MATH 122. LECTURE NOTES AND HOMEWORK PROBLEMS

LEVENT ALPOGE AND DENNIS GAITSGORY

Abstract. These are notes from Math 122 (Algebra-I), taught at Harvard in Fall 2012.

1. Tuesday, Sept. 4

1.1. **Semi-groups, monoids and groups.**

We begin with the following definition:

Definition 1.1.1. *A semi-group is a set A equipped with a binary operation*

$$A \times A \overset{mult}{\longrightarrow} A, \quad (a_1, a_2) \mapsto a_1 \cdot a_2$$

which satisfies the associativity axiom*:*

$$\forall\, a_1, a_2, a_3 \in A, \quad a_1 \cdot (a_2 \cdot a_3) = (a_1 \cdot a_2) \cdot a_3.$$

We can rewrite the associativity axiom also as follows: the diagram of sets

$$\begin{tikzcd}
A \times A \times A \arrow[r, "\mathrm{id}_A \times mult"] \arrow[d, "mult \times \mathrm{id}_A"'] & A \times A \arrow[d, "mult"] \\
A \times A \arrow[r, "mult"] & A
\end{tikzcd}$$

commutes, where e.g. $\mathrm{id}_A \times mult\,(a_1, a_2, a_3) = (a_1, a_2 \cdot a_3)$. I.e., the two maps from the upper-left corner to the lower-right corner coincide.

1.1.2. We will now impose various conditions on semi-groups.

Definition 1.1.3. *A semi-group A is said to be a monoid if there exists an element $1 \in A$ that satisfies*

$$\forall a \in A, \quad 1 \cdot a = a = a \cdot 1.$$

An element $1 \in A$ is called the "unit" or the "identity" in A.

Lemma 1.1.4. *A monoid contains a unique unit element.*

Proof. Let $1' \in A$ be another unit. We want to show that $1' = 1$. We have: $1 = 1 \cdot 1'$, since $1'$ is a unit, and $1 \cdot 1' = 1'$, since 1 is a unit. Hence

$$1 = 1 \cdot 1' = 1'.$$

□

In algebra, it is often the case that there is not really much one can do besides "follow one's nose". Above and below we implement this strategy. For instance, in trying to prove uniqueness of a unit element, we are confronted with showing two candidate units must be the same. So we have two elements of a group, and that's it. The only thing we can possibly do is multiply them and see what happens. The above proof constitutes "seeing what happens".

Let A be a monoid and $a \in A$ an element.

Definition 1.1.5. *An inverse of a is an element $a^{-1} \in A$ such that*

$$a \cdot a^{-1} = 1 = a^{-1} \cdot a.$$

Lemma 1.1.6. *If $a \in A$ admits an inverse, then this inverse is unique.*

Again, we do the only thing possible and see what happens.

Proof. Let a_1^{-1} and a_2^{-1} be both inverses of a. We have

$$a_1^{-1} = a_1^{-1} \cdot 1 = a_1^{-1} \cdot (a \cdot a_2^{-1}) = (a_1^{-1} \cdot a) \cdot a_2^{-1} = 1 \cdot a_2^{-1} = a_2^{-1}.$$

□

Definition 1.1.7. *A monoid is said to be a group if every element admits an inverse.*

1.1.8. *Examples.*

(i) $A = \mathbb{Z}$ with the operation of addition is a group.

(ii) $A = \mathbb{Z}$ with the operation of multiplication is a monoid, but not a group.

(iii) $A = \mathbb{R}$ with the operation of addition is a group.

(iv) $A = \mathbb{R}$ with the operation of multiplication is a monoid, but not a group.

(v) $A = \mathbb{R}^* := \mathbb{R} - \{0\}$ with the operation of multiplication is a group.

(vi) $A = \{\pm 1\} \subset \mathbb{R}$ with the operation of multiplication is a group. This group is denoted $\mathbb{Z}_2$.

(vii) $A = \mathbb{C}^* := \mathbb{C} - \{0\}$ with the operation of multiplication is a group.

(viii) $A = \{z \in \mathbb{C}^* : \ |z| = 1\}$ with the operation of multiplication is a group. This group is denoted S^1.

(ix) $A = \{z \in \mathbb{C} : \ z^3 = 1\}$ with the operation of multiplication is a group. This group is denoted $\mathbb{Z}_3$.

(x) $A = \mathbb{Z} \times \mathbb{Z}$. The binary operation is defined as follows

$$(m_1, n_1) \cdot (m_2, n_2) := (m_1 + n_1, m_2 + n_2).$$

This is a group.

Verifications in all of the above cases are easy, but you need to perform them!

1.1.9. *Commutativity.*

Definition 1.1.10. *A semi-group/monoid/group A is said to be commutative if*

$$\forall\, a_1, a_2 \in A, \quad a_1 \cdot a_2 = a_2 \cdot a_1.$$

We also call such a thing "abelian", after Niels Henrik Abel. The two mean exactly the same thing.

We can rewrite the commutatvity condition as the commutativity of the diagram

$$\begin{tikzcd}
A \times A \arrow[r, "mult"] \arrow[d, "swap_A"'] & A \arrow[d, "\mathrm{id}_A"] \\
A \times A \arrow[r, "mult"] & A,
\end{tikzcd}$$

where for any set X, we denote by $swap_X$ the map

$$X \times X \to X \times X, \quad (x_1, x_2) \mapsto (x_2, x_1).$$

1.1.11. All of the above examples of monoids and groups were commutative. There are plenty of interesting non-commutative groups, but we will get to them only later in the semester.

1.2. **Group homomorphisms.** When defining a mathematical structure, after introducing the objects, the next step is to define the way in which two objects of the specified kind communicate with each other. For groups this communication is called a group homomorphism.

Thus, let A and B be two groups.

Definition 1.2.1. *A group homomomorphism from A to B is a map of sets $\phi : A \to B$ that satisfies the following axiom:*

$$\forall\, a_1, a_2 \in A, \quad \phi(a_1) \cdot \phi(a_2) = \phi(a_1 \cdot a_2).$$

We can rewrite the condition on a map of sets to be a group homomorphism as the requirement that the diagram

$$\begin{tikzcd}
A \times A \arrow[r, "mult_A"] \arrow[d, "\phi\times\phi"'] & A \arrow[d, "\phi"] \\
B \times B \arrow[r, "mult_A"] & B
\end{tikzcd}$$

be commutative.

We let $\mathrm{Hom}_{\mathrm{Grp}}(A, B)$ denote the set of group homomorphisms from A to B.

1.2.2. Here are a few assertions about group homomorphisms:

Lemma 1.2.3. *Let $\phi : A \to B$ be a group homomorphism. Then $\phi(1_A) = 1_B$.*

We start with an auxilliary statement:

Lemma 1.2.4. *If a is an element of a group A such that $a \cdot a = a$, then $a = 1$.*

Proof. We have:

$$1 = a^{-1} \cdot a = a^{-1} \cdot (a \cdot a) = (a^{-1} \cdot a) \cdot a = 1 \cdot a = a.$$

□

Proof of Lemma 1.2.3. We have

$$\phi(1_A) \cdot \phi(1_A) = \phi(1_A \cdot 1_A) = \phi(1_A).$$

Now apply Lemma 1.2.4. □

Lemma 1.2.5. *Let $\phi : A \to B$ be a group homomorphism. Then for every $a \in A$, we have*

$$\phi(a)^{-1} = \phi(a^{-1}).$$

Proof. We need to show that $\phi(a^{-1})$ is the inverse of $\phi(a)$, i.e., that

$$\phi(a^{-1}) \cdot \phi(a) = 1_B.$$

However, we have:

$$\phi(a^{-1}) \cdot \phi(a) = \phi(a^{-1} \cdot a) = \phi(1_A),$$

which equals 1_B, by Lemma 1.2.3. □

1.2.6. *Examples.*

(i) Take $A = B = \mathbb{Z}$ (with addition). Define $\phi(n) = 2 \cdot n$. This is a group homomorphism.

(ii) Take $A = B = \mathbb{Z}$ (with addition). Define $\phi(n) = n^2$. This is *not* a group homomorphism.

(iii) Take $A = \mathbb{Z}$, $B = \mathbb{R}$ (with addition). Set $\phi(n) = \pi \cdot n$. This is a group homomorphism.

(iv) Take $A = \mathbb{Z}$ (with addition), $B = \mathbb{C}^*$ (with multiplication). Let $z \in \mathbb{C}^*$ be any element. Set $\phi(n) = z^n$. This is a group homomorphism.

(v) Take $A = \mathbb{Z} \times \mathbb{Z}$ and $B = \mathbb{Z}$. Set $\phi(m, n) = m$. This is a group homomorphism.

1.2.7. *Properties of group homomorphisms.* Let $\phi : A \to B$ be a group homomorphism.

Definition 1.2.8. *We say that ϕ is injective/surjective/bijective if it such as a map of sets.*

Recall that, thanks to the axiom of choice, if $\phi : A \to B$ is an injective map of sets, there always exists a map $\psi : B \to A$ such that

$$\psi \circ \phi = \mathrm{id}_A .$$

Similarly, recall that if $\phi : A \to B$ is a surjective map of sets, there always exists a map $\psi : B \to A$ such that

$$\phi \circ \psi = \mathrm{id}_B .$$

Week 1, HW Problem 1.

(a) *Take $A = B = \mathbb{Z}$ and ϕ given by $n \mapsto 2 \cdot n$. Show that ϕ is injective. Show that there does* not *exist a group homomorphism $\psi : B \to A$ such that $\psi \circ \phi = \mathrm{id}_A$. Hint: suppose that ψ existed. Consider the element $\psi(1)$ and arrive at a contradiction.*

(b) *Take $A = B = \mathbb{C}^*$ and ϕ given by $z \mapsto z^2$. Show that ϕ is sujective. Show that there does* not *exist a group homomorphism $\psi : B \to A$ such that $\phi \circ \psi = \mathrm{id}_B$. Hint: suppose that ψ existed. Consider the element $\psi(-1)$ and arrive at a contradiction.*

Recall that to say that $\phi : A \to B$ is a bijective map of sets is to say that there exists a (unique) map $\psi : B \to A$ such that

$$\psi \circ \phi = \mathrm{id}_A \text{ and } \phi \circ \psi = \mathrm{id}_B .$$

Week 1, HW Problem 2. *Let ϕ be a bijective group homomorphism. Show that the inverse map of sets ψ is also a group homomorphism.*

Bijective group homomorphisms are also called “isomorphisms”. Note that, by Problem 2, isomorphisms can be inverted. Two groups A and B are said to be isomorphic of there exists an isomorphism between them.

1.2.9. *Homomorphisms from $\mathbb{Z}$.*

Let A be a group. Consider the set $\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, A)$ of group homomorphisms $\mathbb{Z} \to A$. Consider the map of sets

$$\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, A) \to A$$

that assigns to a homomorphism ϕ the element $\phi(1) \in A$.

Week 1, HW Problem 3. *Show that the above map defines a bijection of sets from $\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, A)$ to A. I.e., show that for every element $a \in A$ there exists a unique group homomorphism $\phi_a : \mathbb{Z} \to A$ that sends $1 \mapsto a$.*

1.3. **Subgroups.**

1.3.1. Let A be a semi-group/monoid/group, and let $A' \subset A$ be a subset.

Definition 1.3.2. *We shall say that A' is a*

(a) *Sub-semi group if $\forall\, a_1, a_2 \in A'$, the element $a_1 \cdot a_1$ also belongs to A'.*

(b) *Submonoid if it is a sub-semi group and $1_A \in A'$.*

(c) *Subgroup if it is a submonoid and $\forall\, a \in A'$, the element a^{-1} also belongs to A'.*

Week 1, HW Problem 4. *Write a complete proof of the following statement made in class:*

Let $A' \subset A$ be a group and a subgroup. Let $\phi : A' \to A$ denote the tautological map of sets. Then A' has a unique group structure for which ϕ is a group homomorphism.

1.3.3. *Examples.*

(i) $\mathbb{Z}^{\geq 1} \subset \mathbb{Z}$ is a sub-semi group, but not a submonoid.

(ii) $\mathbb{Z}^{\geq 0} \subset \mathbb{Z}$ is a submonoid, but not a subgroup.

(iii) The set of even integers divisible by a given integer k is a subgroup of $\mathbb{Z}$.

(iv) For any group, the subset $\{1\}$ is a subgroup.

(v) $\{z \in \mathbb{C}^* : \ |z| = 1\} \subset \mathbb{C}^*$ is a subgroup.

1.3.4. *Kernels.* Let $\phi : A \to B$ be a group homomorphism. We define the kernel of ϕ as

$$\ker(\phi) = \{a \in A : \ \phi(a) = 1_B\}.$$

Week 1, HW Problem 5. *Write a complete proof of the following two statements proved in class:*

(a) $\ker(\phi)$ *is a subgroup.*

(b) $\ker(\phi) = \{1\}$ *if and only if ϕ is injective.*

2. Thursday, Sept. 6

2.1. **Subgroups, continued.** Notice that $\ker(\phi) = \phi^{-1}(\{1\})$, so we might generalize the above as follows.

Lemma 2.1.1. *Let $\phi : A \to B$ be a group homomorphism. Let $B' \subset B$ be a subgroup. Then $\phi^{-1}(B') \subset A$ is a subgroup.*

Proof. Let a_1, a_2 be two elements of $\phi^{-1}(B')$. First, we need to show that $a_1 \cdot a_2$ is also an element of $\phi^{-1}(B')$. We have

$$\phi(a_1 \cdot a_2) = \phi(a_1) \cdot \phi(a_2),$$

while $\phi(a_1), \phi(a_2) \in B'$. Since B' is a subgroup, $\phi(a_1) \cdot \phi(a_2) \in B'$, so $\phi(a_1 \cdot a_2) \in B'$, as required.

Next, we need to show that $1_A \in \phi^{-1}(B')$. We have $\phi(1_A) = 1_B$, by Lemma 1.2.3. Now, $1_B \in B'$, since B' is a subgroup, so $\phi(1_A) \in B'$, as required.

Finally, we need to show that if $a \in \phi^{-1}(B')$, then $a^{-1} \in \phi^{-1}(B')$. We have:

$$\phi(a^{-1}) = (\phi(a))^{-1},$$

by Lemma 1.2.5. By assumption $\phi(a) \in B'$, hence $(\phi(a))^{-1} \in B'$, since B' is a subgroup. Hence, $\phi(a^{-1}) \in B'$, as required. □

Lemma 2.1.2. *Let $\phi : A \to B$ be a group homomorphism. Then $\mathrm{Im}(\phi) \subset B$ is a subgroup.*

Week 1, HW Problem 6. *Write a complete proof of Lemma 2.1.2.*

2.2. **Equivalence relations.** When examining an object, sometimes it pays to take many, many steps back until only the large scale structure can be seen. Using this large scale structure — which is often easier to study — one can often deduce nontrivial facts about the original object itself. What are we doing when we step so far back that we can only see blobs? We are, in some sense, setting everything in one blob *equal* to everything else in the blob. As mathematicians, we must formalize this. We do this as follows.

Let X be a set.

Definition 2.2.1. *A relation on X is a subset $R \subset X \times X$.*

Given a relation on X, for $x_1, x_2 \in X$ we shall write $x_1 \sim x_2$ if and only if $(x_1, x_2) \in R$.

Definition 2.2.2. *A relation on X is called an equivalence relation if and only if the following conditions hold:*

Reflexivity: for all $x \in X$, we have $x \sim x$;

Symmetry: if $x_1 \sim x_2$ then $x_2 \sim x_1$;

Transitivity: if $x_1 \sim x_2$ and $x_2 \sim x_3$ then $x_1 \sim x_2$.

These are just axiomatizations of what we'd expect from something behaving like "=".

2.2.3. *Example.* Take $X = \mathbb{Z}$ and declare $n_1 \sim n_2$ if and only if $n_1 - n_2$ is even. This is an equivalence relation (check this!). (Imagine wrapping the real line around into an infinite coil, with one full revolution every two units. Here we are, in some sense, looking down on this coil from above.)

2.2.4. *Cosets.* Let X be a set with an equivalence relation $\sim$.

Definition 2.2.5. *A coset with respect to $\sim$ is a subset $X' \subset X$ that satisfies:*
(0) $X' \neq \emptyset$;
(1) If $x_1 \in X'$ and $x_1 \sim x_2$, then $x_2 \in X'$;
(2) If $x_1, x_2 \in X'$, then $x_1 \sim x_2$.

This is just a formalization of our notion of "blob" above!

2.2.6. *Example.* Consider the equivalence relation in Example 2.2.3. Note that $\mathbb{Z}$ has exactly two cosets: that of even integers and that of odd integers. (That is to say, when looking down on our coil, we'd only see two thick points, corresponding to the coset containing 0, and that containing 1.)

Lemma 2.2.7. *Let X be a set with an equivalence relation $\sim$. For every element $x \in X$, there exists a unique coset, denoted $\overline{x}$, such that $x \in \overline{x}$.*

That is to say, nothing disappears when we blur our vision.

Proof. First, we prove the existence. Given x, define

$$\overline{x} = \{x_1 \in X \,|\, x \sim x_1\}.$$

This is a subset that contains x (reflexivity).

Let us show that $\overline{x}$ is a coset. It is non-empty, since it contains x. If $x_1 \in \overline{x}$ and $x_1 \sim x_2$, then $x \sim x_2$ (transitivity), hence $x_2 \in \overline{x}$. Finally, if $x_1, x_2 \in X$, we have $x_1 \sim x$ (symmetry), and hence $x_1 \sim x_2$ (again, reflexivity).

Let us now prove the uniqueness. Let $X' \subset X$ be another coset that contains x. We need to show that $X' = \overline{x}$. I.e., we have to prove inclusions in each direction.

Let x_1 be an element of $\overline{x}$. We have $x \in X'$ and $x \sim x_1$. Hence $x_1 \in X'$ (condition (1) for X'). Hence, $\overline{x} \subset X'$.

Let x_1 be an element of X'. We have $x, x_1 \in X'$, hence $x \sim x_1$ (condition (2) for X'). Hence, $x_1 \in \overline{x}$. Hence, $X' \subset \overline{x}$.

□

2.2.8. *The quotient set.* Let X be a set with an equivalence relation $\sim$.

We introduce a new set $X/\sim$, called *the quotient of X with respect to $\sim$*, as follows: $X/\sim$ is a subset of the set Subsets(X) of all subsets of X, defined by the condition

$$X' \in X/\sim \text{ if and only if } X' \text{ is a coset.}$$

2.2.9. *The projection.* Let X be a set with an equivalence relation $\sim$, and consider the quotient set $X/\sim$. We define a map

$$\pi : X \to X/\sim$$

by sending x to the coset $\overline{x}$, the latter being the unique coset containing x.

Lemma 2.2.10. *The map π is surjective.*

Proof. We need to show that any coset X' can be realized as $\overline{x}$. Since X' is non-empty, there exists $x \in X'$. Now, by Lemma 2.2.7, we have $X' = \overline{x}$. □

Lemma 2.2.11. *Let $x_1, x_2 \in X$ be two elements. Then*

$$\pi(x_1) = \pi(x_2) \Leftrightarrow x_1 \sim x_2.$$

Proof. Suppose $x_1 \sim x_2$. We need to show that $\overline{x_1} = \overline{x_2}$. Note that both $\overline{x_2}$ is a coset that contains x_2, Hence, it also contains x_1, by condition (1) on being a coset. Hence, $\overline{x_2}$ is a coset that contains x_1. Now, the uniquness assertion of Lemma 2.2.7 implies that $\overline{x_2} = \overline{x_1}$.

Vice versa, suppose that $\pi(x_1) = \pi(x_2)$, which by definition means that $\overline{x_1} = \overline{x_2}$. I.e., $x_1 \in \overline{x_2}$, while $x_2 \in \overline{x_2}$ by definition. By condition (1) on being a coset, this implies that $x_1 \sim x_2$.

□

2.2.12. *Mapping out of the quotient set.* What we will see now will be the first example of characterizing an object by a *universal property.*

Proposition 2.2.13. *Let X be a set with an equivalence relation $\sim$. Let $\phi : X \to Y$ be a mapof sets such that*

$$x_1 \sim x_2 \Rightarrow \phi(x_1) = \phi(x_2).$$

Then there exists a uniquely defined map $\widetilde{\phi} : X/\sim \to Y$ that makes the triangle

(1)
$$\begin{tikzcd}
X \arrow[r, "\phi"] \arrow[d, "\pi"'] & Y. \\
X/\sim \arrow[ur, "\widetilde{\phi}"'] &
\end{tikzcd}$$

commute.

Proof. We first prove uniqueness. We will prove a more general assertion:

Lemma 2.2.14. *Let X, Y, Z be sets and $\phi : X \to Y$, $\pi : X \to Z$ and $\psi_1, \psi_2 : Y \to Z$ be maps. Assume that both triangles*

$$\begin{tikzcd}
X \arrow[r, "\phi"] \arrow[d, "\pi"'] & Y \\
Z \arrow[ur, "\psi_1"'] &
\end{tikzcd}$$

and

$$\begin{tikzcd}
X \arrow[r, "\phi"] \arrow[d, "\pi"'] & Y \\
Z \arrow[ur, "\psi_2"'] &
\end{tikzcd}$$

commute. Assume also that π is surjective. Then $\psi_1 = \psi_2$.

