlewood-Richardson-Robinson-Schensted-Knuth-Thomas (and others) rule. More details on this in a later lecture.

It is worth remarking how extremely numerous the divisibility conditions (consistent sequences as subscripts) are:

- for \(2 \times 2\) matrices, there are 4 conditions,
- for \(3 \times 3\) matrices, there are 13 conditions,
- for \(4 \times 4\) matrices, there are 42 conditions,

\[ \ldots \]

- for \(7 \times 7\) matrices, there are 2053 conditions.
I recently did a search of the literature on Young Tableaux in the Mathematics Review data base at Lockheed Dialogue (= Knowledge Index.) I found 138 references, many of them connected to problems in physics, but there were a couple that appeared to offer promise for finding a formula for counting the number of admissible sequences. I haven't yet had time to pursue this, but I regard it as an interesting problem.

Now, we turn to the invariant factors for similarity, working over a field $F$. For a matrix $A$ with entries in a field, these similarity invariant factors are the invariant factors of the polynomial matrix $\lambda I - A$. The equality of similarity invariant factors for matrices $A, B$ is well known to be the necessary and sufficient conditions for $A$ and $B$ to be similar. We are now going to rework the ideas above for this new situation. There will be some analogous facts, and some which differ tremendously.

A key remark is that the invariant factors (for similarity) for an $n \times n$ matrix are not just arbitrary polynomials, they satisfy an extra condition, namely the sum of the degrees of the invariant factors is $n$. This additional condition causes a great amount of extra difficulty.

Let us look at a typical situation. We have matrices $A, B, C = A + B$ with entries in a field. We ask: how do the similarity invariants for $C$ depend on those of $A$ and $B$? A natural initial reaction is that there are no theorems here, and this has been said to me more than once by knowledgeable people. But this reaction is wrong. For if $B$ is scalar, $B = \beta I$, then adding $B$ to $A$ changes only the eigenvalues (adds $\beta$ to them), but does not affect the similarity invariants in any other way. One need only look at the Jordan form to see this. So the general picture will be that the nearer $B$ is to being scalar, the closer must the similarity invariants of $C$ be to those of $A$. The divisibility conditions with $s = 1$ (the one term conditions) capture this fact to a certain extent. On the other hand, when $C$ is required to be far from being scalar, perhaps adding it to $A$ affects the similarity invariants less.

Consider the easy case: $B = A + X$, where $X$ is variable with rank one, and $A, B$ have entries in a field. How do the similarity invariants of $A, B$ relate? Clearly

$$\lambda I - B = \lambda I - A + \text{a rank one matrix},$$
and therefore the previous results from the integral case apply:

\[ s_1(A) s_2(B) s_3(A) s_4(B) l \ldots \]

\[ s_1(B) s_2(A) s_3(B) s_4(A) l \ldots \]

It turns out, with a bit of additional logic, that these conditions are also sufficient for the existence of two matrices over a field to have prescribed similarity invariants and to differ by a rank at most one matrix.

This theorem was used in the lecture on the exponential function.

F. C. Silva has worked on this question of the similarity invariants of a sum \( C = A + B \) of matrices over a field, when all three are to have prescribed similarity invariants, and his results follow the general pattern: If one of the matrices has only similarity invariants of degree two or less, then there are constraints on the similarity invariants of the sum, otherwise constraints are absent. But I do not think complete results have been achieved.

An analogous problem is the similarity invariants of a product of matrices over a field, and this has not been much worked on. Here the closer one of the factors is to the identity matrix, the more the similarity factors of the product are constrained. The expectation is that if \( B \) has invariant factors only of degrees two or less, then the similarity factors of the product are constrained, otherwise not. But this has not been worked on.

