**Summaries, April 7 and 9**

**linear algebra over a ring**

The most basic problem of linear algebra is solving a system $AX = B$ of linear equations. For example, when $R$ is the ring of integers $\mathbb{Z}$ and $A, B$ have coeffiients in $\mathbb{Z}$, one can ask for integer solutions of.

**Example 1.**

$$\begin{pmatrix} 1 & 1 & 0 \\ 2 & 0 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$

We can ask to find the integers $x_1, x_2, x_3$ that solve the system We'll come back to this example below.

Linear algebra over a field $F$ is usually expressed in terms of $F$-vector spaces. Over a ring $R$, the analogous concept is called an *$R$-module*. The definition of $R$-module is the same as that of a vector space. An $R$-module $V$ is a set with two laws of composition: addition $v + w$ of elements o $V$ and scalar multiplication $av$ of an element $v$ of $V$ by an element $a$ of $R$. The operatiosn are required to satisfy these relations:

• With addition, $V$ is an abelian group. Its identity is denoted by $0$.

• Scalar multiplication is associative: $(ab)v = a(bv)$, and multiplication by the unit element $1$ of $R$ is the identtity operator: $1v = v$.

• Two asociative laws hold: $(a + b)v = av + bv$ and $a(v + w) = av + aw$, for all $a, b$ in $R$ and all $v, w$ in $V$.

These are the axioms for a vector space, when $R$ is a field.

**Example 2.** $R = \mathbb{Z}$. To give a module $V$ over the ring of integers, one must, first of all, give an $V$ the structdure of an abelian group. Then one must define scalar multiplication by integers. However, scalar multiplication is already determined: $2v = (1 + 1)v = 1v + 1v = v + v$, etc. So we don't need to define it separately.

**Corollary.** $\mathbb{Z}$-module and abelian group, with law of composition written as addition, are equivalent concepts.

**Example 3.** $R = F[x]$ is the ring of polynomials over a field $F$. Given an $F[x]$-module $V$, scalar multiplication by any polynomal is defined. In particular, one can do scalar multiplication by constant polynomials, elements of $F$. If we look only at the addition law and at scalar multiplication by elements of $F$, $V$ becomes an $F$-vector space. Then scalar multiplication by $x$ becomes a linear operator on that vector space: $x(v + w) = xv + xw$ and $x(av) = (xa)v = (ax)v = a(xv)$. And when we know how to multiply by $x$, multiplication by a polynomial is uniquely determined: $(x^2)v = x(xv)$, for instance.

**Corollary.** Modules over thie ring $F[x]$ of polynomials correspond to $F$-vector spaces with a chosen linear operator.

As these examples show, $R$-modules encompass several important concepts.

**homomorpisms, submodules, quotient modules**

A homomorphism of $R$-modules is a map $V \overset{\varphi}{r} rrW$ that satisfies the requirements of a lineartransformation: $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$, and $\varphi(av+ = a\varphi(v)$ for $a \in R$.

A *submodule* $U$ of an $R$-module $V$ is a subset closed under addition and scalar multiplication: If $u_1, u_2$ are in $U$ then $u_1 + u_2$ and $au_1$ are in $U$. For example, the *kernel* of the homomorphism $\varphi$ is the set of elements $v \in V$ such that $\varphi(v) = 0$. It is a submodule of $V$.

If $U$ is a submodule of a module $V$, the *quotient module* $\overline{V} = V/U$ is the set of (additive) cosets $\overline{v} = v + U$ of $U$. II like to think of the quotient module as the set of equivalence classes, the equivalence relation being $v' \sim v$ if $v'$ is in the coset $v + U$. The quotient is made into a module in the usual way.

There is a canonical homomorphism $V \xrightarrow{\pi} \overline{V}$ that sends $v$ to $\overline{v}$.

*mapping property* Homomorphisms $\overline{V}\overline{\varphi} \longrightarrow W$ corespond bijectively to homomorphism $V \xrightarrow{\varphi} W$ whose kernels contain $U$.

**basis** A *basis* for an $R$-module $V$ is a set $B = (v_1, ..., v_n)$ of elements of $V$ such that every element $v$ of $V$ is a combination: $v = r_1v_1 + \cdots + r_nv_n$ in a unique way. This means that the map (a homomorphism) $R^n \xrightarrow{B} V$ that sends a column vector $X = (x_1, ..., x_n)^t$ to the combination $BX = v_1x_1 + \cdots + v_nx_n$ is a *bijective* map.

If that map is surjective, one says that $B = (v_1, ..., v_n)$ *generates* $V$, and if that map is injective, the set $B$ is *independent*.

A set $B$ that generates $V$ exists quite often, but such a set is rarely independent, and therefore rearely a basis of $V$. When $R$ isn't a field, most $R$-modules will have no basis. For example, a finite abelian group is a $\mathbb{Z}$-module that has no basis. If $F$ is a field, a linear operator $x$ on a finite-dimensional $F$-vector space $V$ makes $V$ into an $F[x]$-module that has no basis.

**mapping property** Let $B = (v_1, ..., v_n)$ be a set that generates an $R$-module $V$, so that the map $R^n \xrightarrow{B} V$ that sends $X$ to $BX$ is surjective. Let $K$ be the kernel of that map $B$. Then $V$ is isomorphic to $R^n/K$.

We go back to a system $AX = B$ of linear equations with coefficients in a ring $R$. Say that $A$ is an $m \times n$ matrix, $B$ is a $1 \times m$ an $n$-dimensional column vector, both with entries in $R$, and $X$ is an unknown $m$-dimensional column vector. To find the solutions in $R$, one may try to simplify $A$ and $B$.

Let $P$ be an $n \times n$ matrix with entries in $R$, that has an inverse $P^{-1}$ whose oefficients are also in $R$, Similarly, let $Q$ be an $m \times m$ matrix such that both $Q$ and an inverse $Q^{-1}$ have coefficients in $R$.

For example, $P$ and $Q$ might be products of elementary matrices that have entries in $R$ and whose inverses also have entries in $R$. There are many such matrices because they include those that operate by adding an $R$-multiple of one row to another.

Let $A' = Q^{-1}AP$, $B' = Q^{-1}B$, and $X' = P^{-1}X$, and onsider the system of equations $A'X' = B'$. If we can solve this new system, we will also be able to solve the orginal one, by $A = QA'P^{-1}$, $B = QB'$, and $X = PX'$. So we can try to simplify $A$ by elementary row and column operations (staying in $R$).

**Example 1, again** Using elementary operations, we can simplify the coefficient matrix:

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 0 & 4 \end{pmatrix} \to A' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

In fact, one can do this entirely with column operatons. In this simple example, row operations aren't needed. So $B$ is unchanged. The solution of the equation $A'X = B$ becomes $X' = (2, 1, a)^t$ where $a$ is arbitrary. To solve the original equaiton, one needs to multiply the elementary matrices used. Let's not bother to do this.

**Theorem.** Let $A$ be an $m \times n$ integer matrix, There exist an $m \times m$ matrix $P$ and an $n \times n$ matrix $Q$, both products of invertible elementary integer matrices, such that $A' = Q^{-1}AP$ is diagonal, and if the diagonal entries re $d_1, d_2, ..., d_k$, then $d_1|d_2|\cdots|d_k$.

The proof isn't hard.