Note that the assertion of Lemma 2.2.14 indeed implies the uniquness of $\widetilde{\phi}$, since $\pi : X \to X/\sim$ is surjective by Lemma 2.2.10.

Proof of Lemma 2.2.14. We need to show that for every $y \in Y$, we have $\psi_1(y) = \psi_2(y)$. Using the fact that π is surjective, there exists $x \in X$ such that $\pi(x) = y$. We have:

$$\phi(x) = \psi_1(\pi(x))$$

(commutativity of the first triangle), and

$$\phi(x) = \psi_2(\pi(x))$$

(commutativity of the second triangle).

Hence,

$$\psi_1(y) = \psi_1(\pi(x)) = \phi(x) = \psi_2(\pi(x)) = \psi_2(y),$$

as required. □

We shall now prove the existence of $\widetilde{\phi}$. For an element $y \in X/\sim$ choose $x \in X$ such that $\pi(x) = y$. Define

$$\widetilde{\phi}(y) := \phi(x).$$

Let us show that this definition is independent of the choice of x.

Indeed, suppose $\pi(x_1) = y = \pi(x_2)$. We need to show that $\phi(x_1) = \phi(x_2)$. By Lemma 2.2.11, $x_1 \sim x_2$, which implies the required equality by the assumption on ϕ.

Let us show that for $\widetilde{\phi}$ constructed as above, the triangle (1) commutes. I.e., we need to show that for $x \in X$, we have

$$\phi(x) = \widetilde{\phi}(\pi(x)).$$

Consider $y = \pi(x) \in X/\sim$. Since x is *an* element that maps to y by means of π, the required equality follows from the definition of $\widetilde{\phi}$.

□

Week 1, HW Problem 7. *Let us be in the situation of Proposition 2.2.13.*

(a) *Show that $\widetilde{\phi}$ is surjective if and only if ϕ is.*

(b) *Show that $\widetilde{\phi}$ is injective if and only if whenever $\phi(x_1) = \phi(x_2)$, we have $x_1 \sim x_2$.*

2.3. **Subgroups and equivalence relations.** Here we formalize our example picking out the evens and odds as cosets in $\mathbb{Z}$, keeping in mind that $\mathbb{Z}$ is commutative, while a random group might not be.

Let A be a group and $A' \subset A$ a subgroup. We define the *left* relation on A with respect to A' by declaring that for two elements $a_1, a_2 \in A$, we have $a_1 \sim a_2$ if and only if there exists an element $a' \in A$ such that

$$a_2 = a' \cdot a_1.$$

Note that if a' as above exists, it equals $a_2 \cdot (a_1)^{-1}$. Indeed,

$$a_2 \cdot (a_1)^{-1} = a' \cdot a_1 \cdot (a_1)^{-1} = a'.$$

Hence, we can equivalently say that

$$a_1 \sim a_2 \Leftrightarrow a_2 \cdot (a_1)^{-1} \in A'.$$

Lemma 2.3.1. *The above relation is an equivalence relation.*

Proof. We have $a = 1 \cdot a$ while $1 \in A'$. Hence $a \sim a$. If $a_2 = a' \cdot a_1$ then $a_1 = (a')^{-1} \cdot a_2$, and if $a' \in A'$, then $(a')^{-1} \in A'$. Hence $a_1 \sim a_2 \Rightarrow a_2 \sim a_1$. Finally, if

$$a_2 = a' \cdot a_1 \text{ and } a_3 = a'' \cdot a_2 \text{ then } a_3 = (a'' \cdot a') \cdot a_1,$$

and if $a', a'' \in A'$, then $a'' \cdot a' \in A'$. Hence

$$a_1 \sim a_2 \text{ and } a_2 \sim a_3 \Rightarrow a_1 \sim a_3.$$

□

NB: We shall sometimes denote the above equivalence relation by $\sim^l$, where "l" stands for "left". We shall denote the quotient set $A/\sim^l$ by $A'\backslash A$.

2.3.2. We define the *right* relation on A with respect to A' by declaring that for two elements $a_1, a_2 \in A$, we have $a_1 \sim a_2$ if and only if there exists an element $a' \in A$ such that

$$a_2 = a_1 \cdot a'.$$

We have:

Lemma 2.3.3. *The right relation on A is an equivalence relation.*

Proof. The same as for the left relation. □

NB: We shall sometimes denote the right equivalence relation by $\sim^r$, where "r" stands for "right". We shall denote the quotient set $A/\sim^r$ by A/A'.

2.3.4. *Normal subgroups.* Recall that we had defined how two groups "talk to" each other: via homomorphisms. Given a homomorphism, we also found two interesting subgroups associated to it: its kernel and image. If $A' \subset A$ is a subgroup, then the tautological inclusion map $A' \to A$ exhibits A' as the image of a homomorphism. So images of homomorphisms are rather boring.

But it turns out that kernels of homomorphisms are very much not boring. You might imagine a homomorphism as squishing one object into another (and maybe not taking up all of the space), potentially crushing some parts completely. Here you should see an example of the blurring of vision mentioned before: we study an object by all of its collections of blobs, which we've now called quotients. Given that quotients are important, and that kernels exactly determine quotients (which we'll see later), evidently it makes sense to study which subgroups can be kernels. We do that here.

Definition 2.3.5. *Let $A' \subset A$ be a subgroup. We shall say that A' is* normal *if for every $a \in A$ and $a' \in A'$, the element*

$$a \cdot a' \cdot a^{-1}$$

also belongs to A'.

Note that if A is abelian, then any subgroup is normal. Indeed, in this case

$$a \cdot a' \cdot a^{-1} = a \cdot a^{-1} \cdot a' = a'.$$

Week 1, HW Problem 8. *Let $\phi : A \to B$ be a homomorphism. Show that* $\ker(\phi)$ *is always a normal subgroup.*

We want to go in the opposite direction. To do this, we'll use our previously developed knowledge about equivalence relations.

2.3.6. *Normality and cosets.* We are going to prove:

Lemma 2.3.7. *Suppose that $A' \subset A$ is normal. Then the left and right equivalence relations on A with respect to A' coincide.*

Proof. We need to show that $a_1 \sim^l a_2$ implies $x_1 \sim^r a_2$, and vice versa. Suppose $a_2 = a' \cdot a_1$. Then

$$a_2 = a_1 \cdot ((a_1)^{-1} \cdot a' \cdot a_1).$$

If $a' \in A$, then $(a_1)^{-1} \cdot a' \cdot a_1 \in A'$, since A' was assumed normal.

The implication $x_1 \sim^r a_2 \Rightarrow x_1 \sim^l a_2$ is proved similarly. □

Week 1, HW Problem 9. *Let $A' \subset A$ be a subgroup such that $\sim^l$ is the same as $\sim^r$. Show that A' is normal.*

2.3.8. *Quotient by a normal subgroup.* Let A be a group and $A' \subset A$ be a normal subgroup. According to Lemma 2.3.7, left cosets on A with respect to A' are the same as right cosets. I.e., the quotient sets A/A' and $A' \backslash A$ are the same.

We now claim:

Theorem 2.3.9. *If A is a normal subgroup of A, the set A/A' has a unique group structure for which the map $\pi : A \to A/A'$ is a group homomorphism.*

Week 1, HW Problem 10. *Write a complete proof of Theorem 2.3.9. Suggested strategy: use the same idea as in the proof of Proposition 2.2.13.*

So now we have our converse: observe that $\ker(\pi) = A'$, whence normal subgroups and kernels of homomorphisms exactly coincide.

3. Tuesday, Sept. 11

3.1. **The first isomorphism theorem.**

3.1.1. Let's study how this quotient guy talks to other groups. That is to say, let's ask ourselves what it takes to write down a map out of this object, since if we have a map out $A/A' \to B$, we can just precompose with $A \to A/A'$ to get a map $A \to B$ via $A \to A/A' \to B$.

Theorem 3.1.2. *Let $\phi : A \to B$ be a group homomorphism, and let $A' \subset A$ be a normal subgroup such that ϕ sends A' to 1_B, i.e., $A' \subset \ker(\phi)$. Then there exists a unique group homomorphism $\widetilde{\phi} : A/A' \to B$ such that the triangle*

$$\begin{tikzcd}
A \arrow[r, "\phi"] \arrow[d, "\pi"'] & B. \\
A/A' \arrow[ur, "\widetilde{\phi}"'] &
\end{tikzcd}$$

commutes.

Week 2, HW Problem 1.

(a) *Write a complete proof of theorem 3.1.2.*

(b) *Show that* $\mathrm{Im}(\phi) = \mathrm{Im}(\widetilde{\phi})$.

(c) *Show that* $\widetilde{\phi}$ *is injective if and only if the inclusion* $A' \subset \ker(\phi)$ *is an equality.*

3.1.3. Let $\phi : A \to B$ be again a group homomorphism. Set $A' = \ker(\phi)$. By [Problem 8, Week 1], A' is a normal subgroup. By 3.1.2, we obtain a group homomorphism

$$\phi : A/A' \to B.$$

Furthermore, by [Problem 1, Week 2](b) above, the image of the above homomorphism $\widetilde{\phi}$ equals $\mathrm{Im}(\phi)$.

Hence, we obtain a group homomorphism

$$A/\ker(\phi) \to \mathrm{Im}(\phi). \tag{2}$$

Theorem 3.1.4. *The homomorphism* (2) *is an isomorphism.*

Proof. By [Problem 2, Week 1], it suffices to show that map in question is injective and surjective. It is surjective by [Problem 1, Week 2](b). It is injective by [Problem 1, Week 2](a). □

The above corollary is called "the first isomorphism theorem," but giving it a name makes it seem like something you should remember on its own. You shouldn't. This theorem will soon become second- or third-nature — what it tells us is that if we find ourselves with a map that loses some information, squinting our eyes enough (so that the kernel looks like a point) will make it look like an inclusion.

3.1.5. As a particular case of Theorem 3.1.4, we have:

Corollary 3.1.6. *Let* $\phi : A \to B$ *be a surjective group homomorphism. Then the homomorphism*

$$\widetilde{\phi} : A/\ker(A') \to B,$$

given by Theorem 3.1.2, is an isomorphism.

3.1.7. *Example.* Take $A = \mathbb{Z}_6, B = \mathbb{Z}_3$, and $A \to B$ the reduction mod 3 map. This tells us that, since the kernel is $3\mathbb{Z}_6$, $\mathbb{Z}_6/3\mathbb{Z}_6 \simeq \mathbb{Z}_3$.

3.2. **The second isomorphism theorem.** In this section we let A be a group, $A_1 \subset A$ be a subgroup, and $A_2 \subset A$ be a normal subgroup.

3.2.1. Let $A_1 \cdot A_2 \subset A$ be the subset of elements that can be written as products $a_1 \cdot a_2$, with $a_1 \in A_1$ and $a_2 \in A_2$.

Week 2, HW Problem 2. *Show that* $A_1 \cdot A_2$ *is a subgroup of* A.

3.2.2. Note that A_2 is contained in $A_1 \cdot A_2$. Since A_2 is normal in A, it is also normal in $A_1 \cdot A_2$ (prove it!). Hence, we can form the quotient group

$$(A_1 \cdot A_2)/A_2.$$

This group will be the right-hand side in the second isomorphism theorem.

3.2.3. We have:

Week 2, HW Problem 3. *Let A be a group, and A', A'' two subgroups.*

(a) *Show that $A' \subset A''$ is also a subgroup.*

(b) *Show that if both A' and A'' are normal, then so is $A' \subset A''$.*

(c) *Show that if A'' is normal in A, then $A' \cap A''$ is normal in A'.*

3.2.4. From [Problem 3, Week 2](c) we obtain that $A_1 \cap A_2$ is a normal subgroup of A_1. Hence, we can form the quotient group

$$A_1/A_1 \cap A_2.$$

This group will be the left-hand side in the second isomorphism theorem.

3.2.5. Consider the inclusion $A_1 \hookrightarrow (A_1 \cdot A_2)$, considered as a group homomorphism. We let

$$\phi : A_1 \to (A_1 \cdot A_2)/A_2$$

denote its composition with the map $A_1 \cdot A_2 \to (A_1 \cdot A_2)/A_2$.

Week 2, HW Problem 4.

(a) *Show that the kernel of the above map $\phi : A_1 \to (A_1 \cdot A_2)/A_2$ equals $A_1 \cap A_2$.*

(b) *Show that the above map $\phi : A_1 \to (A_1 \cdot A_2)/A_2$ is surjective.*

3.2.6. Using [Week 2, HW Problem 4](a) and Theorem 3.1.2 we obtain a group homomorphism:

$$A_1/A_1 \cap A_2 \to (A_1 \cdot A_2)/A_2. \tag{3}$$

We have:

Theorem 3.2.7. *The map* (3) *is an isomorphism.*

Proof. This follows from Corollary 3.1.6 using [Week 2, HW Problem 4](a) and [Week 2, HW Problem 4](b). □

In essence we may "cancel" groups as we would fractions, except for the (now obvious) exceptions (i.e., $A_1 \cap A_2$ above).

3.2.8. *Example.* Here's a simple question related to cancelling. We have $\mathbb{Z}_3$ as the quotient $\mathbb{Z}/3\mathbb{Z}$. What about $10\mathbb{Z}/30\mathbb{Z}$? Can't we just cancel the 10s? Well, take $A_1 = 10\mathbb{Z}, A_2 = 3\mathbb{Z}$, and $A = \mathbb{Z}$. Note that $A_1 \cdot A_2 = \{10x+3y | x, y \in \mathbb{Z}\} = \mathbb{Z}$ since 3 and 10 are relatively prime. For the same reason, $A_1 \cap A_2 = 30\mathbb{Z}$. Hence, by second isomorphism, the inclusion $10\mathbb{Z} \to \mathbb{Z}$ induces an isomorphism $10\mathbb{Z}/30\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z}$.

You should not be shocked, because there is nothing shocking about this result. It really is just cancellation formalized. But note that it sweeps away all of the case-by-case nonsense we might have done had we sit down and tried to generalize this $10\mathbb{Z}/30\mathbb{Z}$ observation. (Not that we would have anyway!)

3.3. **The third isomorphism theorem.** Let A be a group, and $A_1 \subset A_2 \subset A$ be two normal subgroups. In particular, A_1 is a normal subgroup in A_2. The third isomorphism theorem establishes a relation between the quotients A/A_1, A/A_2 and A_2/A_1.

3.3.1. Consider the tautological map $A_2 \to A$, and let ϕ_1 denote the composed map

$$A_2 \to A \to A/A_1.$$

It is easy to see (prove it!) that $\ker(\phi_1) = A_1$.

Hence, by Theorem 3.1.2 we obtain a group hohomorphism

$$\widetilde{\phi}_1 : A_2/A_1 \to A/A_1.$$

Note that $\widetilde{\phi}_1$ is injective by [Week 2, HW Problem 1](c). Hence, by Theorem 3.1.4, the homomorphism $\widetilde{\phi}_1$ defines an isomorphism

$$A_2/A_1 \to \operatorname{Im}(\widetilde{\phi}_1). \tag{4}$$

3.3.2. Consider the map $\phi_2 : A \to A/A_2$. Note that $A_1 \subset \ker(\phi_2)$. Hence, by Theorem 3.1.2 we obtain a group hohomorphism

$$\widetilde{\phi}_2 : A/A_1 \to A/A_2.$$

Note that $\widetilde{\phi}_2$ is surjective by [Week 2, HW Problem 1](b).

Week 2, HW Problem 5. *Show that* $\ker(\widetilde{\phi}_2) = \operatorname{Im}(\widetilde{\phi}_1)$.

Hence, by Theorem 3.1.2, we obtain a group homomorphism

$$(A/A_1)/(A_2/A_1) \to A/A_2. \tag{5}$$

NB: In the above formula we are abusing the notation slightly: properly speaking we should write $(A/A_1)/\operatorname{Im}(\widetilde{\phi}_1)$ rather than $(A/A_1)/(A_2/A_1)$. We are identifying A_2/A_1 and $\operatorname{Im}(\widetilde{\phi}_1)$ via the isomorphism (4).

Theorem 3.3.3. *The map* (5) *is an isomorphism.*

Proof. This follows from Corollary 3.1.6 and [Week 2, HW Problem 5]. □

Again, we can cancel as we might have hoped.

3.4. Rings.

3.4.1. A ring is a set R with two operations:

- A map add : $R \times R \to R$, which makes R into a commutative group; the corresponding operation will be denoted
$$r_1, r_2 \mapsto r_1 + r_2,$$
and the unit is denoted by 0.
- A map mult : $R \times R \to R$, which makes R into a monoid; the corresponding operation will be denoted
$$r_1, r_2 \mapsto r_1 \cdot r_2,$$
and the unit is denoted by 1.
- For any $r, r_1, r_2 \in R$ we have
$$r \cdot (r_1 + r_2) = r \cdot r_1 + r \cdot r_2 \text{ and } (r_1 + r_2) \cdot r = r_1 \cdot r + r_2 \cdot r.$$

NB: What we call above a "ring" is sometimes called a "unital ring". I.e., in this course all rings will be assumed unital.

A ring is called commutative if the monoid structure on it with respect to mult is commutative.

3.4.2. *Examples.*

(i) $R = \mathbb{Z}$ with the usual addition and multiplication.

(ii) $R = \mathbb{R}$ with the usual addition and multiplication.

(iii) $R = \mathbb{C}$ with the usual addition and multiplication.

(iv) $R = \mathbb{R}[t]$, the set of polynomials in one variable, with the usual addition and multiplication.

(v) $R = \mathbb{R}[t_1, \ldots, t_n]$, the set of polynomials in n variables, with the usual addition and multiplication.

All of the above rings are commutative.

(vi) $R = \mathrm{Mat}_{n\times n}(\mathbb{R})$, the set of real-valued $n \times n$-matrices, with the usual addition and multiplication. This ring is non-commutative.

3.4.3. *Some properties.* We have:

Lemma 3.4.4. *For any $r \in R$,*

$$r \cdot 0 = 0 = 0 \cdot r.$$

Proof.

$$r \cdot 0 + r \cdot 0 = r \cdot (0 + 0) = r \cdot 0.$$

Hence, $r \cdot 0 = 0$ by Lemma 1.2.4. The fact that $0 \cdot r = 0$ is proved similarly. □

4. Thursday, Sept. 13

4.1. **Rings, continued.** Let R be a ring. We have:

Lemma 4.1.1. *For every $r \in R$, $(-1) \cdot r = -r$.*

Proof. We need to show that $(-1) \cdot r + r = 0$. We have

$$(-1) \cdot r + r = (-1) \cdot r + 1 \cdot r = ((-1) + 1) \cdot r = 0 \cdot r,$$

which equals 0 by Lemma 3.4.4. □

4.1.2. *Fields.* We shall say that a ring R is a field if:

- The elements 0 and 1 in R are distinct;
- $R - \{0\} \subset R$ is a sub-monoid, i.e., $r_1, r_2 \neq 0 \Rightarrow r_1 \cdot r_2 \neq 0$;
- $R - \{0\}$ is a group, i.e., every non-zero element admits a multiplicative inverse.

NB: We usually denote fields by letters k, K or F.

4.1.3. *Examples.*

(i) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

(ii) $\mathbb{Z}$ is not a field.

(iii) $\mathbb{C}[t]$ is not a field.

4.2. **Modules.** For the rest of this lecture we fix a ring R.

4.2.1. An R-module is an abelian group M, with an additional structure of a map

$$act_M : R \times M \to M, \quad r, m \mapsto r \cdot m,$$

such that the following properties hold:

- For every $m \in M$, we have $1 \cdot m = m$;
- For every $r_1, r_2 \in R$ and $m \in M$, we have $r_1 \cdot (r_2 \cdot m) = (r_1 \cdot r_2) \cdot m$;
- For every $r_1, r_2 \in R$ and $m \in M$, we have $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$;
- For every $r \in R$ and $m_1, m_2 \in M$, we have $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.

Note that the last property is equivalent to saying that for every $r \in R$, the map

$$M \to M, \quad m \mapsto r \cdot m$$

is a group homomorphism.

4.2.2. Here are some basic facts about modules.

Lemma 4.2.3. *For any $r \in R$ we have $r \cdot 0_M = 0_M$. For any $m \in M$, we have $0_R \cdot m = 0_M$ and $(-1) \cdot m = -m$.*

Proof. The same as Lemmas 3.4.4 and 4.1.1. □

4.2.4. *Terminology.* When the ring R is a field k, instead of saying "R-module" we usuall say "k-vector space", or just "vector space" if k is fixed. We shall most typically use symbols V and W for vector spaces (rather than M and N used for modules over general rings).

4.2.5. *Examples.*

(i) The 0 module (i.e., M has only the element 0) is an R-module.