Now we come to the submatrix problem. Let

\[ C = \begin{pmatrix} AX \\ YB \end{pmatrix} \]

for matrices over a field, and ask how the similarity invariants of \( A \) and \( C \) are related. There is a theorem here that has received some notoriety, now called the Sa-Thompson theorem. The notoriety is due the great difficulty of its proof. How do the similarity invariants of \( A \) and \( C \) relate? Since

\[ \lambda I - C = \begin{pmatrix} \lambda I - A & -X \\ -Y & \lambda I - B \end{pmatrix} \]
we can apply the divisibility relations to the invariant factors of $A$ and $C$ that follow from the Chatelet theorem.

\[ s_i(C) | s_i(A) | s_{i+2(n-k)}(C), \]

for all $i$, where $C$ is $n \times n$ and $A$ is $k \times k$.

But there is also another condition: the sum of the degrees of the invariant factors of $A$ is $k$, where $A$ is $k \times k$, and the sum of the degrees of the invariant factors of $C$ is $n$, where $C$ is $n \times n$.

\[ \text{degree } (s_1(A) \cdots s_k(A)) = k, \quad \text{degree } (s_1(C) \cdots s_n(C)) = n. \]

This seemingly mild additional constraint causes great difficulty in the sufficiency (constructive) part of the proof, when $k < n-1$. The difficulty arises in the attempt to move to smaller submatrices by using an induction. One can write down by repeated use of interlacing a candidate polynomial matrix that works in the $A$ submatrix position, but to be the characteristic matrix, i.e. to be $\lambda I - A$, it is necessary that the degree condition be satisfied at all stages in the induction, and it is here that the trouble arises. It was handled by me a purely ad hoc and somewhat combinatorial argument that ran through many pages and lemmas. As I usually do, I got the argument simply by working examples and observing what happened in them. It was handled by Sa by a totally surprising device, in which he used the approximation property of an integral by the integral of step functions. Unfortunately, neither of us could understand the other's proof! Another proof was produced by my student P Y Cheng. A better and understandable proof has recently been found by Sa. But the best proof has recently been given by I Zaballa, who tied it to ideas from control theory. It is this proof that will live! The Sa-Thompson theorem is therefore one in control theory.

We return to the product $C = AB$ of matrices over $\mathcal{R}$, and ask for the invariant factors of $C$ in terms of those of $A$ and $B$ when $\det A$ and $\det B$ are relatively prime elements of $\mathcal{R}$. The relatively prime case is always important in number theory. There is a very nice theorem here, due to M. Newman. I will give two proofs of it. The theorem is:

\[ s_i(C) = s_i(A)s_i(B), \quad \text{for all } i. \]
That is, the invariant factors multiply when the matrices multiply, if the determinants of the matrices are without common factor.

First proof. From the Weyl inequality for invariant factors,

\[ s_i(A)s_1(B) \mid s_i(C) \mid s_i(A)s_n(B). \]

This implies that any power of a prime \( p \) in \( s_i(A) \) is present to exactly the same power in \( s_i(C) \), since it cannot be present in any invariant factor of \( B \), by the relative primeness of \( \det A \) and \( \det C \). Interchange the roles of \( A \) and \( B \), and the result follows. This is my proof of Newman's theorem.

Second proof. Let \( \mathcal{R}_p \) be the local ring consisting of all fractions formed from elements of \( \mathcal{R} \), but excluding those with denominators involving \( p \). The ring \( \mathcal{R}_p \) is a principal ideal ring (all ideals are \( (p^k) \) for \( k = 0, 1, 2, \ldots \)). Over \( \mathcal{R}_p \), one of \( A \) or \( B \) (say \( B \)) has unit determinant, so is unimodular, and so \( C \) and \( A \) have the same invariant factors over \( \mathcal{R}_p \), which of course are just the elementary divisors for \( p \). Thus \( A \) and \( C \) have the same elementary divisors for \( p \). Doing this argument for every prime \( p \), we get the multiplicativity of the invariant factors. This proof of Newman's theorem is due to L. Gerstein.

End of Lecture 3