(ii) Take $M = R$, with the structure of abelian group the same as on R. We define $act_M := mult_R$. The module axioms follow from the ring axioms on R.

(iii) Take $M = R^{\times 2} := R \times R$. The abelian group structure is defined "componentwise" — i.e., by

$$(r_1', r_1'') + (r_2', r_2'') = (r_1' + r_2', r_1'' + r_2'').$$

The action of R is also defined componentwise, by

$$r \cdot (r_1, r_2) = (r \cdot r_1, r \cdot r_2).$$

(iv) Generalizing example (iii), we can take $M = R^{\times n}$ for any positive integer n.

4.2.6. *Modules over $\mathbb{Z}$.* Let us consider the example of $R = \mathbb{Z}$. We claim that any abelian group A carries a natural (uniquely defined!) structure of $\mathbb{Z}$-module.

Indeed, whatever this structure is for $a \in A$ we need to have

$$1 \cdot a = a.$$

Week 2, HW Problem 6. *Show that if the above $\mathbb{Z}$-module structure is well-defined, it is given by*

$$n \cdot a = \underbrace{a + \cdots + a}_{n}, \quad n > 0$$

and

$$n \cdot a = -\underbrace{(a + \cdots + a)}_{n}, \quad n > 0.$$

Week 2, HW Problem 7. *Show that for any abelian group A, the above formulas define a structure of $\mathbb{Z}$-module on A. Deduce that there is a bijection between $\mathbb{Z}$-modules and abelian groups.*

Note that the above bijection is actually meaningful, and not just some strange thing that exists for cardinality reasons (admittedly, both sides aren't even sets, but let's ignore that for now!).

4.3. **Homomorphisms of R-modules.** You should be getting the hang of this. That is to say, on being given a new mathematical object, the first thing to study is how it talks to other, similar objects, and then whether it has any tractable subobjects or quotients (and how it can be recovered from knowledge of these).

4.3.1. Let M_1 and M_2 be R-modules. An R-module homomorphism from M_1 to M_2 is a map of sets $\phi : M_1 \to M_2$ such that:

- ϕ is a group homomorphism.
- For every $r \in R$ and $m \in M$, we have $\phi(r \cdot m) = r \cdot \phi(m)$.

Note that the last condition can be phrased as commutation of the diagram

$$\begin{tikzcd}
R \times M_1 \arrow[r, "\mathrm{id} \times \phi"] \arrow[d, "act_{M_1}"'] & R \times M_2 \arrow[d, "act_{M_2}"] \\
M_1 \arrow[r, "\phi"] & M_2.
\end{tikzcd}$$

4.3.2. *Terminology.* The set of R-module homomorphisms $M_1 \to M_2$ is denoted $\mathrm{Hom}_{R\text{-mod}}(M_1, M_2)$, or simply $\mathrm{Hom}_R(M_1, M_2)$.

In addition to "R-module homomorphism" we shall also say "R-linear map", or just "map of R-modules". When R is a field k, and so M_1 and M_2 are vector spaces V_1 and V_2 respectively, we will also use"linear transformation from V_1 to V_2."

4.3.3. *Compositions.* Let $\phi : M_1 \to M_2$ and $\psi : M_2 \to M_3$ be R-module homomorphisms. Then it is easy to see that the composed map

$$\psi \circ \phi : M_1 \to M_3$$

is also an R-module homomorphism.

We can regard the operation of composition as a map of sets

$$\mathrm{Hom}_R(M_2, M_3) \times \mathrm{Hom}_R(M_1, M_2) \to \mathrm{Hom}_R(M_1, M_3). \tag{6}$$

4.4. **Free modules.** How do those examples of modules we gave above talk to other modules?

4.4.1. Let M be an arbitrary R-module. Consider the set $\mathrm{Hom}_R(R, M)$, where R is considered as an R-module as in Example 4.2.5(ii).

We define the map of sets (which we might call "evaluation at 1")

$$\mathrm{ev} : \mathrm{Hom}_R(R, M) \to M$$

by sending $\phi \in \mathrm{Hom}_R(R, M)$ to the element

$$\mathrm{ev}(\phi) := \phi(1) \in M.$$

Week 2, HW Problem 8. *Prove that the map* ev *defined above is a bijection of sets.*

That is to say, to give a map of modules $R \to M$ is just the same thing as to give an element of M.

Suggested strategy for the above problem: Define a map $T : M \to \mathrm{Hom}_R(R, M)$ by sending $m \in M$ to the R-module homomorphism $\phi_m : R \to M$, defined by the formula $\phi_m(r) := r \cdot m$. Prove that this is indeed an R-module homomorphism, and that resulting maps

$$\mathrm{Hom}_R(R, M) \underset{T}{\overset{\mathrm{ev}}{\rightleftarrows}} M$$

are mutually inverse.

4.4.2. We again take M to be an arbitrary R-module. Consider now the set $\mathrm{Hom}_R(R^{\times 2}, M)$, where $R^{\times 2}$ is considered as an R-module as in Example 4.2.5(iii).

We define the map of sets

$$\mathrm{ev} : \mathrm{Hom}_R(R^{\times 2}, M) \to M \times M$$

by sending $\phi \in \mathrm{Hom}_R(R^{\times 2}, M)$ to the pair of elements

$$\mathrm{ev}(\phi) := (\phi(1, 0), \phi(0, 1)) \in M \times M.$$

Week 2, HW Problem 9. *Prove that the map* ev *defined above is a bijection of sets.*

Generalizing the above construction, we obtain a bijection

$$\mathrm{ev} : \mathrm{Hom}_R(R^{\times n}, M) \to M^{\times n}.$$

4.4.3. In particular, taking $M = R^{\times m}$, we obtain a bijection

$$\mathrm{ev} : \mathrm{Hom}_R(R^{\times n}, R^{\times m}) \simeq (M^{\times m})^{\times n}.$$

Note that we can think of elements of $(M^{\times m})^{\times n}$ as n-tuples of m-tuples of elements of R. Thus, the set $(M^{\times m})^{\times n}$ is in a bijection with the set $\mathrm{Mat}_{m\times n}(R)$ of $(m \times n)$-matrices with values in R (here m is the height and n is the width in the usual convention).

4.4.4. Let now fix three positive integers n_1, n_2, n_3. We have the bijections

$$\mathrm{Hom}_R(R^{\times n_1}, R^{\times n_2}) \simeq \mathrm{Mat}_{n_1\times n_2}(R),\ \mathrm{Hom}_R(R^{\times n_2}, R^{\times n_3}) \simeq \mathrm{Mat}_{n_2\times n_3}(R)$$

and

$$\mathrm{Hom}_R(R^{\times n_1}, R^{\times n_3}) \simeq \mathrm{Mat}_{n_1\times n_3}(R).$$

Consider the composition map

$$\mathrm{Hom}_R(R^{\times n_2}, R^{\times n_3}) \times \mathrm{Hom}_R(R^{\times n_1}, R^{\times n_2}) \to \mathrm{Hom}_R(R^{\times n_1}, R^{\times n_3})$$

of (6).

Week 2, HW Problem 10. *Show that the following diagram of maps of sets commutes*

$$\begin{tikzcd}
\mathrm{Hom}_R(R^{\times n_2}, R^{\times n_3}) \times \mathrm{Hom}_R(R^{\times n_1}, R^{\times n_2}) \arrow[r] \arrow[d, "\mathrm{ev} \times \mathrm{ev}"'] & \mathrm{Hom}_R(R^{\times n_1}, R^{\times n_3}) \arrow[d, "\mathrm{ev}"] \\
\mathrm{Mat}_{n_2\times n_3}(R) \times \mathrm{Mat}_{n_1\times n_2}(R) \arrow[r] & \mathrm{Mat}_{n_1\times n_3}(R),
\end{tikzcd}$$

where the bottom arrow is the map given by matrix multiplication.

4.5. **Submodules and quotient modules.**

4.5.1. Let M be an R-module. A subset $M' \subset M$ is called an R-submodule if:

- M' is a subgroup;
- For every $r \in R$ and $m \in M'$, the element $r \cdot m$ also belongs to M'.

As in [Problem 4, Week 1], an R-submodule M' itself acquires a structure of R-module via

$$r, m \mapsto r \cdot m,$$

where the operation is taken inside M.

We have:

Lemma 4.5.2. *Let $\phi : M_1 \to M_2$ be a homomorphism of R-modules. Then* $\ker(\phi) \subset M_1$ *and* $\mathrm{Im}(\phi) \subset M_2$ *are submodules.*

Proof. Same as [Problems 5 and 6, Week 1]. □

4.5.3. Let M be an R-module, and $M' \subset M$ a submodule.

Proposition 4.5.4. *The quotient group M/M' has a unique structure of R-module such that the map*

$$\pi : M \to M/M'$$

is a homomorphism of R-modules.

Proof. First, we claim that for every $r \in R$ there exists a unique group homomorphism

$$act_{M/M'}(r) : M/M' \to M/M'$$

which makes the diagram

$$\begin{tikzcd} M \arrow[r, "act_M(r)"] \arrow[d, "\pi"'] & M \arrow[d, "\pi"] \\ M/M' \arrow[r, "act_{M/M'}(r)"] & M/M' \end{tikzcd} \tag{7}$$

commute.

Indeed, we consider the clock-wise circuit as a map of groups $\phi_r : M \to M/M'$. We claim that $M' \subset \ker(\phi_r)$. Indeed, for $m \in M'$, we have

$$\pi \circ act_M(r)(m) = \pi(r \cdot m).$$

Now, $r \cdot m$ belongs to M', and so π sends M' to 0.

Existence and uniqueness of $act_{M/M'}(r)$ follow from Theorem 3.1.2.

Let us check that the map

$$R \times M/M' \to M/M', \quad r, \bar{m} \mapsto r \cdot \bar{m} := act_{M/M'}(r)(\bar{m})$$

indeed defines a structure of R-module on M/M'.

By definition, for every fixed r, the map

$$\bar{m} \mapsto r \cdot \bar{m}$$

is a group homomorphism. Hence, it remains to verify three properties:

- $1 \cdot \bar{m} = \bar{m}$, for all $\bar{m} \in M/M'$.
- $r_1 \cdot (r_2 \cdot \bar{m}) = (r_1 \cdot r_2) \cdot \bar{m}$, for all $\bar{m} \in M/M'$, $r_1, r_2 \in R$.
- $(r_1 + r_2) \cdot \bar{m} = r_1 \cdot \bar{m} + r_2 \cdot \bar{m}$, for all $\bar{m} \in M/M'$, $r_1, r_2 \in R$.

Let us verify the second of these properties (the other two are checked similarly). For a given $\bar{m} \in M/M'$ choose $m \in M$ so that $\pi(m) = \bar{m}$. We have

$$r_1 \cdot (r_2 \cdot \bar{m}) = r_1 \cdot (r_2 \cdot \pi(m)),$$

using (7), we have:

$$r_1 \cdot (r_2 \cdot \pi(m)) = r_1 \cdot (\pi(r_2 \cdot m)) = \pi(r_1 \cdot (r_2 \cdot m)) = \pi((r_1 \cdot r_2) \cdot m) = (r_1 \cdot r_2) \cdot \pi(m),$$

which is the same as $(r_1 \cdot r_2) \cdot \bar{m}$, as required.

Finally, the fact that π is an R-module homomorphism follows from the commutativity of (7).

□

5. Tuesday, Sept. 18

5.1. **Quotient modules, continued.**

5.1.1. *Addendum to the previous lecture.* Let $\phi : M \to N$ be a homomorphism of R-modules.

Lemma 5.1.2. *Suppose that ϕ is bijective as a map of sets. Then the uniquely defined set-theoretic inverse $\psi : N \to M$ is an R-module homomorphism.*

The proof is the same as [Problem 2, Week 1]. Hence, we obtain that bijective R-module homomorphisms are isomorphisms.

5.1.3. Let $\phi : M \to N$ be a homomorphism of R-modules, and let $M' \subset M$ be an R-submodule such that $\phi|_{M'} = 0$.

We claim:

Proposition 5.1.4. *There exists a unique homomorphism of R-modules*

$$\widetilde{\phi} : M/M' \to N$$

such that the triangle

$$\begin{tikzcd}
M \arrow[rr, "\phi"] \arrow[d, "\pi"'] & & N. \\
M/M' \arrow[urr, "\widetilde{\phi}"'] & &
\end{tikzcd}$$

commutes.

Proof. The existence and uniqness of $\widetilde{\phi} : M/M' \to N$ as a group homomorphism follows from Theorem 3.1.2. It remains to show that $\widetilde{\phi}$ is a homomorphism of R-modules. I.e., we need to show that for any $r \in R$, the diagram

$$\begin{tikzcd}
M/M' \arrow[r, "act_{M/M'}(r)"] \arrow[d, "\widetilde{\phi}"'] & M/M' \arrow[d, "\widetilde{\phi}"] \\
N \arrow[r, "act_N(r)"] & N
\end{tikzcd}$$

commutes.

However, this follows from the fact that in the diagram

$$\begin{tikzcd}
M \arrow[r, "act_M(r)"] \arrow[d, "\pi"'] & M \arrow[d, "\pi"] \\
M/M' \arrow[r, "act_{M/M'}(r)"] \arrow[d, "\widetilde{\phi}"'] & M/M' \arrow[d, "\widetilde{\phi}"] \\
N \arrow[r, "act_N(r)"] & N
\end{tikzcd}$$

the top and the outer square commute, and the upper left vertical arrow is surjective, see Lemma 2.2.14.

□

5.1.5. *Short exact sequences.* Let

$$\phi : M_1 \to M \text{ and } \psi : M \to M_2$$

be R-module homomorphisms.

We shall say that

$$0 \to M_1 \to M \to M_2 \to 0$$

is a *short exact sequence* if

- ϕ is injective;
- ψ is surjective;
- $\mathrm{Im}(\phi) = \ker(\psi)$.

Let us denote $M' := \mathrm{Im}(\phi)$; this is an R-submodule of M by Lemma 4.5.2. By the first isomorphism theorem (Theorem 3.1.4), the map ϕ defines an isomorphism

$$M_1 \to M'.$$

For the same reason, the induced map

$$\widetilde{\psi} : M/M' \to M_2$$

is an isomorphism.

So, every short exact sequence looks like this:

$$\begin{tikzcd}
 & M_1 \arrow[d, "\sim"'] & & & \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M/M' \arrow[r] \arrow[d, "\sim"] & 0 \\
 & & & M_2 &
\end{tikzcd}$$

where $M' \to M$ is the inclusion of a submodule, and $M \to M/M'$ is the canonical projection.

5.2. **Direct sums.**

5.2.1. Let M_1 and M_2 be a pair of R-modules. Consider the set $M := M_1 \times M_2$, equipped with the two projections

$$p_1 : M \to M_1 \text{ and } p_2 : M \to M_2.$$

It is easy to see that M carries a unique structure of R-module for which the maps p_1 and p_2 are R-module homomorphisms.

Explicitly, for $(m_1', m_2') \in M_1 \times M_2$ and $(m_1'', m_2'') \in M_1 \times M_2$ we set

$$(m_1', m_2') + (m_1'', m_2'') = (m_1' + m_1'', m_2' + m_2'').$$

And for $r \in R$ and $(m_1, m_2) \in M$,

$$r \cdot (m_1, m_2) = (r \cdot m_1, r \cdot m_2).$$

We denote $M := M_1 \times M_2$ with the above structure of R-module by $M_1 \oplus M_2$.

5.2.2. Let N be another R-module. Consider the map of sets

$$\mathrm{Hom}_R(N, M_1 \oplus M_2) \to \mathrm{Hom}_R(N, M_1) \times \mathrm{Hom}_R(N, M_2) \tag{8}$$

that sends $\phi \in \mathrm{Hom}_R(N, M_1 \oplus M_2)$ to the element

$$(\phi_1, \phi_2) \in \mathrm{Hom}_R(N, M_1) \times \mathrm{Hom}_R(N, M_2)$$

where

$$\phi_1 = p_1 \circ \phi \text{ and } \phi_2 = p_2 \circ \phi.$$

Week 3, HW Problem 1. *Show that the map in* (8)*, constructed above, is an isomorphism.*

The assertion in the above problem can be reformulated as follows: to specify a map $N \to M_1 \oplus M_2$ is the same as to specify a pair of maps $N \to M_1$ and $N \to M_2$.

5.2.3. Note that we have the maps

$$i_1 : M_1 \to M_1 \oplus M_2 \text{ and } i_2 : M_2 \to M_1 \oplus M_2,$$

where

$$i_1(m_1) = (m_1, 0) \text{ and } i_2(m_2) = (0, m_2).$$

In terms of the bijection of [Problem 1, Week 3], the map i_1 corresponds to the pair $(\mathrm{id}_{M_1}, 0)$ and $(0, \mathrm{id}_{M_2})$, where 0 is the zero homomorphism (which collapses everything to 0).

5.2.4. For a module N we define a map of sets

$$\mathrm{Hom}_R(M_1 \oplus M_2, N) \to \mathrm{Hom}_R(M_1, N) \times \mathrm{Hom}_R(M_2, N) \tag{9}$$

that sends $\phi \in \mathrm{Hom}_R(M_1 \oplus M_2, N)$ to the element

$$(\phi_1, \phi_2) \in \mathrm{Hom}_R(M_1, N) \times \mathrm{Hom}_R(M_2, N)$$

where

$$\phi_1 = \phi \circ i_1 \text{ and } \phi_2 = \phi \circ i_2.$$

Week 3, HW Problem 2. *Show that the map in* (9)*, constructed above, is an isomorphism.*

The assertion in the above problem can be reformulated as follows: to specify a map $M_1 \oplus M_2 \to N$ is the same as to specify a pair of maps $M_1 \to N$ and $M_2 \to N$.

5.2.5. *Splittings of short exact sequences.* The material in this subsection was not part of the lecture. You will develop it in the form of a problem.

Let

$$0 \to M_1 \overset{\phi}{\to} M \overset{\psi}{\to} M_2 \to 0 \tag{10}$$

be a short exact sequence.

We define a *splitting* of the short exact sequence to be an isomorphism of modules

$$\xi : M \to M_1 \oplus M_2$$

such that

- $\xi \circ \phi = i_1$ as maps $M_1 \to M_1 \oplus M_2$;
- $\psi = p_2 \circ \xi$ as maps $M \to M_2$.

We let $\mathrm{Split}(M)$ denote the set of splittings, i.e., the set of isomorphisms ξ satisfying the above conditions.

We define a map from $\mathrm{Split}(M)$ to the set of $\text{L-inv}(\phi)$ of left inverses of the map ϕ (i.e., maps $q : M \to M_1$, such that $q \circ \phi = \mathrm{id}_{M_1}$) by sending ξ to the map $p_1 \circ \xi$.

We define a map from $\mathrm{Split}(M)$ to the set of $\text{R-inv}(\psi)$ of right inverses of the map ψ (i.e., maps $j : M_2 \to M$, such that $\psi \circ j = \mathrm{id}_{M_2}$) by sending ξ to the map $\xi^{-1} \circ i_2$, where ξ^{-1} is the map inverse to ξ.

Week 3, HW Problem 3. *Show that the maps*

$$\text{L-inv}(\phi) \leftarrow \mathrm{Split}(M) \to \text{R-inv}(\psi),$$

defined above, are isomorphisms.

Week 3, HW Problem 4. *Show that the short exact sequence*

$$0 \to \mathbb{Z} \overset{2\cdot -}{\to} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

does not admit a splitting.

5.3. **Generation and linear dependence.**

5.3.1. Let M be an R-module, and let us go back to the setting of [Problem 9, Week 2]. I.e. we have a bijection of sets

$$\mathrm{ev} : \mathrm{Hom}_R(R^{\oplus n}, M) \to M^{\times n}$$

that sends an element $\phi \in \mathrm{Hom}_R(R^{\oplus n}, M)$ to the n-tuple $(m_1, \ldots, m_n)$, where

$$m_i = \phi(e_i), \quad e_i = (0, \ldots, 0, 1, 0, \ldots, 0), \text{ 1 in the i-th slot.}$$

Let $\phi : R^{\oplus n} \to M$ be a map, and let $(m_1, \ldots, m_n)$ be the corresponding n-tuple of elements of M.

Lemma 5.3.2. *The following conditions are equivalent:*

(i) *The map ϕ is surjective;*

(ii) *For every $m \in M$ there exist elements $r_1, \ldots, r_n \in R$ such that*

$$m = r_1 \cdot m_1 + \cdots + r_n \cdot m_n.$$

The proof is immediate.

Definition 5.3.3. *We shall say that the elements $(m_1, \ldots, m_n)$* span *(or* generate*) M if the equivalent conditions of the above lemma are satisfied.*

Definition 5.3.4. *We shall say that a module M is finitely generated if there exists a finite collection of elements that generates it.*

The following will be useful in what is to come:

Lemma 5.3.5. *Suppose that the elements $(m_1, m_2, \ldots, m_n)$ generate M and assume that*

$$m_1 = r_2 \cdot m_2 + \cdots + r_n \cdot m_n.$$

Then the elements $(m_2, \ldots, m_n)$ also generate M.

Proof. Exercise. □

5.3.6. We also give the following definitions:

Lemma 5.3.7. *The following conditions are equivalent:*

(i) *The map ϕ is injective;*

(ii) *Whenever $r_1, \ldots, r_n \in R$ are such that*

$$r_1 \cdot m_1 + \cdots + r_n \cdot m_n = 0,$$

then all $r_i = 0$.

The proof is immediate.

Definition 5.3.8. *We shall say that the elements $(m_1, \ldots, m_n)$ are* linearly independent *if the equivalent conditions of the above lemma are satisfied.*

Lemma 5.3.9. *The following conditions are equivalent:*

(i) *The map ϕ is bijective;*

(ii) *For every $m \in M$ there exists a unique n-tuple of elements $r_1, \ldots, r_n \in R$ such that*

$$m = r_1 \cdot m_1 + \cdots + r_n \cdot m_n.$$

Proof. This follows by combining Lemma 5.3.2 and 5.3.7. □

Definition 5.3.10. *We shall say that the elements $(m_1, \ldots, m_n)$* form a basis *(or* freely generate*) M if the equivalent conditions of the above lemma are satisfied.*

5.3.11. Let $M = R^{\oplus m}$, and let $m_1, \ldots, m_n$ be given by the m-tuples of elements

$$(r_i^1, \ldots, r_i^m), \quad i \in \{1, \ldots, n\},$$

respectively.

For another m-tuple $(r_0^1, \ldots, r_0^m)$ consider the problem of finding elements

$$(a_1, \ldots, a_n) \in R$$

such that

$$a_1 \cdot r_1^j + \cdots + a_n \cdot r_n^j = r_0^j, \quad j \in \{1, \ldots, m\}. \tag{11}$$

Week 3, HW Problem 5. *Show that:*

(a) The elements $m_1, \ldots, m_n$ generate $R^{\oplus m}$ if and only if the system of linear equations (11) *admits a solution for every m-tuple $(r_0^1, \ldots, r_0^m)$.*

(b) The elements $m_1, \ldots, m_n$ are linearly independent if and only if the system of linear equations (11) *with $r_0^1 = \cdots = r_0^m = 0$ admits only the trivial solution (i.e., one with $a_1 = \cdots = a_n = 0$).*

(c) The elements $m_1, \ldots, m_n$ form a basis of $R^{\oplus m}$ if and only if the system of linear equations (11) *admits a unique solution for every m-tuple $(r_0^1, \ldots, r_0^m)$.*

5.4. **Bases for vector spaces.** In this subsection we will assume that our ring R is a field k. So, instead of modules we will talk about vector spaces (over k).

5.4.1. Let V be a vector space, and let $v_1, \ldots, v_n \in V$ be elements.

Proposition 5.4.2. *The following conditions are equivalent:*

(1) *The elements* $(v_1, \ldots, v_n)$ *form a basis for* V*;*

(2) *The elements* $(v_1, \ldots, v_n)$ *span* V*, but any proper subcollection of* $(v_1, \ldots, v_n)$ *no longer does.*

(3) *The elements* $(v_1, \ldots, v_n)$ *are linearly independent, but for any* $v \in V$*, the collection* $(v, v_1, \ldots, v_n)$ *is no longer linearly independent.*

Proof. The implications (1) ⇒ (2) and (1) ⇒ (3) are immediate (and do not require our ring to be a field).

Let us show that (2) implies (1). Suppose by contradiction that $(v_1, \ldots, v_n)$ is not a basis. Then these elements are linearly dependent. I.e., there exist elements $a_1, \ldots, a_n \in k$, not all equal to zero, such that

$$a_1 \cdot v_1 + \cdots + a_n \cdot v_n = 0.$$

Up to reindexing, let us assume that $a_1 \neq 0$. Then we have:

$$v_1 = b_2 \cdot v_2 + \cdots + b_n \cdot v_n,$$

where $b_i = -(a_1)^{-1} \cdot a_i$, $i = 2, \ldots, n$. Hence, the elements $v_2, \ldots, v_n$ span V by Lemma 5.3.5. This is a contradiction to the assumption in (2).

Let us show that (3) implies (1). I.e., let us show that $(v_1, \ldots, v_n)$ span V. Let $v \in V$ be an element. We know that the collection $(v, v_1, \ldots, v_n)$ is linearly dependent. Hence, there exist elements $(a_0, a_1, \ldots, a_n) \in k$ not all equal to zero such that

$$a_0 \cdot v + a_1 \cdot v_1 + \cdots + a_n \cdot v_n = 0.$$

Note that $a_0 \neq 0$, for otherwise, the elements $(v_1, \ldots, v_n)$ would be linearly dependent, contradicting the assumption in (3). Hence, we obtain:

$$v = b_1 \cdot v_1 + \ldots + b_n \cdot v_n, \quad b_i = -(a_0)^{-1} \cdot a_i.$$

□

Corollary 5.4.3. *Let a vector space* V *be finitely generated. Then it admits a basis.*

Proof. By assumption V admits a finite spanning set of elements $S_0 = (v_1, \ldots, v_n)$. Let us choose a subset $S \subset (v_1, \ldots, v_n)$ with the following two properties:

- The vectors from S still span V.
- No proper subset of S spans V.

It is clear that such an S exists (eliminate elements from the original set S_0 keeping it spanning). Then the resulting set of elements satisfies assumption (2) of Proposition 5.4.2.

□

5.5. **The notion of dimension.**

Below is the fundamental theorem that makes the theory of finitely generated vector spaces work:

Theorem 5.5.1. *Let V be a vector space. Let $(v_1, \ldots, v_n)$ be a spanning collection of elements and $(w_1, \ldots, w_m)$ a linearly independent collection of elements. Then $m \leq n$.*

As an immediate consequence, we obtain:

Theorem 5.5.2. *Let V be a vector space with bases $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_m)$. Then $m = n$.*

The integer n from Theorem 5.5.2 is called the dimension of V. The above theorem ensures that it is well-defined, i.e., it is independent of the choice of a basis.

Henceforth we shall call finitely generated vector spaces “finite-dimensional”.

6. Thursday, Sept. 20

6.1. **Dimension of vector spaces, continued.**

6.1.1. As another corollary, we obtain the following analog of the pigeonhole principle for vector spaces:

Corollary 6.1.2. *Let T be a map $k^n \to k^m$.*

(a) *If T is surjective, then $n \geq m$.*

(b) *If T is injective, then $n \leq m$.*

(c) *If T is bijective, then $n = m$.*

Proof. Let $e_1, \ldots, e_n$ be the standard basis for k^n, and let $f_1, \ldots, f_m$ be the standard basis for k^m.

For point (a) we apply Theorem 5.5.1 to $v_i = e_i$ and $w_j = f_j$.

For point (b) we apply Theorem 5.5.1 to $v_i = f_i$ and $w_j = e_j$.

Point (c) is a formal consequence of points (a) and (b).

□

6.1.3. *Completion to a basis.* Let us give several more corollaries of Theorem 5.5.1:

Corollary 6.1.4. *Let V be a vector space of dimension n, and $V' \subset V$ be a linear subspace. Let $v_1, \ldots, v_m$ be a linearly independent set of elements of V'. Then the above set can be completed to a basis of V', whose cardinailty is $\leq n$.*

Proof. Suppose not. We define the elements v_{m+k}, $k = 1, 2 \ldots$ inductively. Suppose the corresponding vectors have been defined for $k' < k + 1$ (we set $v_{m+0} := v_m$). By assumption, the set

$$v_1, \ldots, v_{m+k}$$

is not a basis. Hence, by Proposition 5.4.2, we can choose a vector $v_{m+k+1} \in V'$, so that the set

$$v_1, \ldots, v_{m+k+1}$$

is still linearly independent.

In particular, for $k > n - m$, we obtain a linearly independent set

$$v_1, \ldots, v_{m+k}$$

in V', and hence in V. However, this contradicts Theorem 5.5.1.

□

NB: The argument above formalizes the only thing one can do in this situation, which is to add independent vectors until a finiteness condition (here, a dimension theorem) kicks in. That is to say, behind the above proof is the following algorithm to extend any linearly independent set to a basis: keep adding vectors that aren't in the span of the current list, and keep track of the number of vectors. Once the dimension is hit, stop. The resulting list is necessarily a basis.

Corollary 6.1.5. *A linearly independent set of elements of a finite-dimensional vector space can be completed to a basis.*

Proof. In Corollary 6.1.4 take $V' = V$. □

NB: Note that the proof of Corollary 6.1.4 in the case $V = V'$ gives an algorithm for the completion to a basis: keep adding linearly independent elements, and once you've added $n - m$ of them you know you've got a basis.

6.1.6. As yet another corollary, we obtain:

Corollary 6.1.7. *A linear subspace of a finite-dimensional vector space is finite-dimensional.*

Proof. Apply Corollary 6.1.4 to the case $m = 0$. □

NB: One might wonder whether the analog of Corollary 6.1.7 holds more generally for rings. I.e., is it true that if M is a finitely-generated module over a ring R, and M' is a submodule of M, then M' is also finitely generated? For general rings, this is false. Rings that have this property are called Noetherian.

6.2. **Proof of Theorem 5.5.1.**

6.2.1. *Step 1.* The proof proceeds by induction. We assume that the statement holds for any

$$\widetilde{V}, (\widetilde{v}_1, \ldots, \widetilde{v}_{\widetilde{n}}), (\widetilde{w}_1, \ldots, \widetilde{w}_{\widetilde{m}})$$

whenever $\widetilde{m} < m$. The base of induction is $m = 0$, in which case there is nothing to prove (0 is $\leq$ any non-negative integer).

6.2.2. *Step 2.* Since $(v_1, \ldots, v_n)$ span V, we can write

$$w_1 = a_1 \cdot v_1 + \ldots + a_n \cdot v_n.$$

Since $w_1 \neq 0$, not all $a_i = 0$. Hence, up to reindexing, we can assume that $a_1 \neq 0$. Hence,

$$v_1 = (a_1)^{-1} \cdot w_1 - (a_1)^{-1} \cdot a_2 \cdot w_2 - \ldots - (a_1)^{-1} \cdot a_n \cdot w_n.$$

Since the elements

$$(w_1, v_1, v_2, \ldots, v_n)$$

span V, from Lemma 5.3.5 we obtain that so too do the elements

$$(w_1, v_2, \ldots, v_n).$$

6.2.3. *Step 3.* Define $V' = \text{Span}(w_1) \subset V$, and consider the vector space V/V'. Since the elements $(w_1, v_2, \ldots, v_n)$ span V, then their images

$$(\bar{w}_1, \bar{v}_2, \ldots, \bar{v}_n)$$

spane V/V'. However, $\bar{w}_1 = 0$. Hence,

$$(\bar{v}_2, \ldots, \bar{v}_n)$$

is a spanning set for V/V'.

6.2.4. *Step 4.* Consider the elements

$$(\bar{w}_2, \ldots, \bar{w}_m) \in V/V'.$$

We claim that they are linearly independent. Indeed, suppose that

$$b_2 \cdot \bar{w}_2 + \ldots + b_n \cdot \bar{w}_m = 0.$$

Set

$$v = b_2 \cdot w_2 + \ldots + b_n \cdot w_m.$$

We obtain $\bar{v} = 0$, hence $v \in V'$, i.e., $V = b_1 \cdot w_1$ for some $b_1 \in k$. Hence, we obtain

$$-b_1 \cdot w_1 + b_2 \cdot w_2 + \ldots + b_n \cdot w_m = 0.$$

However, by assumption, the elements $(w_1, \ldots, w_m)$ were linearly independent. Hence, all $b_i = 0$.

6.2.5. *Step 5.* We obtain that in the vector space V/V', the set $(\bar{v}_2, \ldots, \bar{v}_n)$ is spanning, and $(\bar{w}_2, \ldots, \bar{w}_m)$ is linearly independent. Hence, by the induction hypothesis,

$$m - 1 \leq n - 1,$$

and hence $m \leq n$, as required.

□

6.3. **Behavior of dimension.**

6.3.1. Let V be a vector space, and $V' \subset V$ a subspace. Let $(v_1, \ldots, v_n)$ be a collection of elements in V', and let $(u_1, \ldots, u_m)$ be a collection of elements in V; denote by $(\bar{u}_1, \ldots, \bar{u}_m)$ their images in V/V'.

Proposition 6.3.2. *Consider the collection $(v_1, \ldots, v_n, u_1, \ldots, u_m)$ in V.*
(a) *If $(v_1, \ldots, v_n)$ are linearly independent in V' (same as in V), and $(u_1, \ldots, u_m)$ are linearly independent in V/V', then*

$$(v_1, \ldots, v_n, u_1, \ldots, u_m)$$

are linearly independent in V.
(b) *If $(v_1, \ldots, v_n)$ span V', and $(u_1, \ldots, u_m)$ span V/V', then*

$$(v_1, \ldots, v_n, u_1, \ldots, u_m)$$

span V.
(c) *If $(v_1, \ldots, v_n)$ form a basis in V' (same as in V), and $(u_1, \ldots, u_m)$ form a basis in V/V', then*

$$(v_1, \ldots, v_n, u_1, \ldots, u_m)$$

form a basis in V.

Week 3, HW Problem 6. *Prove Proposition 6.3.2.*

Corollary 6.3.3. *Let V be a vector space and $V' \subset V$ a linear subspace. Then*

$$\dim(V) = \dim(V') + \dim(V/V').$$

Proof. Choose a basis $(v_1, \dots, v_n)$ in V, and a basis $(\bar{u}_1, \dots, \bar{u}_m)$ in V/V'. Lift the elements $\bar{u}_i \in V/V'$ to elements $u_i \in V$, and apply Proposition 6.3.2(c) to the set $(v_1, \dots, v_n, u_1, \dots, u_m)$. □

6.3.4. Let $T : V \to W$ be a linear map between finite-dimensional vector spaces. We define

$$\text{rk}(T) := \dim(\text{Im}(T)).$$

Corollary 6.3.5. $\dim(V) = \text{rk}(T) + \dim(\ker(T))$.

Proof. Take $V' = \ker(T)$. Then by the first isomorphism theorem, Theorem 3.1.4, the map T induces an isomorphism

$$\widetilde{T} : V/V' \to \text{Im}(T).$$

In particular, $\dim(V/V') = \dim(\text{Im}(T))$. Now apply Corollary 6.3.3. □

6.3.6. We introduce the notation:

$$\text{coker}(T) := W/\operatorname{Im}(T).$$

Corollary 6.3.7. $\dim(V) - \dim(\ker(T)) = \dim(W) - \dim(\text{coker}(T))$.

Proof. By Corollary 6.3.5, the left-hand side is $\text{rk}(T) := \dim(\text{Im}(T))$. Now, the assertion follows from Corollary 6.3.3. □

Corollary 6.3.8. *Suppose that* $\dim(V) = \dim(W)$*. Then T is injective if and only if it is surjective.*

Proof. T is injective $\Leftrightarrow \ker(T) = 0 \Leftrightarrow \dim(\ker(T)) = 0$, which by Corollary 6.3.7 is equivalent to $\dim(\text{coker}(T)) = 0 \Leftrightarrow \text{coker}(T) = 0 \Leftrightarrow \text{Im}(T) = W$.

□

As a particular case, we obtain:

Corollary 6.3.9. *Let T be an endomorphism of V, i.e., a linear map from V to itself. Then it is injective if and only if it is surjective.*

6.3.10. Let now V_1 and V_2 be two subspaces of V.

Week 3, HW Problem 7. *Prove that*

$$\dim(V_1) + \dim(V_2) = \dim(V_1 \cap V_2) + \dim(V_1 + V_2),$$

where $V_1 + V_2$ is the subspace from Sect. 3.2.1.

Suggested strategy: Use the second isomorphism theorem.

6.4. **Modules of maps.** In this subsection we will take R to be an arbitrary ring.

6.4.1. Let M and N be R-module. Consider the set

$$\mathrm{Hom}_R(M,N).$$

We define on $\mathrm{Hom}_R(M,N)$ a structure of abelian group by setting for $\phi_1,\phi_2\in\mathrm{Hom}_R(M,N)$ their sum $\phi_1+\phi_2\in\mathrm{Hom}_R(M,N)$ to be the homomorphism defined by the formula

$$(\phi_1+\phi_2)(m)=\phi_1(m)+\phi_2(m).$$

It is easy to check that the above indeed defines a structure of abelian group on $\mathrm{Hom}_R(M,N)$ (check it!).

6.4.2. From now on, for the duration of this subsection, we will assume that R is *commutative*. We claim that in this case the abelian group structure on $\mathrm{Hom}_R(M,N)$ can be upgraded to that of an R-module.

Namely, for $\phi\in\mathrm{Hom}_R(M,N)$ and $r\in R$, we let $r\cdot\phi\in\mathrm{Hom}_R(M,N)$ be the homomorphism defined by the formula

$$(r\cdot\phi)(m)=r\cdot\phi(m).$$

Let us check that $r\cdot\phi$ is indeed an R-module homomorphism. The fact that $r\cdot\phi$ is a homomorphism of abelian groups is straightforward (and does not require R to be commutative). Let us show that $r\cdot\phi$ is R-linear. For $r'\in R$ and $m\in M$ we need to show that

$$(r\cdot\phi)(r'\cdot m)=r'\cdot((r\cdot\phi)(m)).$$

The left-hand side equals by definition

$$r\cdot(\phi(r'\cdot m))=r\cdot(r'\cdot\phi(m))=(r\cdot r')\cdot\phi(m).$$

The right-hand side equals $(r'\cdot r)\cdot\phi(m)$. The two are equal because $r\cdot r'=r'\cdot r$ by assumption.

Week 3, HW Problem 8. *Show that the operations*

$$\phi_1,\phi_2\mapsto\phi_1+\phi_2 \text{ and } r,\phi\mapsto r\cdot\phi,$$

defined above do indeed satisfy the axioms of R-module on $\mathrm{Hom}_R(M,N)$.

6.4.3. *Compositions.* Let $\psi:N_1\to N_2$ be a map of R-modules. Composition with ψ defines a map of sets

$$\mathrm{Hom}_R(M,N_1)\to\mathrm{Hom}_R(M,N_2). \tag{12}$$

Let $\xi:M_1\to M_2$ be a map of R-modules. Pre-composition with ξ defines a map of sets

$$\mathrm{Hom}_R(M_2,N)\to\mathrm{Hom}_R(M_1,N). \tag{13}$$

Week 3, HW Problem 9. *Show that the maps in* (12) *and* (13) *are maps of R-modules.*

6.4.4. *The dual module.* For an R-module M we define

$$M^* := \mathrm{Hom}_R(M, R),$$

viewed as an R-module. We call M^* the module dual to M.

Let $\phi : M_1 \to M_2$ be a map of R-modules. Precomposition with ϕ defines a map

$$M_2^* \to M_1^*,$$

which is an R-module homomorphism by [Problem 9, Week 3].

This above homomorphism is denoted by ϕ^* and is called the homomorphism dual to ϕ.

6.4.5. *Direct sums.* Recall the map

$$\mathrm{Hom}_R(M, N_1 \oplus N_2) \to \mathrm{Hom}_R(M, N_1) \times \mathrm{Hom}_R(M, N_2)$$

of (8). We regard $\mathrm{Hom}_R(M, N_1) \times \mathrm{Hom}_R(M, N_2)$ as the R-module

$$\mathrm{Hom}_R(M, N_1) \oplus \mathrm{Hom}_R(M, N_2).$$

Recall also the map

$$\mathrm{Hom}_R(M_1 \oplus M_2, N) \to \mathrm{Hom}_R(M_1, N) \times \mathrm{Hom}_R(M_2, N)$$

of (9). We regard $\mathrm{Hom}_R(M_1, N) \times \mathrm{Hom}_R(M_2, N)$ as the R-module

$$\mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N).$$

Week 3, HW Problem 10. *Show that the resulting maps*

$$\mathrm{Hom}_R(M, N_1 \oplus N_2) \to \mathrm{Hom}_R(M, N_1) \oplus \mathrm{Hom}_R(M, N_2)$$

and

$$\mathrm{Hom}_R(M_1 \oplus M_2, N) \to \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N)$$

are R-module homomorphisms.

7. Tuesday, Sept. 25

7.1. Modules of maps, continued.

7.1.1. Recall from [Problem 10, Week 3] that we have an R-module isomorphism:

$$\mathrm{Hom}_R(M_1 \oplus M_2, N) \to \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N) \tag{14}$$

that sends $\phi \in \mathrm{Hom}_R(M_1 \oplus M_2, N)$ to

$$(\phi_1, \phi_2) \in \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N),$$

where

$$\phi_1 := \phi \circ i_1 \text{ and } \phi_2 := \phi \circ i_2.$$

We shall now construct an explicit map in the opposite direction. Recall from [Problem 10, Week 3] that we have an R-module isomorphism:

$$\mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N) \to \mathrm{Hom}_R(M_1 \oplus M_2, N) \tag{15}$$

Recall (see [Problem 2, Week 3]) that the datum of a map in (15) is equivalent to that of a pair of maps

$$\mathrm{Hom}_R(M_1, N) \to \mathrm{Hom}_R(M_1 \oplus M_2, N) \text{ and } \mathrm{Hom}_R(M_2, N) \to \mathrm{Hom}_R(M_1 \oplus M_2, N).$$

We let the latter be given by precomposition with π_1 and π_2 respectively.

Week 4, HW Problem 1. *Show that the map in* (15) *thus constructed is the inverse of the map in* (14).

7.1.2. Recall (see [Problem 8, Week 2]) that evaluation on $1 \in R$ defines an isomorphism of sets

$$\mathrm{Hom}_R(R, M) \to M. \tag{16}$$

Lemma 7.1.3. *The map* (16) *is an R-module homomorphism.*

Week 4, HW Problem 2. *Prove Lemma 7.1.3.*

7.2. **Dual modules, continued.**

7.2.1. From [Problem 10, Week 3] and [Problem 1, Week 4] we obtain that we have canonical isomorphisms

$$(M_1 \oplus M_2)^* \simeq M_1^* \oplus M_2^*. \tag{17}$$

Week 4, HW Problem 3. *Show that the maps in* (14) *and* (15) *indeed amount to the following:*

We send $\xi \in (M_1 \oplus M_2)^*$ to the element $(\xi_1, \xi_2) \in M_1^* \oplus M_2^*$, where

$$\xi_1(m_1) = \xi(m_1, 0) \text{ and } \xi_2(m_2) = \xi(0, m_2).$$

In the other direction, we send an element $(\xi_1, \xi_2) \in M_1^* \oplus M_2^*$ to $\xi \in (M_1 \oplus M_2)^*$, where

$$\xi(m_1, m_2) = \xi_1(m_1) + \xi_2(m_2).$$

7.2.2. From Lemma 7.1.3 we obtain:

Corollary 7.2.3. *There exists a canonical isomorphism of R-modules $R^* \simeq R$.*

Concretely, this sends the element $\xi \in R^*$ to $\xi(1)$, and the element $r \in R$ to $r \cdot \mathrm{id}_R$.

Combining Corollary 7.2.3 with (17) we obtain:

Corollary 7.2.4. *There exists a canonical isomorphism*

$$(R^n)^* \simeq R^n.$$

7.2.5. *Notation.* Let $e_1, \ldots, e_n$ denote the standard basis elements of R^n.

By [Problem 9, Week 2], the isomorphism

$$R^n \to (R^n)^* \tag{18}$$

defines a basis in the R-module $(R^n)^*$. We let $e_1^*, \ldots, e_n^*$ denote the corresponding basis elements in $(R^n)^*$.

Week 4, HW Problem 4. *Show that the elements $e_j^* \in (R^n)^*$, viewed as R-module homomorphisms $R^n \to R$, satisfy:*

$$e_j^*(e_k) = \begin{cases} 1, & j = k, \\ 0, & j \neq k. \end{cases}$$

7.2.6. In what follows, given an R-module M that admits a basis $e_1, \ldots, e_n$, i.e., an isomorphism

$$\phi : R^n \to M,$$

we let $e_1^*, \ldots, e_n^*$ denote the basis of M^* obtained from the isomorphism

$$M^* \overset{\phi^*}{\simeq} (R^n)^* \overset{\text{Equation (18)}}{\simeq} R^n.$$

By [Problem 4, Week 4], the values of $e_j^*(e_k)$ are given by Kronecker's δ — i.e., $e_j^*(e_k) = \delta_{jk}$.

7.3. **Dual maps, continued.**

7.3.1. Let $\phi : M_1 \to M_2$ and $\psi : M_2 \to M_3$ be R-module homomorphisms.

Week 4, HW Problem 5. *Show that $\phi^* \circ \psi^* = (\psi \circ \phi)^*$ as R-module homomorphisms $M_3^* \to M_1^*$.*

Week 4, HW Problem 6. *Suppose that the map $\phi : M_1 \to M_2$ is surjective. Show that the map $\phi^* : M_2^* \to M_1^*$ is injective.*

7.3.2. Recall that according to Sect. 4.4.3, the set of R-module homomorphisms $\text{Hom}_R(R^n, R^m)$ is in bijection with the set $\text{Mat}_{m\times n}(R)$ of $(m \times n)$-matrices with values in R.

For a given $\phi : R^n \to R^m$, let $\text{Mat}(\phi) \in \text{Mat}_{m\times n}(R)$ denote the corresponding matrix.

Consider now the dual map

$$\phi^* : (R^m)^* \to (R^n)^*.$$

Using Corollary 7.2.4, we obtain a map

$$R^m \simeq (R^m)^* \xrightarrow{\phi^*} (R^n)^* \simeq R^n.$$

Denote the latter map by ψ. Note that $\text{Mat}(\psi) \in \text{Mat}_{n\times m}(R)$ is an $(n \times m)$-matrix.

Week 4, HW Problem 7. *Show that the matrix* $\text{Mat}(\psi)$ *is the transpose of* $\text{Mat}(\phi)$.

So the above problem gives a mathematical meaning to the operation of taking the transpose of a matrix.

7.4. **The double dual.**

7.4.1. Let M be an R-module. We are going to construct a canonical map of R-modules

$$\mathbf{d}_M : M \to (M^*)^*. \tag{19}$$

Given an element $m \in M$ we define an element $\mathbf{d}_M(m) \in (M^*)^*$ to be the map

$$M^* \to R \tag{20}$$

that sends $\xi \in M^*$ to the element $\xi(m) \in R$. It is easy to see (check this!) that the map in (20) is indeed an R-module homomorphism. (One might also notate this map ev_{-}, taking $m \mapsto \text{ev}_m$, "evaluation at m".)

Week 4, HW Problem 8. *Show that the map $\mathbf{d}_M$, constructed above, is an R-module homomorphism.*

7.4.2. Let $\phi : M_1 \to M_2$ be a homomorphism of R-modules. Consider the dual map $\phi^* : M_2^* \to M_1^*$. And now consider the dual of ϕ^*

$$(\phi^*)^* : (M_1^*)^* \to (M_2^*)^*.$$

Week 4, HW Problem 9. *Show that the diagram*

$$\begin{tikzcd} M_1 \arrow[r, "\mathbf{d}_{M_1}"] \arrow[d, "\phi"'] & (M_1^*)^* \arrow[d, "(\phi^*)^*"] \\ M_2 \arrow[r, "\mathbf{d}_{M_2}"] & (M_2^*)^* \end{tikzcd}$$

commutes.

7.4.3. Let M be an R-module, equipped with a basis $e_1, \ldots, e_n$.

According to Sect. 7.2.6, the module M^* acquires a basis $e_1^*, \ldots, e_n^*$. Hence, the double dual $(M^*)^*$ also acquires a basis $(e_1^*)^*, \ldots, (e_n^*)^*$.

Week 4, HW Problem 10.

(a) Show that the map $\mathbf{d}_M$ sends $e_i \mapsto (e_i^*)^*$.

(b) Deduce that if M admits a basis, then the map $\mathbf{d}_M$ is an isomorphism.

8. Tuesday, Oct. 2

8.1. **Dual maps, continued.**

8.1.1. Let $T : V_1 \to V_2$ be a map between finite-dimensional vector spaces. Consider the dual map $T^* : V_2^* \to V_1^*$.

Proposition 8.1.2.

(a) *T is surjective if and only if T^* is injective.*

(b) *T is injective if and only if T^* is surjective.*

Proof. We first prove (a). If T is surjective, then T^* is injective by [Problem 6, Week 4]. Now consider the vector space

$$\operatorname{coker}(T) := V_2/\operatorname{Im}(T),$$

the *cokernel* of the map T. If T^* is injective, then observe that the surjectivity of the tautological projection $\pi : V_2 \to \operatorname{coker}(T)$ implies the injectivity of the dual map

$$\pi^* : (\operatorname{coker}(T))^* \to V_2^*,$$

from the forward direction of (a). But

$$\pi \circ T = 0 : V_1 \to V_2 \to V_2/\operatorname{Im}(T)$$

by definition, whence

$$0 = (\pi \circ T)^* = T^* \circ \pi^*$$

by [Problem 5, Week 4]. Hence, $\operatorname{Im}(\pi^*) \subset \ker(T^*)$. But this last vector space is 0 by our injectivity assumption. Hence $\operatorname{Im}(\pi^*) = 0$. But π^* was injective in the first place, so that

$$(\operatorname{coker}(T))^* = 0.$$

But

$$\operatorname{coker}(T) \simeq ((\operatorname{coker}(T))^*)^* = 0^* = 0,$$

which is to say that

$$\mathrm{Im}(T) = V_2,$$

as desired.

Let us now prove point (b). Consider the map

$$T^* : V_2^* \to V_1^*.$$

By point (a), T^* is surjective if and only if $(T^*)^*$ is injective. Now the assertion follows from the commutative diagram

$$\begin{tikzcd}
V_1 \arrow[r] \arrow[d, "T"'] & (V_1^*)^* \arrow[d, "(T^*)^*"] \\
V_2 \arrow[r] & (V_2^*)^*
\end{tikzcd}$$

in which the horizontal arrows are isomorphisms by [Problem 10(b), Week 4].

□

Week 5, HW Problem 1. *Let M be an $(m \times n)$-matrix. Show that its columns span k^m if and only if its rows are linearly independent in k^n.*

8.1.3. Let V be a finite-dimensional vector space and let $V' \subset V$ be a linear subspace. Define $(V')^\perp$ to be the subset of V^* consisting of elements $\xi \in V^*$ such that

$$\xi(v') = 0, \, \forall v' \in V'.$$

Week 5, HW Problem 2. *Show that $(V')^\perp$ is a linear subspace of V^*. Construct an isomorphism $V^*/(V')^\perp \simeq (V')^*$.*

8.2. **Representation of linear maps by matrices.**

8.2.1. Let $T : V \to W$ be a linear map between finite-dimensional vector spaces.

Let

$$\underline{e} = \{e_1, \ldots, e_n\} \text{ and } \underline{f} = \{f_1, \ldots, f_m\}$$

be bases in V and W, respectively. Let

$$\phi_{\underline{e}} : k^n \to V \text{ and } \phi_{\underline{f}} : k^m \to W$$

be the corresponding isomorphisms (see [Problem 9, Week 2] and Lemma 5.3.9).

Consider the map

$$M_{T,\underline{e},\underline{f}} : k^n \to k^m$$

equal to

$$(\phi_{\underline{f}})^{-1} \circ T \circ \phi_{\underline{e}}.$$

I.e., this is the map that makes the following diagram commutative:

$$\begin{tikzcd}
V \arrow[r, "T"] & W \\
k^n \arrow[u, "\phi_{\underline{e}}"] \arrow[r, "M_{T,\underline{e},\underline{f}}"] & k^m . \arrow[u, "\phi_{\underline{f}}"']
\end{tikzcd}$$

By Sect. 4.4.3, the linear transformation $M_{T,\underline{e},\underline{f}}$ is encoded by an $(m \times n)$ matrix. We shall say that this is the matrix that encodes T in the pair of bases $\underline{e}$ and $\underline{f}$.

Week 5, HW Problem 3. *Let $T : V \to W$ be as above. Show that there exist bases $\underline{e}$ of V and $\underline{f}$ of W, respectively, such that the matrix $M_{T,\underline{e},\underline{f}}$ looks as follows: its entries $a_{i,j}$ vanish if $i \neq j$, $a_{i,i} = 1$ for $1 \leq i \leq \mathrm{rk}(T)$, and $a_{i,i} = 0$ for $i > \mathrm{rk}(T)$.*

What this tells us is that the theory of maps between finite dimensional vector spaces is really quite boring if we are free to choose bases for the domain V and codomain W. "Thankfully," we usually can't do such a thing (namely, usually we are presented with a map $V \to V$ and at best we are free to choose a basis only *simultaneously* for the domain and codomain, which are now both V).

8.2.2. Suppose now that we choose another pair of bases

$$\underline{e}' = \{e'_1, \ldots, e'_n\} \text{ and } \underline{f}' = \{f'_1, \ldots, f'_m\},$$

respectively.

Consider the corresponding maps

$$\phi_{\underline{e}'} : k^n \to V \text{ and } \phi_{\underline{f}'} : k^m \to W.$$

Denote

$$S_{\underline{e},\underline{e}'} := (\phi_{\underline{e}'})^{-1} \circ \phi_{\underline{e}} \text{ and } S_{\underline{f},\underline{f}'} := (\phi_{\underline{f}'})^{-1} \circ \phi_{\underline{f}}.$$

$$\begin{tikzcd}
k^n \arrow[dr, "\phi_{\underline{e}'}"] & & & k^m \arrow[dl, "\phi_{\underline{f}'}"'] \\
& V & W & \\
k^n \arrow[uu, "S_{\underline{e},\underline{e}'}"] \arrow[ur, "\phi_{\underline{e}}"'] & & & k^m \arrow[uu, "S_{\underline{f},\underline{f}'}"'] \arrow[ul, "\phi_{\underline{f}}"]
\end{tikzcd}$$

Being a map from $k^n \to k^n$ (resp., $k^m \to k^m$), the linear transformation $S_{\underline{e},\underline{e}'}$ (resp., $S_{\underline{f},\underline{f}'}$) is encoded by an $(n \times n)$ (resp., $(m \times m)$) matrix.

The matrix corresponding to $S_{\underline{e},\underline{e}'}$ (resp., $S_{\underline{f},\underline{f}'}$) is called the *change of basis matrix.*

Note that

$$S_{\underline{e}',\underline{e}} = (S_{\underline{e},\underline{e}'})^{-1} \text{ and } S_{\underline{f}',\underline{f}} = (S_{\underline{f},\underline{f}'})^{-1}.$$

Week 5, HW Problem 4. *For $1 \leq i \leq n$ and $1 \leq j \leq n$ write*

$$e_i = \sum_j a_{i,j} \cdot e'_j.$$

Show that $a_{i,j}$ is the $(j \times i)$-th entry of the matrix corresponding to $S_{\underline{e},\underline{e}'}$, where our conventions are such that the first index corresponds to the vertical coordinate in a matrix, and the second to the horizontal coordinate.

8.2.3. Let $M_{T,\underline{e}',\underline{f}'}$ be the linear transformation corresponding to T and the pair of bases $\underline{e}'$, $\underline{f}'$. How can we express $M_{T,\underline{e}',\underline{f}'}$ in terms of $M_{T,\underline{e},\underline{f}}$?

Consider the diagram

$$\begin{tikzcd}
k^n. \arrow[rrr, "M_{T,\underline{e}',\underline{f}'}"'] \arrow[dr, "\phi_{\underline{e}'}"'] \arrow[dd, "S_{\underline{e}',\underline{e}}"'] & & & k^m. \arrow[dl, "\phi_{\underline{f}'}"] \\
& V \arrow[r, "T"'] & W & \\
k^n \arrow[ur, "\phi_{\underline{e}}"] \arrow[rrr, "M_{T,\underline{e},\underline{f}}"] & & & k^m \arrow[ul, "\phi_{\underline{f}}"'] \arrow[uu, "S_{\underline{f},\underline{f}'}"']
\end{tikzcd}$$

From this diagram it is clear that

$$M_{T,\underline{e}',\underline{f}'} = S_{\underline{f},\underline{f}'} \circ M_{T,\underline{e},\underline{f}} \circ S_{\underline{e}',\underline{e}}.$$

8.2.4. Let us consider the particular case when $W = V$ and $\underline{f} = \underline{e}$ and $\underline{f}' = \underline{e}'$. In this case, we obtain:

$$M_{T,\underline{e}',\underline{e}'} = S_{\underline{e},\underline{e}'} \circ M_{T,\underline{e},\underline{e}} \circ (S_{\underline{e},\underline{e}'})^{-1}.$$

8.3. **Endomorphisms.** For the next few weeks we will be mainly concerned with analyzing endomorphisms

$$T : V \to V$$

for a given finite-dimensional space V.

8.3.1. Recall Corollary 6.3.9 that says that T is injective if and only if it is surjective. I.e., for an endomorphism

$$\text{injective} = \text{bijective} = \text{surjective}.$$

In what follows, instead of "bijective" we shall more often say "invertible".

8.3.2. *Invariant subspaces.* Let $V' \subset V$ be a subspace.

Definition 8.3.3. *We shall say that V' is T-invariant if T sends V' to V'.*

Here are examples of invariant subspaces:

Lemma 8.3.4. *For any n, the subspaces*

$$\ker(T^n) \text{ and } \operatorname{Im}(T^n)$$

are T-invariant.

Proof. For the kernels, we need to show that if $v \in V$ is such that $T^n v = 0$ then $T^n(Tv) = 0$. However,

$$T^n(Tv) = T(T^n v),$$

and the assertion follows.

For the images, we need to show that if v is of the form $T^n(v')$ for some v', then Tv is also of the form $T^n(v'')$ for some v''. However, it suffices to take $v'' = T(v')$. □

The following is also evident:

Lemma 8.3.5. *Let V' and V'' be T-invariant subspaces. Then so is $V' \cap V''$.*

8.3.6. If V' is T-invariant, the restriction of T to V' defines an endomorphism

$$T|_{V'} : V' \to V'$$

of V'.

Lemma 8.3.7. *If T is invertible, and $V' \subset V$ is a T-invariant subspace, then $T|_{V'}$ is also invertible.*

Proof. It suffices to show that $T|_{V'}$ is injective, and this much is evident. □

We can phrase the conclusion of the above lemma as follows: the property of being invertible is inherited under restriction to invariant subspaces.

8.3.8. Let $V' \subset V$ be T-invariant. From Proposition 5.1.4 we obtain that there exists a unique linear map

$$T|_{V/V'} : V/V' \to V/V'$$

that makes the diagram

$$\begin{tikzcd}
V \arrow[r, "\pi"] \arrow[d, "T"'] & V/V' \arrow[d, "T|_{V/V'}"] \\
V \arrow[r, "\pi"] & V/V'
\end{tikzcd} \tag{21}$$

commute.

8.3.9. We have:

Lemma 8.3.10. *If T is invertible, and $V' \subset V$ is a T-invariant subspace, then $T|_{V/V'}$ is also invertible.*

Proof. It suffices to show that $T|_{V/V'}$ is surjective, and this is evident from (21) since the lower horizontal arrow is surjective. □

We can phrase the conclusion of the above lemma as follows: the property of being invertible is inherited under passage to quotients by invariant subspaces.

8.4. **Stabilization of kernels.**

8.4.1. Let $T : V \to V$ be as before. Consider the sequence of subspaces

$$0 \subset \ker(T) \subset \ker(T^2) \subset \cdots \subset \ker(T^i) \subset \cdots \tag{22}$$

Theorem 8.4.2. *For any non-negative integer N, the inclusion*

$$\ker(T^{\dim(V)}) \subset \ker(T^{\dim(V)+N})$$

is an equality.

Proof. Consider the sequence of subspaces (22). Let n be the first integer such that the inclusion

$$\ker(T^n) \subset \ker(T^{n+1})$$

is an equality. It is clear that $n \leq \dim(V)$. For otherwise, we would have a chain of proper inclusions, and we would obtain that $\dim(\ker(T^n)) > \dim(V)$.

We claim that for any $i \geq 0$, the inclusions

$$\ker(T^n) \subset \ker(T^{n+1}) \subset \cdots \subset \ker(T^{n+i})$$

are all equalities. This would imply the assertion of the theorem.

We prove the claim by induction on i. The case of $i = 1$ is the initial assumption. Let us assume the validity for i and deduce it for $i+1$. Thus, we need to show that the inclusion

$$\ker(T^{n+i}) \subset \ker(T^{n+i+1})$$

is an equality.

Let v be an element of $\ker(T^{n+i+1})$, i.e., $T^{n+i+1}v = 0$. We want to show that v belongs to $\ker(T^{n+i})$, i.e., that $T^{n+i}v = 0$. Set $v' = T^i v$. We have $T^{n+1}(v') = 0$, i.e., $V' \in \ker(T^{n+1})$. By assumption, $\ker(T^n) = \ker(T^{n+1})$, so $v' \in \ker(T^n)$, i.e., $T^n(v') = 0$. Hence,

$$T^{n+i}v = T^n(v') = 0,$$

as desired.

□

8.4.3. The above theorem has multiple corollaries.

Consider the chain of subspaces

$$V \supset \mathrm{Im}(T) \supset \mathrm{Im}(T^2) \supset \cdots \supset \mathrm{Im}(T^i) \supset \cdots \tag{23}$$

Corollary 8.4.4. *For any non-negative integer N, the inclusion*

$$\mathrm{Im}(T^{\dim(V)}) \supset \mathrm{Im}(T^{\dim(V)+N})$$

is an equality.

Proof. It is enough to show that

$$\dim \mathrm{Im}(T^{\dim(V)}) = \dim \mathrm{Im}(T^{\dim(V)+N}).$$

However, by Corollary 6.3.9,

$$\dim \mathrm{Im}(T^{\dim(V)}) = \dim V - \dim \ker(T^{\dim(V)})$$

and

$$\dim \mathrm{Im}(T^{\dim(V)+N}) = \dim V - \dim \ker(T^{\dim(V)+N}),$$

and the assertion follows from Theorem 8.4.2. □

8.4.5. In what follows we will use the notation

$$\ker(T^\infty)$$

for the subspace $\ker(T^N)$ for any $N \geq \dim(V)$. By Theorem 8.4.2, this is independent of the choice of N. We shall refer to $\ker(T^\infty)$ as the eventual kernel of T.

We will use the notation

$$\mathrm{Im}(T^\infty)$$

for the subspace $\mathrm{Im}(T^N)$ for any $N \geq \dim(V)$. By Theorem 8.4.2, this is independent of the choice of N. We shall refer to $\mathrm{Im}(T^\infty)$ as the eventual kernel of T.

From Lemma 8.3.4, both $\ker(T^\infty)$ and $\mathrm{Im}(T^\infty)$ are T-invariant subspaces of V.

8.5. **Nilpotent endomorphisms.**

8.5.1. Let $T : V \to V$ be as above.

Proposition 8.5.2. *The following conditions are equivalent:*

(a) *For every $v \in V$ there exists n such that $T^n v = 0$.*

(b) *There exists n such that $T^n = 0$.*

(c) $T^{\dim(V)} = 0$.

Week 5, HW Problem 5. *Prove Proposition 8.5.2.*

In what follows we shall say that an endomorphism T of V is nilpotent if it satisfies the equivalent conditions of Proposition 8.5.2.

8.5.3. Let $V' \subset V$ be a T-invariant subspace.

Lemma 8.5.4. *Suppose that T is nilpotent. Then both $T|_{V'}$ and $T|_{V/V'}$ are nilpotent.*

Proof. Obvious. □

We can phrase the conclusion of the above lemma as follows: the property of being nilpotent is inherited by restriction to invariant subspaces and under passage to quotients by invariant subspaces.

8.6. **Decomposition into nilpotent and invertible parts.**

8.6.1. Let now $T : V \to V$ be an endomorphism of a finite-dimensional vector space.

Lemma 8.6.2. *The restriction $T|_{\ker(T^\infty)}$ is nilpotent.*

Proof. We will check condition (b) of Proposition 8.5.2 for $n = \dim(V)$. (Note that this integer is at least the dimension of $\ker(T^\infty)$, c.f. condition (c).)

We have:

$$(T|_{\ker(T^\infty)})^{\dim(V)} = T^{\dim(V)}|_{\ker(T^\infty)} = 0,$$

since $\ker(T^\infty) = \ker(T^{\dim(V)})$. □

8.6.3. We claim:

Lemma 8.6.4. *The restriction $T|_{\mathrm{Im}(T^\infty)}$ is invertible.*

Proof. We will show that $T|_{\mathrm{Im}(T^\infty)}$ is surjective.

For any n, the map T induces a surjection

$$\mathrm{Im}(T^n) \to \mathrm{Im}(T^{n+1}).$$

Taking $n \geq \dim(V)$, we derive the conclusion of the lemma. □

8.6.5. *A digression.* Let V be a vector space and V', V'' two linear subspaces. Consider the direct sum

$$V' \oplus V''$$

as an abstract vector space.

The tautological maps $V' \to V$ and $V'' \to V$ give rise to a map

$$V' \oplus V'' \to V$$

by [Problem 10, Week 3].

Lemma 8.6.6. *The following conditions are equivalent:*

(a) *The map $V' \oplus V'' \to V$ is injective;*

(b) *The intersection $V' \cap V''$, as subspaces of V, is zero.*

Proof. The kernel of $V' \oplus V'' \to V$ consists of pairs $(v' \in V', v'' \in V'')$ such that $v' + v'' = 0$. These are the same as $(v, -v)$, $v \in V' \cap V''$.

□

8.6.7. Consider the subspaces

$$\ker(T^\infty) \text{ and } \operatorname{Im}(T^\infty)$$

of V.

Theorem 8.6.8. *The map*

$$\ker(T^\infty) \oplus \operatorname{Im}(T^\infty) \to V \tag{24}$$

is an isomorphism.

Proof. We will first show that the map in question is injective. By Lemma 8.6.6, it suffices to show that for

$$V' := \ker(T^\infty) \cap \operatorname{Im}(T^\infty)$$

we have $V' = 0$.

By Lemmas 8.6.2 and 8.5.4, the operator $T|_{V'}$ is nilpotent. By Lemmas 8.6.4 and 8.3.6, the operator $T|_{V'}$ is invertible.

However, we claim that if W is a vector space and S is an endomorphism of W such that S is both nilpotent and invertible, then $W = 0$. Indeed, if S is invertible, so are all of its powers, but $S^{\dim(W)} = 0$. Now, the zero endomorphism is invertible only if the vector space is zero.

It remains to show that the map (24) is surjective.

Take any $N \geq \dim(V)$, so that

$$\ker(T^\infty) = \ker(T^N) \text{ and } \operatorname{Im}(T^\infty) = \operatorname{Im}(T^N).$$

By Corollary 6.3.9,

$$\dim \ker(T^N) + \dim \operatorname{Im}(T^N) = \dim(V).$$

Hence, both vector space appearing in (24) have the same dimension. Therefore, since the map in question is injective, it is also surjective by Corollary 6.3.8.

□

9. Thursday, Oct. 4

9.1. **Decomposition into nilpotent and invertible parts, continued.**

9.1.1. *A degression.* Let M be a module over a ring, and M', M'' be two submodules. Consider the resulting map

$$M' \oplus M'' \to M. \tag{25}$$

Definition 9.1.2. *We shall say that M' and M'' define a direct sum decomposition of M if the map* (25) *is an isomorphism.*

Let now N be another submodule of M.

Definition 9.1.3. *We shall say that N is compatible with the direct sum decomposition*

$$M' \oplus M'' \simeq M$$

if the map

$$(N \cap M') \oplus (N \cap M'') \to N \tag{26}$$

is an isomorphism.

Note that the map (26) is always injective. So, the compatibility condition above is equivalent to requiring that this map be surjective.

We have:

Lemma 9.1.4. *The submodule N is compatible with the direct sum decomposition $M' \oplus M'' \simeq M$ if and only if whenever $m' \in M'$ and $m' \in M''$ are such that $m' + m'' \in N$, then $m', m'' \in N$.*

Week 5, HW Problem 6. *Prove the above lemma.*

9.1.5. Let V be a finite-dimensional vector space and $T : V \to V$ a linear operator. Note that we can reformulate Theorem 8.6.8 as saying that the subspaces

$$\ker(T^\infty), \mathrm{Im}(T^\infty) \subset V$$

define a direct sum decomposition.

We now claim:

Proposition 9.1.6. *Let $W \subset V$ be a T-stable subspace. Then it is compatible with the direct sum decomposition of Theorem 8.6.8.*

Proof. We need to show that the map

$$(W \cap \ker(T^\infty)) \oplus (W \cap \mathrm{Im}(T^\infty)) \to W \tag{27}$$

is surjective.

Consider the vector subspaces

$$\ker((T|_W)^\infty) \subset W \text{ and } \mathrm{Im}((T|_W)^\infty) \subset W.$$

It is easy to see that

$$\ker((T|_W)^\infty) \subset \ker(T^\infty) \text{ and } \mathrm{Im}((T|_W)^\infty) \subset \mathrm{Im}(T^\infty).$$

Conider the composed map

$$\ker((T|_W)^\infty) \oplus \mathrm{Im}((T|_W)^\infty) \to (W \cap \ker(T^\infty)) \oplus (W \cap \mathrm{Im}(T^\infty)) \to W.$$

This map is surjective by Theorem 8.6.8, applied to $(W, T|_W)$. Hence, the map (27) is also surjective. □

9.1.7. Let now T_1 and T_2 be two operators $V \to V$.

Definition 9.1.8. *We shall say that T_1 and T_2 commute if $T_1 \circ T_2 = T_2 \circ T_1$.*

Consider the subspaces

$$\ker(T_1^\infty) \cap \ker(T_2^\infty),\ \mathrm{Im}(T_1^\infty) \cap \ker(T_2^\infty),\ \ker(T_1^\infty) \cap \mathrm{Im}(T_2^\infty),\ \mathrm{Im}(T_1^\infty) \cap \mathrm{Im}(T_2^\infty).$$

Consider the resulting map

$$(28) \quad (\ker(T_1^\infty) \cap \ker(T_2^\infty)) \oplus (\mathrm{Im}(T_1^\infty) \cap \ker(T_2^\infty)) \oplus \\ \oplus (\ker(T_1^\infty) \cap \mathrm{Im}(T_2^\infty)) \oplus (\mathrm{Im}(T_1^\infty) \cap \mathrm{Im}(T_2^\infty)) \to V.$$

Week 5, HW Problem 6. *Show that if T_1 and T_2 commute, the map* (28) *is an isomorphism.*

Hint: use Proposition 9.1.6.

9.2. **Eigenvectors and eigenvalues.**

9.2.1. Let $T : V \to V$ be a linear operator.

Definition 9.2.2. *We shall say that $v \in V$ is an* eigenvector *of T if*

$$Tv = \lambda \cdot v$$

for some $\lambda \in k$.

Evidently, $0 \in V$ is an eigenvector.

Definition 9.2.3. *We shall say that $\lambda \in k$ is an* eigenvalue *of T on V if there exists a* non-zero *eigenvector v such that $Tv = \lambda \cdot v$.*

The set of eigenvalues of T on V is called *the spectrum* of T on V. We denote this set by $\mathrm{Spec}\, T$.

For $\lambda \in k$ we set

$$V^\lambda = \{v \in V,\, Tv = \lambda \cdot v\} = \ker(T - \lambda \cdot \mathrm{Id}).$$

We call V^λ the λ-*eigenspace.*

With our conventions, $V^\lambda \neq 0$ if and only if λ is an eigenvalue.

9.2.4. We have the following basic fact:

Proposition 9.2.5. *Non-zero eigenvectors corresponding to distinct eigenvalues are linearly independent.*

Proof. Let $v_1, \ldots, v_n$ be a collection of non-zero eigevectors with pairwise distinct eigenvalues $\lambda_1, \ldots, \lambda_n$. We wish to show that $v_1, \ldots, v_n$ are linearly independent. We shall argue by induction on n.

For $n = 1$, there is nothing to prove. Assume the claim for $n - 1$. Suppose that

$$a_1 \cdot v_1 + \cdots + a_n \cdot v_n = 0.$$

Then

$$T(a_1 \cdot v_1 + \cdots + a_n \cdot v_n) = \lambda_1 \cdot a_1 \cdot v_1 + \cdots . + \lambda_n \cdot a_n \cdot v_n = 0.$$

Hence,

$$\lambda_1 \cdot (a_1 \cdot v_1 + \cdots + a_n \cdot v_n) - (\lambda_1 \cdot a_1 \cdot v_1 + \cdots . + \lambda_n \cdot a_n \cdot v_n) =$$
$$= (\lambda_1 - \lambda_2) \cdot a_2 \cdot v_2 + \cdots + (\lambda_1 - \lambda_n) \cdot a_n \cdot v_n = 0.$$

By the induction hypothesis, this implies that

$$(\lambda_1 - \lambda_2) \cdot a_2 = \cdots = (\lambda_1 - \lambda_n) \cdot a_n = 0.$$

Since $\lambda_1 \neq \lambda_i$, $i \neq 1$, we obtain that $a_i = 0$ for $i \neq 1$. The latter also implies that $a_1 = 0$, since $v_1 \neq 0$.

□

Corollary 9.2.6. *The spectrum of T on V consists of at most* $\dim(V)$ *elements.*

9.3. **Diagonalizabilty.**

9.3.1. We give the following definition:

Definition 9.3.2. *A linear operator $T : V \to V$ is called* diagonalizable *(or* semi-simple*) if V admits a basis consisting of eigenvectors of T.*

The reason for this terminology is that $\underline{e} = \{e_1, \dots, e_n\}$ is a basis consisting of eigenvectors of T if and only if the matrix $M_{T,\underline{e},\underline{e}}$ is diagonal (all off-diagonal entries are 0).

9.3.3. Not all operators are diagonalizable:

Proposition 9.3.4. *If T is nilpotent and diagonalizable, then $T = 0$.*

For the proof of the proposition we will use the following:

Lemma 9.3.5. *If T is nilpotent, then its only eigenvalue is* 0*.*

Proof of Lemma 9.3.5. If $Tv = \lambda \cdot v$, then for any n,

$$T^n v = \lambda^n \cdot v.$$

However, $T^n = 0$ for $n \gg 0$. Hence, $\lambda^n = 0$ for some n, and hence $\lambda = 0$. □

Proof of Proposition 9.3.4. By Lemma 9.3.5, any eigenvector of T has eigenvalue 0, and hence belongs to $\ker(T)$. Hence, if V is spanned by eigenvectors, $V = \ker(T)$. I.e., $T = 0$. □

9.3.6. Another source of non-diagonalizabilty is the fact that our field k may not be algebraically closed. E.g., take T to be a nontrivial rotation operator on $\mathbb{R}^2$.

We shall soon prove that if k is algebraically closed, then "nilpotence" is the only obstruction.

9.3.7. But first we are going to prove the following characterization of diagonalizable operators that does not refer to the choice of basis:

Proposition 9.3.8. *Let $T : V \to V$ be a linear operator. Then the following conditions are equivalent:*

(a) *T is diagonalizable.*

(b) *V admits a direct sum decomposition $\underset{\lambda}{\oplus} V_\lambda \simeq V$, where each V_λ is T-invariant and $T|_{V_\lambda} = \lambda \cdot \mathrm{Id}_{V_\lambda}$.*

(c) *The map $\underset{\lambda \in \mathrm{Spec}(T)}{\oplus} V^\lambda \simeq V$ is an isomorphism.*

Note the difference between (b) and (c): in (b) the subspaces V_λ are *some* T-invariant subspaces with the specified properties. In (c) they are specifically the eigenspaces.

Proof. Let us first show that (b) implies (a). Indeed, given (b), choose bases in each V_λ, and string them together to obtain a basis for V. Then T is diagonal in this basis.

Conversely, given (a), let $e_1, \dots, e_n$ be a basis in which T is diagonal. Define

$$V_\lambda = \text{Span}(\{e_i \,|\, T(e_i) = \lambda \cdot e_i\})$$

(i.e., group the basis elements according to eigenvalue, and take the corresponding spans).

It is clear that (c) implies (b). Finally, let us show that (b) implies (c). With no restriction of generality, we can assume that all λ's are distinct (otherwise group the corresponding V_λ's together), and that each V_λ is non-zero (otherwise, omit it).

Then every λ appearing in (b) is an eigenvalue and

$$V_\lambda \subset V^\lambda.$$

It suffices to show that for every λ, the inclusion is $V_\lambda \subset V^\lambda$ is an equality. Take $v \in V^\lambda$. Since (b) gives a direct sum decomposition, we can write

$$v = v_{\lambda_1} + v_{\lambda_2} + \cdots + v_{\lambda_n},$$

where $\lambda_1 = \lambda$, and each $v_{\lambda_i} \in V_{\lambda_i} \subset V^{\lambda_i}$. Hence,

$$(v_{\lambda_1} - v) + v_{\lambda_2} + \cdots + v_{\lambda_n} = 0.$$

By Proposition 9.2.5, this implies that $v_{\lambda_2} = \cdots = v_{\lambda_n} = 0$ and $v = v_{\lambda_1}$, as desired.

□

10. Midterm Exam. Due: Mon, Oct. 8 at 3pm, by email

Problem 1. 5pts. Let $V_i, T_i : V_i \to V_i$, $i = 1, 2$ be a pair of finite-dimensional vector spaces equipped with an endomorphism. Let $S : V_1 \to V_2$ be a linear map such that the following diagram commutes

$$\begin{tikzcd}
V_1 \arrow[r, "S"] \arrow[d, "T_1"'] & V_2 \arrow[d, "T_2"] \\
V_1 \arrow[r, "S"] & V_2.
\end{tikzcd}$$

(In this case we say that S *intertwines* T_1 and T_2.) Note that in this case S maps $\ker(T_1)$ to $\ker(T_2)$, $\text{Im}(T_1)$ to $\text{Im}(T_2)$, etc.

Assume that S is surjective.

(a) 2pts. Give an example where the resulting map $\ker(T_1) \to \ker(T_2)$ is *not* surjective.

(b) 3pts. Prove that the map $\ker(T_1^\infty) \to \ker(T_2^\infty)$, induced by S, is surjective.

Problem 2. 5pts. Let V be a finite-dimensional vector space and $T : V \to V$ a nilpotent operator. Let $n := \dim(V)$.

(a) 2pts. Show that for $i = 1, \ldots, n$,

$$\dim(\ker(T^i)) \geq i.$$

(b) 3pts. Show that there exists a squence of vector subspaces

$$0 = V_0 \subset V_1 \subset V_2 \subset \ldots \subset V_{n-1} \subset V_n = V$$

such that T maps V_i to V_{i-1}.

Problem 3. 5pts. Let V be a finite-dimensional vector space and $T : V \to V$ a linear operator.

(a) 2pts. Assume that V admits a basis in which the matrix of T is *strictly upper-triangular* (i.e., all entries below *and* on the diagonal are zero). Show that T is nilpotent.

(b) 3pts. Assume that T is nilpotent. Show that V admits a basis in which the matrix of T is strictly upper triangular.

11. Tuesday, Oct. 9

11.1. **Generalized eigenspaces and eigenvectors.**

11.1.1. Let V be a finite-dimensional vector space, and $T : V \to V$ an endomorphism. Let λ be an element of the field k.

We define the *generalized eigenspace* $V^{(\lambda)}$ as

$$V^{(\lambda)} := \ker((T - \lambda)^\infty).$$

We shall refer to the elements of $V^{(\lambda)}$ as *generalized eigenvectors*.

We shall call the integer $\dim(V^{(\lambda)})$ the *multiplicity* of λ in $\operatorname{Spec}(T)$.

Lemma 11.1.2. *For $\lambda \in k$ the following conditions are equivalent:*
(a) $\lambda \in \operatorname{Spec}(T)$.
(b) $T - \lambda$ *is non-invertible.*
(c) $V^{(\lambda)} \neq 0$.

Proof. Obvious from Corollary 6.3.9. □

Week 6, HW Problem 1. *Let $V' \subset V$ be a T-invariant subspace. Show that T is invertible (resp., nilpotent) if and only if both $T|_{V'}$ and $T|_{V/V'}$ are invertible (resp., nilpotent).*

Week 6, HW Problem 2. *$V' \subset V$ be a T-invariant subspace. Show that* $\operatorname{Spec}(T) = \operatorname{Spec}(T|_{V'}) \cup \operatorname{Spec}(T|_{V/V'})$.

Week 6, HW Problem 3. *Let V have a basis such that the matrix of T in this basis is upper triangular. Let $\lambda_1, \ldots, \lambda_n$ be its diagonal entries (with possible repetitions). Show that the set $\{\lambda_1, \ldots, \lambda_n\}$ equals the spectrum of T.*

11.1.3. It is easy to see that $V^{(\lambda)}$ is T-invariant (this follows e.g. from the fact that the operator T commutes with $T-\lambda$).

Define

$$V^{\text{non-sp}} := \bigcap_{\lambda\in\operatorname{Spec}(T)} \operatorname{Im}((T-\lambda)^\infty).$$

This space is also T-invariant.

The following is the first version of the spectral decomposition theorem:

Theorem 11.1.4. (a) *The map*

$$\left(\bigoplus_{\lambda\in\operatorname{Spec}(T)} V^{(\lambda)}\right)\bigoplus V^{\text{non-sp}} \to V$$

is an isomorphism.

(a') *The restriction $T|_{V^{\text{non-sp}}}$ has an empty spectrum.*

(b) *Let $0\neq V_{(\lambda)}\subset V$ and $V_{\text{non-sp}}\subset V$ be T-invariant subspaces such that*

- *For each λ, the restriction $(T-\lambda)|_{V_{(\lambda)}}$ is nilpotent.*
- *The restriction $(T-\lambda)|_{V_{\text{non-sp}}}$ has an empty spectrum.*

Assume that the map

$$\left(\bigoplus_{\lambda} V_{(\lambda)}\right)\bigoplus V_{\text{non-sp}} \to V$$

is an isomorphism. Then the set of λ is precisely $\operatorname{Spec} T$, *$V_{(\lambda)}=V^{(\lambda)}$ for all λ, and $V_{\text{non-sp}}=V^{\text{non-sp}}$.*

The meaning of this theorem is that the pair (T,V) uniquely splits as a direct sum of "elementary" situations of the following two kinds:

- T is of the form $T_0+\lambda$, for some $\lambda\in k$, and where T_0 is nilpotent.
- T has an empty spectrum.

11.1.5. Here is an immediate corollary of Theorem 11.1.4:

Corollary 11.1.6. *Let $v_{\lambda_1},\dots,v_{\lambda_n}$ be non-zero generalized eigenvectors with distinct eigenvalues. Then the collection $\{v_{\lambda_1},\dots,v_{\lambda_n}\}$ is linearly independent.*

Note that the above corollary generalizes Proposition 9.2.5. But a direct proof would be much more complicated.

11.1.7. The rest of this subsection is devoted to the proof of Theorem 11.1.4.

First, we have:

Lemma 11.1.8. *Let W be a finite-dimensional vector space, and $S:W\to W$ a nilpotent endomorphism. Then for any $\lambda\neq 0$, the operator $S-\lambda$ is invertible.*

Proof. Follows by combining Lemmas 11.1.2 and 9.3.5. □

(Concretely, e.g. the inverse of $1-S$ is $1+S+S^2+S^3+\cdots$, a finite sum since S is nilpotent.)

Corollary 11.1.9. *Suppose that $\lambda_1\neq\lambda_2$. Then $V^{(\lambda_1)}\cap V^{(\lambda_2)}=0$.*

Proof. It is enough to show that $T - \lambda_1$ is invertible on $V^{(\lambda_2)}$. Now apply Lemma 11.1.8 to $W = V^{(\lambda_2)}$, $S = T - \lambda_2$, $\lambda = \lambda_1 - \lambda_2$. □

The assertion of part (a) of Theorem 11.1.4 follows from the next proposition:

Proposition 11.1.10. *Let $\lambda_1, \ldots, \lambda_n$ be pairwise distinct elements of k. Then the map*

$$\left(V^{(\lambda_1)} \oplus \cdots \oplus V^{(\lambda_n)}\right) \bigoplus \left(\bigcap_{i=1,\ldots,n} \mathrm{Im}((T-\lambda_i)^\infty)\right) \to V$$

is an isomorphism.

Week 6, HW Problem 4. *Prove Proposition 11.1.10.*

Hint: Argue by induction on n, using Theorem 8.6.8 and Corollary 11.1.9.

11.1.11. Let us now prove part (a'). We need to show that for any $\lambda \in k$, the operator $(T-\lambda)|_{V^{\text{non-sp}}}$ has zero kernel. However, if $v \in \ker((T-\lambda)|_{V^{\text{non-sp}}})$, then $v \in \ker(T-\lambda)$, and hence $v \in V^\lambda \subset V^{(\lambda)}$, which contradicts the direct sum decomposition of point (a).

11.1.12. Finally, let us prove point (b). By assumption

$$V_{(\lambda)} \subset V^{(\lambda)}.$$

In particular, $\{\lambda\} \subseteq \operatorname{Spec} T$.

We claim that $V_{\text{non-sp}} \subset V^{\text{non-sp}}$. For this it is enough to show that

$$V_{\text{non-sp}} \subset \mathrm{Im}((T-\lambda)^\infty)$$

for every λ. The latter follows from Proposition 9.1.6.

Hence, we obtain that the map

$$\left(\bigoplus_\lambda V_{(\lambda)}\right) \bigoplus V_{\text{non-sp}} \to V \to 0$$

factors as

$$\left(\bigoplus_\lambda V_{(\lambda)}\right) \bigoplus V_{\text{non-sp}} \to \left(\bigoplus_{\lambda \in \mathrm{Spec}(T)} V^{(\lambda)}\right) \bigoplus V^{\text{non-sp}} \to V$$

(i.e., as the direct sum of the inclusion maps on each factor), where the second arrow is an isomorphism by point (a), and the composition is an isomorphism by assumption. Hence, the first arrow is an isomorphism, implying that it is an isomorphism on each direct summand (and that $\{\lambda\} = \operatorname{Spec} T$, since if any factors were left out it couldn't possibly be surjective).

□

Week 6, HW Problem 5. *Let $V' \subset V$ be a T-invariant subspace. Denote $T' := T|_{V'}$, $V'' := V/V'$ and $T'' := T|_{V/V'}$. Show that we have the exact sequences*

$$0 \to (V')^{(\lambda)} \to V^{(\lambda)} \to (V'')^{(\lambda)} \to 0, \quad \forall \lambda \in \mathrm{Spec}(T)$$

and

$$0 \to (V')^{\text{non-sp}} \to V^{\text{non-sp}} \to (V'')^{\text{non-sp}} \to 0.$$

11.2. **Algebraically closed versus non-algebraically closed fields.**

11.2.1. We recall the following definition:

Definition 11.2.2. *A field k is said to be algebraically closed if every polynomial with coefficients in k has a root in k.*

For example, $\mathbb{C}$ is algebraically closed (the "fundamental theorem of algebra"), though this is really a topological fact.

We are going to prove:

Proposition 11.2.3. *Suppose that k is* not *algebraically closed. Then there exists a pair (T, V) with* $\operatorname{Spec}(T) = \emptyset$.

Proof. Let $p(t) \in k[t]$ be a polynomial that has no root. With no restriction of generality, we may assume that $p(t)$ is irreducible (that is to say, it cannot be factored as a product of two polynomials of smaller degrees). By assumption $\deg(p(t)) > 1$.

Consider the vector space $k[t]$, polynomials with coefficients in k, with the evident addition and scalar multiplication. Let V denote the quotient space of $k[t]$ by the vector subspace $W := p(t) \cdot k[t]$. I.e., W consists of all polynomials that are divisible by $p(t)$. We shall denote the canonical projection $k[t] \to V$ by $q(t) \mapsto \overline{q(t)}$. Note that V is finite-dimensional. In fact, it has as a basis

$$1, \bar{t}, \ldots, \overline{t^n},$$

where $n = \deg(p(t)) - 1$.

The operator given by multiplication by t (i.e., $q(t) \mapsto t \cdot q(t)$) defines a linear map $k[t] \to k[t]$ that sends W to itself. Hence, it gives rise to an endomorphism of V, which we shall denote by T. I.e.,

$$T(\overline{q(t)}) = \overline{t \cdot q(t)}.$$

We claim that $\operatorname{Spec}(T)$ is empty. Indeed, suppose that λ is an eigenvalue of T, i.e., the operator $T - \lambda$ has a non-zero kernel. I.e., we assume that there exists $q(t) \in k[t]$ with $\overline{q(t)} \neq 0$, but such that $(T - \lambda)(\overline{q(t)}) = 0$. That is to say, $q(t) \notin W$ but $(t - \lambda) \cdot q(t) \in W$. I.e., $p(t)$ divides $(t - \lambda) \cdot q(t)$ but does not divide either $q(t)$ or $t - \lambda$ (the latter because $\deg(p(t)) > 1$). This is a contradiction in view of the following:

Lemma 11.2.4. *If an irreducible polynimial $p(t)$ divides a product $q_1(t) \cdot q_2(t)$ then it divides at least one of the factors.*

□

12. Thursday, Oct. 11

12.1. **Homomorphisms of rings.**

12.1.1. Let R_1 and R_2 be a pair of rings. A ring homomorphism is a map of sets

$$\phi : R_1 \to R_2$$

such that

- ϕ is a homomorphism of abelian groups (with respect to addition on both sides);
- $\phi(r' \cdot r'') = \phi(r') \cdot \phi(r'')$.
- $\phi(1_{R_1}) = 1_{R_2}$.

12.1.2. The following example will be used in the sequel. Let $R_2 = R$ be an arbitrary ring, and let $R_1 = R_0[t]$ be the ring of polynimials in one variable over another ring R_0. Let

$$\phi : R_0[t] \to R'$$

be a ring homomorphism.

We attach to it the data of (ϕ_0, T), where

$$\phi_0 =: \phi|_{R_0}, \quad R_0 \to R,$$

(we think of R_0 as a subring of R corresponding to scalar polynomials) and $T := \phi(t)$.

Note that the identity $r_0 \cdot t = t \cdot r_0$ in $R_0[t]$ implies that

$$\phi_0(r_0) \cdot T = \phi(r_0) \cdot \phi(t) = \phi(r_0 \cdot t) = \phi(t \cdot r_0) = \phi(t) \cdot \phi(r_0) = T \cdot \phi_0(r_0).$$

We now claim:

Proposition 12.1.3. *The above assignment $\phi \mapsto (\phi_0, T)$ defines an isomorphism from the set $\operatorname{Hom}_{\text{Ring}}(R_0[t], R)$ to the subset of $\operatorname{Hom}_{\text{Ring}}(R_0, R) \times R$, consisting of pairs*

$$(\phi_0 \in \operatorname{Hom}_{\text{Ring}}(R_0, R), T \in R)$$

satisfying

$$\phi_0(r_0) \cdot T = T \cdot \phi_0(r_0), \quad \forall r_0 \in R_0.$$

Proof. We shall construct an inverse map. Namely, given

$$(\phi_0 \in \operatorname{Hom}_{\text{Ring}}(R_0, R), T \in R)$$

with the specified property, we define a homomorphism

$$\phi : R_0[t] \to R$$

by the formula

$$\phi(a_0 + a_1 \cdot t + \cdots + a_n \cdot t^n) := \phi_0(a_0) + \phi_0(a_1) \cdot T + \cdots + \phi_0(a_n) \cdot T^n.$$

□

12.2. Left ideals and two-sided ideals.

12.2.1. Let R be a ring. A left ideal in R is by definition an R-submodule $I \subset R$, where R is viewed as a module over itself via multiplication on the left. I.e., $I \subset R$ is a subgroup with respect to addition, and

$$i \in I, r \in R \Rightarrow r \cdot i \in I.$$

If $I \subset R$ is a left ideal, we can consider the quotient R/I, which is an R-module.

Week 6, HW Problem 6. *Let R be commutative. Show that R is a field if and only if the only (left) ideals in R are $\{0\}$ and R.*

12.2.2. *Example.* Let R be a ring and $r \in R$ be an element. We consider the subset

$$(r) := \{r' \cdot r \,|\, r' \in R\}.$$

It is clear that (r) is a left ideal.

12.2.3. *Example.* Consider the ring $R = \mathrm{End}(V)$, where V is a vector space over a field. For a vector subspace $W \subset V$ consider

$$I_W := \{T \in \mathrm{End}(V) \,|\, W \subset \ker(T)\}.$$

It is easy to see that I_W is a left ideal.

Bonus Problem 1, 1pt.[1] *Show that any left ideal in* $\mathrm{End}(V)$ *is of the form* I_W *for a uniquely defined vector subspace* $W \subset V$. *Deduce that any two-sided ideal in* $\mathrm{End}(V)$ *(see below) is either* $\{0\}$ *or* $\mathrm{End}(V)$.

12.2.4. Let $I \subset R$ be a left ideal.

Definition 12.2.5. *We shall say that* I *is a two-sided ideal if*

$$i \in I, r \in R \;\Rightarrow\; i \cdot r \in I.$$

Of course, in a commutative ring there is no difference between left and two-sided ideals.

Lemma 12.2.6. *Let* $\phi : R_1 \to R_2$ *be a ring homomorphism. Then*

$$\ker(\phi) := \{r_1 \in R_1 \,|\, \phi(r_1) = 0\}$$

is a two-sided ideal.

Remark 12.2.7. *Note that a two-sided ideal is not a subring — because it does not contain* 1.

12.2.8. The following is proved in the same way as Theorems 2.3.9 and 3.1.2:

Proposition 12.2.9. *Let* R *be a ring and let* $I \subset R$ *be a two-sided ideal.*

(a) *The quotient abelian group* R/I *has a unique structure of ring so that the canonical map* $\pi : R \to R/I$ *is a ring homomorphism.*

(b) *Let* $\phi : R \to R'$ *be a ring homomorphism such that* $\phi|_I = 0$. *Then there exists a uniquely defined ring homomorphism* $\widetilde{\phi} : R/I \to R'$ *such that* $\phi = \widetilde{\phi} \circ \pi$.

12.2.10. We shall now study ideals in the rings $\mathbb{Z}$ and $k[t]$.

Lemma 12.2.11. *Let* R *be either* $\mathbb{Z}$ *or* $k[t]$, *and let* $I \subset R$ *be an ideal, which is neither* 0 *not all of* R.

(a) *If* $R = \mathbb{Z}$, *then* I *is of the form* (n) *for a unique positive integer* n.

(b) *If* $R = k[t]$, *then* I *is of the form* $(p(t))$ *for a unique monic*[2] *polynomial* $p(t)$.

Proof. Apply the Euclidean algorithm in both cases. □

We now claim:

Proposition 12.2.12.

(a) *For* $n \in \mathbb{Z}^{>0}$, *the quotient ring* $\mathbb{Z}/n\mathbb{Z}$ *is a field if and only if* n *is prime.*

(b) *For a monic polynomial* $p(t)$, *the quotient ring* $k[t]/p(t)$ *is a field if and only if* $p(t)$ *is irreducible.*

[1] The score for bonus problems goes toward the total score. These problems are to be submitted to the CA's by the time you turn in your final.

[2] A polynomial $a_n \cdot t^n + \ldots + a_1 \cdot t + a_0$ is called *monic* if $a_n = 1$.

Proof. We will prove point (b). Point (a) is similar, but simpler. For an element $q(t) \in k[t]$ and let $\overline{q(t)}$ denote its image in $k[t]/p(t)$.

First, suppose that $k[t]/p(t)$ is a field. Suppose for contradiction that $p(t)$ is reducible, i.e., that it can be factored as $p_1(t) \cdot p_2(t)$, where $\deg(p_i(t)) < \deg(p(t))$. Then $p_i(t)$, $i = 1, 2$ are not divisible by $p(t)$, and hence $\overline{p_i(t)} \neq 0$. However,

$$\overline{p_1(t)} \cdot \overline{p_2(t)} = \overline{p(t)} = 0,$$

which is a contradiction, since both are invertible.

Assume now that $p(t)$ is irreducible. For an element $q(t) \in k[t]$ such that $\overline{q(t)} \neq 0$, we need to show that $1 \in k[t]/p(t)$ is conatined in the image of the map

$$\overline{q(t)} \cdot - : k[t]/p(t) \to k[t]/p(t).$$

It of course suffices to show that the above map is surjective.

We regard $k[t]/p(t)$ as a finite-dimensional vector space over k. Then $\overline{q(t)} \cdot -$ is a linear operator. Hence, by rank-nullity, it is enough to show that $\overline{q(t)} \cdot -$ is injective. Let $q_1(t) \in k[t]$ such that

$$\overline{q(t)} \cdot \overline{q_1(t)} = 0.$$

Then we obtain that $q(t) \cdot q_1(t)$ is divisible by $p(t)$. But by assumption, $q(t)$ is not divisible by $p(t)$. Hence $p(t)$ divides $q_1(t)$ — that is to say, $\overline{q_1(t)} = 0$.

□

12.2.13. For a prime number p we denote the resulting field $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$. Note that it has the following feature:

$$\underbrace{1 + \ldots + 1}_{p} = 0.$$

12.2.14. Let k be a field, and $p(t)$ an irreducible polynomial of degree > 1 (in particular, by Bezout's theorem, $p(t)$ has no roots).

Let us note the following feature of the field $k' := k[t]/p(t)$ constructed in Proposition 12.2.12. Let us regard $p(t)$ as a polynomial with coefficients in k' via the embedding $k \subset k'$. We claim that $p(t)$ has a root in k'.

Namely, consider the element $\bar{t} \in k[t]/p(t) = k'$. We claim that $p(\bar{t}) = 0$. Indeed,

$$p(\bar{t}) = \overline{p(t)} = 0.$$

We shall say that k' is obtained from k by *adjoining a root of* $p(t)$.

12.3. Spectral decomposition over algebraically closed fields.

12.3.1. We are going to prove:

Theorem 12.3.2. *Let V be a non-zero finite-dimensonal vector space over an algebraically closed field k. Let $T : V \to V$ be a linear operator. Then* $\mathrm{Spec}(T) \neq \emptyset$.

As a corollary, from Theorem 11.1.4 we obtain:

Theorem 12.3.3. *Let V be a non-zero finite-dimensonal vector space over an algebraically closed field k. Let $T : V \to V$ be a linear operator. Then the map*

$$\bigoplus_{\lambda \in \mathrm{Spec}(T)} V^{(\lambda)} \to V$$

is an isomorphism.

Proof of Theorem 12.3.2. Consider the ring $\mathrm{End}(V)$. We have a tautological ring homomorphism

$$\phi_0 : k \to \mathrm{End}(V), \quad \lambda \mapsto \lambda \cdot \mathrm{Id}\,.$$

Using the pair (ϕ_0, T), by Proposition 12.1.3, we obtain a ring homomorphism

$$\phi : k[t] \to \mathrm{End}(V).$$

We claim that ϕ is not injective. Indeed, we can consider $\mathrm{End}(V)$ as a vector space over k. It is finite-dimensional of dimension $\dim(V)^2$. Hence, the elements

$$\mathrm{Id}, T, T^2, \ldots, T^n$$

are linearly dependent as soon as $n > \dim(V)^2$. Hence, for such n, there exist coefficients $a_i \in k$ not all zero such that

$$a_0 \cdot \mathrm{Id} + a_1 \cdot T + \cdots + a_n \cdot T^n = 0.$$

Hence, by construction, the polynomial

$$p(t) := a_0 + a_1 \cdot t + \cdots + a_n \cdot t^n$$

belongs to the kernel of ϕ.

Since k is algebraically closed, by Bezout's theorem, $p(t)$ is of the form

$$a_0 \cdot (t - \lambda_1) \cdot \ldots \cdot (t - \lambda_n),$$

where $0 \neq a_0 \in k$.

Hence, we obtain that the element

$$a_0 \cdot (T - \lambda_1) \cdot \ldots \cdot (T - \lambda_n) \in \mathrm{End}(V)$$

equals 0. This implies that at least one of the operators $T - \lambda_i$ is non-invertible. Hence, we are done by Lemma 11.1.2.

□

12.3.4. Let us go back to the homomorphism

$$\phi : k[t] \to \mathrm{End}(V)$$

constructed in the course of the proof of Theorem 12.3.3. By Lemma 12.2.11, the ideal $\ker(\phi)$ is of the form $(p(t))$ for a uniquely defined monic polynomial $p(t)$.

We shall denote this polynomial by $\min_T(t)$ and refer to it as the *minimal polynomial* of T.

Note that $\min_T(t)$ is defined regardless of whether k is algebraically closed.

Week 6, HW Problem 7. *Let $V' \subset V$ be a T-invariant subspace. Let T' and T'' be as in Problem 5. Show that* $\min_{T'}(t)$ *and* $\min_{T''}(t)$ *each divide* $\min_T(t)$. *Show that* $\min_T(t)$ *divides the product* $\min_{T'}(t) \cdot \min_{T''}(t)$.

Week 6, HW Problem 8. *Assume that T is nilpotent. Show that its minimal polynomial equals t^m for some $1 \leq m \leq \dim(V)$.*

12.3.5. We now claim:

Theorem 12.3.6. *Let V be a finite-dimensional vector space and $T : V \to V$ a linear operator. We have $V^{\text{non-sp}} = 0$ if and only if the polynomial $\min_T(t)$ is of the form*

$$(t - \lambda_1) \cdot \ldots \cdot (t - \lambda_n), \quad \lambda_i \in k.$$

Week 6, HW Problem 9. *Prove Theorem 12.3.6.*

12.3.7. We claim:

Proposition 12.3.8. *An element $\lambda \in k$ is a root of $\min_T(t)$ if and only if it is an eigenvalue of T on V.*

Proof. Suppose that λ is an eigenvalue. Consider the operator $T' := T|_{V^{(\lambda)}}$. By Problem 8, $\min_{T'}(t) = (t-\lambda)^m$ for some m. By Problem 7, $\min_{T'}(t)$ divides $\min_T(t)$. Hence λ is a root of $\min_T(t)$.

Suppose that λ is a root of $\min_T(t)$. Then we can write

$$\min_T(t) = p(t) \cdot (t - \lambda),$$

for some polynomial $p(t)$. By the definition of $\min_T(t)$, we have $p(t) \notin \ker(\phi)$.

We have

$$0 = \phi(\min_T(t)) = \phi(p(t)) \cdot (T - \lambda).$$

Since $\phi(p(t)) \neq 0$, we obtain that $T - \lambda$ is non-invertible. Hence, λ is an eigenvalue. □

Week 6, HW Problem 10. *Let $T : V \to V$ be as above. Show that $V^{\text{non-sp}} = 0$ if and only if V admits a basis in which the matrix of T is upper-triangular. Show that the set of diagonal entries of the corresponding matrix equals* $\text{Spec}(T)$.

13. Tuesday, Oct. 16

13.1. **Minimal polynimal and spectral decomposition.** We will solve some of the problems from last week's problem set.

13.1.1. *Solution to Problem 7, Week 6.* First, we show that $\min_{T'}(t)$ and $\min_{T''}(t)$ each divide $\min_T(t)$. Let

$$\phi' : k[t] \to \text{End}(V') \text{ and } \phi' : k[t] \to \text{End}(V'')$$

be the homomorphisms corresponding to $T' \in \text{End}(V')$ and $T'' \in \text{End}(V'')$, respectively. Note that for $p(t) \in k[t]$, we have:

$$\phi'(p(t)) = \phi(p(t))|_{V'} \text{ and } \phi''(p(t)) = \phi(p(t))|_{V''}. \tag{29}$$

We have to show that

$$\phi'(\min_T) = 0 \text{ and } \phi''(\min_T) = 0.$$

This follows immediately from (29).

To show that $\min(T)$ divides $\min_{T'} \cdot \min_{T''}$ we need to show that the operator $\min_{T'}(T) \cdot \min_{T''}(T)$ vanishes. This follows from the next lemma:

Lemma 13.1.2. *Let S_1, S_2 be two endomorphisms of V, and let $V' \subset V$ be a subspace which is invariant with respect to both S_1 and S_2. Assume that $S_1|_{V'} = 0$ and $S_2|_{V/V'} = 0$. Then $S_1 \circ S_2 = 0$.*

□

Corollary 13.1.3. *Let V be a direct sum of two T-invariant subspaces V_1 and V_2. Then* $\min_T$ *divides* $\min_{T|_{V_1}} \cdot \min_{T|_{V_2}}$.

Proof. The proof follows from [Problem 7, Week 6] using the fact that V_2 maps isomorphically to V/V_1. □

Of course the generalization to direct sums with finitely many factors is immediate by induction.

13.1.4. We will now prove:

Proposition 13.1.5. *Let $T : V \to V$ be such that $\phi(p(t)) = 0$ for some polynomial $p(t)$ that factors as*

$$p(t) = \prod_i (t - \lambda_i).$$

Then $V^{\text{non-sp}} = 0$.

Proof. Observe that the operator

$$\prod_i (T - \lambda_i)$$

is zero on $V^{\text{non-sp}}$. Hence, at least one $T - \lambda_i$ would be non-invertible on $V^{\text{non-sp}}$ if it were nonzero. □

13.1.6. Assume now that $V^{\text{non-sp}} = 0$. I.e., the map

$$\bigoplus_{\lambda \in \text{Spec}(T)} V^{(\lambda)} \to V$$

is an isomorphism.

For each λ, by [Problem 8, Week 6],

$$\min_{T|_{V^{(\lambda)}}} = (t - \lambda)^{m_\lambda}, \quad 1 \leq m_\lambda \leq \dim(V^{(\lambda)}).$$

Proposition 13.1.7. $\min_T = \prod\limits_{\lambda \in \text{Spec}(T)} (t - \lambda)^{m_\lambda}$.

Proof. On the one hand, by Corollary 13.1.3 (with several direct summands instead of two), we obtain that $\min_T$ divides $\prod\limits_{\lambda \in \text{Spec}(T)} (t - \lambda)^{m_\lambda}$. On the other hand, by [Problem 7, Week 6], each $(t-\lambda)^{m_\lambda}$ divides $\min_T$. Since the $(t-\lambda)^{m_\lambda}$'s are relatively prime, we have our claim. □

Note that Propositions 13.1.5 and 13.1.7 together imply Theorem 12.3.6.

Week 7, HW Problem 1. *Show that T is diagonalizable if and only if its minimal polynomial is of the form* $\prod\limits_{\lambda \in \text{Spec}(T)} (t - \lambda)$.

13.1.8. *Solution to Problem 10, Week 6.* Assume that $V^{\text{non-sp}} = 0$. Choose a basis in each $V^{(\lambda)}$ so that $T - \lambda$ is strictly upper-triangular (Problem 3(b) on the Midterm). Then the resulting basis for V has the desired property.

Conversely, let $e_1, \ldots, e_n$ be a basis in which V is upper-triangular. Define $V_i = \text{Span}(e_1, \ldots, e_n)$. Consider the sequence of subspaces

$$0 = V_0 \subset V_1 \subset \cdots \subset V_{n-1} \subset V_n = V.$$

Applying [Problem 7, Week 6] repreatedly, we obtain that $\min_T$ divides the product

$$\prod_{i=1,\ldots,n} \min_{T_{V_i/V_{i-1}}}.$$

Since V_i/V_{i-1} is 1-dimensional (spanned by the image of e_i),

$$\min_{T_{V_i/V_{i-1}}} = t - \lambda_i,$$

where λ_i is the i-th diagonal entry of T. Hence we are done by Proposition 13.1.5. □

Week 7, HW Problem 2. *Show that in a basis in which T is upper-triangular, the number of occurences of $\lambda \in k$ as a diagonal entry of T equals* $\dim(V^{(\lambda)})$.

Suggested strategy: use [Problem 5, Week 6] and use induction.

13.2. **The characteristic polynomial.**

13.2.1. Let T be a finite-dimensional vector space over k, and let $T : V \to V$ be a linear operator. Choosing a basis $\underline{e}$ of V, we attach to T an $(n \times n)$-matrix $M_{T,\underline{e},\underline{e}}$ with coefficients in k.

Consider the commutative ring $R = k[t]$, and consider the $(n \times n)$-matrix with coefficients in R equal to

$$t \cdot \mathbf{1} - M_{T,\underline{e},\underline{e}},$$

where $\mathbf{1}$ denotes the unit matrix (1's on the diagonal and 0's elsewhere).

The characteristic polynomial of T, denoted

$$\text{ch}_T(t) \in k[t]$$

is defined as $\det(t \cdot \mathbf{1} - M_{T,\underline{e},\underline{e}})$ (with e.g. the determinant of an $(n \times n)$ matrix M defined for now as $\sum_{\sigma \in S_n} \text{sign}(\sigma) \prod_{i=1}^n M_{i,\sigma(i)}$).

Here we are using the fact that for any $(n \times n)$-matrix with coefficients in a commutative ring R, its determinant is defined as an element of R.

The usual proof shows that $\text{ch}_T(t)$ is independent of the choice of the basis $\underline{e}$.

13.2.2. Assume for the moment that $V^{\text{non-sp}} = 0$. We claim:

Proposition 13.2.3. $\text{ch}_T(t) = \prod_{\lambda \in \text{Spec}(T)} (t - \lambda)^{\dim(V^{(\lambda)})}$.

Proof. Choose a bases as in the solution to [Problem 10, Week 6]. In this case, the matrix of $t \cdot \mathbf{1} - M_{T,\underline{e},\underline{e}}$ is upper-triangular, with $(t - \lambda)$ appearing as a diagonal entry exactly $\dim(V^{(\lambda)})$ times. The assertion now follows from the fact that, over an arbitrary commutative ring, the determinant of an upper triangular matrix is just the product of its diagonal entries. □

Corollary 13.2.4. *Under the above circumstances,* $\min_T$ *divides* ch_T.

Proof. This follows from Propositions 13.2.3 and 13.1.7. □

13.2.5. *The Cayley-Hamilton theorem.* We are going to prove:

Theorem 13.2.6 (Cayley-Hamilton)**.** *Let V be a finite-dimensional vector space over a field k, and $T : V \to V$ an endomorphism. Then the polynomial* $\min_T$ *divides* ch_T.

Proof. Note that if $\min_T$ factors as a product $\prod\limits_i (t-\lambda_i)$, the assertion of the theorem follows from Corollary 13.2.4 via Theorem 12.3.6.

We will reduce to the above case by the following procedure. First, we claim:

Lemma 13.2.7. *Let k be a field and $p(t) \in k[t]$ a polynomial. Then there exists an embedding of fields $k \hookrightarrow k'$, such that the image of $p(t)$ under $k[t] \to k'[t]$ factors into linear factors.*

(Here by "embedding of fields" we mean an injective ring homomorphism $k \to k'$. We will see that the only nonzero ring homomorphisms between two fields are injective (this because fields have only one nontrivial ideal: the zero ideal — whence the kernel must either be everything or "nothing").)

Proof. This follows by induction by section 12.2.14 (namely, pull off roots of irreducible factors one at a time). □

Thus, we can choose an embedding of fields $k \hookrightarrow k'$ so that the image of $\min_T$ under $k[t] \to k'[t]$ factors into linear factors.

Choose a basis $\underline{e}$ of V. Let

$$\mathrm{ch}_T(t) = a_0 + a_1 \cdot t + \cdots + a_{n-1} \cdot t^{n-1} + t^n, \quad a_i \in k$$

and

$$\min_T(t) = b_0 + b_1 \cdot t + \cdots + b_{m-1} \cdot t^{m-1} + t^m, \quad b_i \in k$$

We need to show the following identity in $\mathrm{Mat}_{n\times n}(k)$

$$a_0 \cdot \mathbf{1} + a_1 \cdot M_{T,\underline{e},\underline{e}} + \cdots + a_{n-1} \cdot M^{n-1}_{T,\underline{e},\underline{e}} + M^n_{T,\underline{e},\underline{e}} = 0,$$

while

$$b_0 \cdot \mathbf{1} + b_1 \cdot M_{T,\underline{e},\underline{e}} + \cdots + b_{m-1} \cdot M^{m-1}_{T,\underline{e},\underline{e}} + M^m_{T,\underline{e},\underline{e}} = 0$$

holds by definition.

Note that the embedding $k \hookrightarrow k'$ induces an injective homomorphism of rings

$$\mathrm{Mat}_{n\times n}(k) \to \mathrm{Mat}_{n\times n}(k').$$

(Namely, apply the homomorphism entry by entry!) Hence, it suffices to prove that the following identity in $\mathrm{Mat}_{n\times n}(k')$

$$a'_0 \cdot \mathbf{1} + a'_1 \cdot M'_{T,\underline{e},\underline{e}} + \cdots + a'_{n-1} \cdot (M'_{T,\underline{e},\underline{e}})^{n-1} + (M'_{T,\underline{e},\underline{e}})^n = 0, \tag{30}$$

while

$$b'_0 \cdot \mathbf{1} + b'_1 \cdot M'_{T,\underline{e},\underline{e}} + \cdots + b'_{m-1} \cdot (M'_{T,\underline{e},\underline{e}})^{m-1} + (M'_{T,\underline{e},\underline{e}})^m = 0, \tag{31}$$

holds tautologically (because the image of zero under any ring homomorphism is zero). Here a'_i (resp., b_i) denotes the image of a_i (resp., b_i) under $k \to k'$, and $M'_{T,\underline{e},\underline{e}}$ denotes the image of $M_{T,\underline{e},\underline{e}}$ under $\mathrm{Mat}_{n\times n}(k) \to \mathrm{Mat}_{n\times n}(k')$.

Note that, by construction,

$$\det(t \cdot \mathbf{1} - M'_{T,\underline{e},\underline{e}}),$$

as an element of $k'[t]$, equals the image of

$$\det(t \cdot \mathbf{1} - M_{T,\underline{e},\underline{e}}) \in k[t]$$

under $k[t] \to k'[t]$. (I.e., the formation of the determinant of a matrix is compatible with ring homomorphisms applied to the entries: one sees this immediately upon writing down our definition of the determinant of a matrix.) Hence,

$$\det(t \cdot \mathbf{1} - M'_{T,\underline{e},\underline{e}}) = a'_0 + a'_1 \cdot t + \cdots + a'_{n-1} \cdot t^{n-1} + t^n.$$

Note that we can regard $M'_{T,\underline{e},\underline{e}}$ as encoding a linear operator $T' : (k')^n \to (k')^n$ in the standard basis for $(k')^n$. Note that (31) implies that $\min_{T'}(t)$ divides the image of $\min_T(t)$ under $k[t] \to k'[t]$. In particular, by assumption, $\min_{T'}(t)$ splits into linear factors. Hence our reduction is complete: the identity (30) follows from applying our earlier work (the first step of this proof) to T'. □

13.3. **Simulataneous generalized eigenspaces.**

Let V be a finite-dimensional vector space. Let

$$T_1, T_2 : V \to V$$

be a pair of endomorphisms. Assume that that T_1 and T_2 commute, i.e.,

$$T_1 \circ T_2 = T_2 \circ T_1.$$

Assume also that $\min_{T_1}$ and $\min_{T_2}$ both split into linear factors. For a pair of elements $\lambda_1, \lambda_2 \in k$ define

$$V^{(\lambda_1,\lambda_2)} := \ker((T_1 - \lambda_1)^\infty) \cap \ker((T_2 - \lambda_2)^\infty).$$

This is the space of *simulataneous generalized eigenvectors* for T_1 and T_2.

We shall say that $(\lambda_1, \lambda_2) \in \mathrm{Spec}(T_1, T_2)$ if $V^{(\lambda_1,\lambda_2)} \neq 0$. We shall refer to the set $\mathrm{Spec}(T_1, T_2)$ as the *joint spectrum* of T_1 and T_2.

Week 7, HW Problem 3. *Show that the map*

$$\bigoplus_{(\lambda_1,\lambda_2) \in \mathrm{Spec}(T_1,T_2)} V^{(\lambda_1,\lambda_2)} \to V$$

is an isomorphism.

Week 7, HW Problem 4. *Formulate and prove an analogue of Problem 3 above, when, instead of a pair of commuting operators, we have a (possibly infinite) family of pairwise commuting operators $T_i \in \mathrm{End}(V)$.*

13.4. **Mini-project: commutative finite-dimensional algebras.**

13.4.1. First, let us note the following construction: let $R_1, \dots, R_n$ be rings. Then we can form a ring

$$R := R_1 \oplus \cdots \oplus R_n,$$

with componentwise addition and multiplication.

Note that the unit in R is the element

$$(1_{R_1}, \dots, 1_{R_n}) \in R_1 \oplus \cdots \oplus R_n.$$

Note that each R_i is a two-sided ideal in R. Conversely, if I_i are two-sided ideals in R such that the map

$$\underset{i}{\oplus} I_i \to R$$

is an isomorphism of abelian groups (here, equivalently, a bijection), then each I_i has a structure of (unital) ring. (Do you see why? Who is the unit in each?) Call these rings (with underlying abelian group I_i) R_i. Then R is recovered as the direct sum of the R_i's in the above sense.

13.4.2. Let k be an algebraically closed field. Let R be a commutative ring equipped with a ring homomorphism $k \to R$.

In this case we shall say that R is a *k-algebra*. A homomorphism of k-algebras $R_1 \to R_2$ is a ring homomorphism that respects the homomorphism of k into each.

The structure on R of module over itself induces a structure on R of k-module, i.e., k-vector space.

13.4.3. For this current mini-project we are going to assume that R is finite-dimensional as a vector space over k.

We define $\text{Spec}(R)$ as the set of k-algebra homomorphisms $\alpha : R \to k$ (i.e., ring homomorphisms $R \to k$ such that $k \to R \to k$ is the identity). For $\alpha \in \text{Spec}(R)$ define

$$R_\alpha := \{r \in R \mid \forall r' \in \ker(\alpha)\ \exists n \in \mathbb{Z}^+ \text{ s.t. } (r')^n \cdot r = 0\}.$$

Bonus Problem 2, 4pts.

(a) *Show that each R_α is an ideal and is non-zero.*

(b) *Show that the map*

$$\underset{\alpha \in \text{Spec}(R)}{\oplus} R_\alpha \to R$$

is an isomorphism.

(c) *Deduce that every R as above can be decomposed uniquely as a direct sum $R \simeq \underset{i \in I}{\oplus} R_i$, where the set I identifies with* $\text{Spec}(R)$ *and, for every $i \in I$, the k-algebra R_i is such that* $\text{Spec}(R_i)$ *is a one-element set.*

(d) Assume that $\text{Spec}(R)$ *is a one-element set. Show that the kernel of the corresponding unique homomorphism $R \to k$ is nilpotent (every element vanishes to some power), and every element not in this kernel is invertible.*

Suggested strategy: Use [Problem 4, Week 7] for $V = R$ with T_i taken to be the operators $r \cdot -$ for $r \in R$.

13.5. **Spectral projectors.**

13.5.1. Let V be a finite-dimensional vector space, and $T \in \operatorname{End}(V)$. Write

$$V \simeq \left(\bigoplus_{\lambda \in \operatorname{Spec}(T)} V^{(\lambda)} \right) \bigoplus V^{\text{non-sp}}.$$

For $\lambda \in \operatorname{Spec}(T)$, define an operator

$$\operatorname{pr}_\lambda : V \to V$$

by

$$\operatorname{pr}_\lambda(v) = \begin{cases} v, & v \in V^{(\lambda)} \\ 0, & v \in V^{(\mu)}, \mu \neq \lambda \\ 0, & v \in V^{\text{non-sp}}. \end{cases}$$

Recall the homomorphism

$$\phi : k[t] \to \operatorname{End}(V), \quad t \mapsto T.$$

Proposition 13.5.2. *There exists a polynomial $p_\lambda(t) \in k[t]$ such that*

$$\operatorname{pr}_\lambda = \phi(p_\lambda(t)).$$

Proof. Write

$$\min_T(t) = (t - \lambda)^{m_\lambda} \cdot q(t),$$

where $q(t)$ and $(t - \lambda)$ are coprime (recall that we now know precisely what $q(t)$ is: the product of the minimal polynomials of T on the non-λ generalized eigenspaces and that of T on the non-spectral part). It follows from [Problems 7 and 8, Week 6] and Proposition 12.3.8 that $(t - \lambda)^{m_\lambda}$ equals $\min_{T|_{V^{(\lambda)}}}$.

Since $q(t)$ and $(t - \lambda)^{m_\lambda}$ are coprime, there exist polynomials $r(t), s(t) \in k[t]$ such that

$$r(t) \cdot (t - \lambda)^{m_\lambda} + s(t) \cdot q(t) = 1.$$

We claim that

$$p_\lambda(t) := s(t) \cdot q(t)$$

has the required property.

Indeed, for $v \in V^{(\lambda)}$, we have

$$r(T) \cdot (T - \lambda)^{m_\lambda} v + s(T) \cdot q(T) v = v,$$

however, $(T - \lambda)^{m_\lambda} v = 0$, since $(T - \lambda)^{m_\lambda}|_{V^{(\lambda)}} = \min_{T|_{V^{(\lambda)}}}$.

For $v \in V^{(\mu)}$ (resp., $v \in V^{\text{non-sp}}$), we have

$$q(T)v = 0,$$

since $q(t)$ is divisible by $\min_{T|_{V^{(\mu)}}}$ (resp., $\min_{T|_{V^{\text{non-sp}}}}$) — again because the minimal polynomial on V is the product of those on the generalized eigenspaces (and that of the non-spectral part). Hence,

$$s(T) \cdot q(T) v = 0.$$

□

13.5.3. Define

$$\mathrm{pr}_{\text{non-sp}} : V \to V$$

by

$$\mathrm{pr}_{\text{non-sp}}(v) = \begin{cases} 0, & v \in V^{(\lambda)}, \quad \lambda \in \mathrm{Spec}(T) \\ v, & v \in V^{\text{non-sp}}. \end{cases}$$

Week 7, HW Problem 5. *Show that there exists $p_{\text{non-sp}} \in k[t]$ such that $\mathrm{pr}_{\text{non-sp}} = \phi(p_{\text{non-sp}}(t))$.*

14. Thursday, Oct. 18

14.1. **Jordan decomposition.** Let $T : V \to V$ be a linear operator. Assume that $V^{\text{non-sp}} = 0$. We have:

Theorem 14.1.1. *There exist operators T^{ss} and T^{nilp} with T^{ss} diagonalizable and T^{nilp} nilpotent such that:*

- $T = T^{\text{ss}} + T^{\text{nilp}}$*;*
- $T^{\text{ss}} \circ T^{\text{nilp}} = T^{\text{nilp}} \circ T^{\text{ss}}$*.*

Furthermore, the operators T^{nilp} with T^{ss} with the above properties are unique.

Week 7, HW Problem 6. *Prove Theorem 14.1.1.*

NB: the decomposition $T = T^{\text{ss}} + T^{\text{nilp}}$ as in the theorem is called the *Jordan decomposition* of T.

Week 7, HW Problem 7. *Let $T = T^{\text{ss}} + T^{\text{nilp}}$ be the Jordan decomposition. Show that:*

(a) *T^{ss} has the same eigenvalues as T, and the eigenspaces of T^{ss} are the same as the generalized eigenspaces of T.*

(b) *There exist polynomials $p^{\text{ss}}(t)$ and $p^{\text{nilp}}(t)$ such that*

$$T^{\text{ss}} = \phi(p^{\text{ss}}(t)) \text{ and } T^{\text{nilp}} = \phi(p^{\text{nilp}}(t)).$$

14.2. **Regular nilpotent elements.**

14.2.1. Let V be a finite-dimensional vector space, and $T : V \to V$ a nilpotent operator. We shall say that T is *regular* (or regular nilpotent) if V admits a basis $e_1, \ldots, e_n$ such that

$$T(e_i) = e_{i-1},\ 1 < i \le n \text{ and } T(e_1) = 0.$$

That is to say, T is the "left-shift" operator with respect to some basis.

14.2.2. We are going to prove:

Proposition 14.2.3. *Let $T : V \to V$ be as above. Set $n = \dim(V)$. The following conditions are equivalent:*

(1) *T is regular;*

(2) *There exists $v \in V$ so that the vectors $v, Tv, \ldots, T^{n-1}v$ are linearly independent,*

(3) *$T^{n-1} \neq 0$.*

(4) *For every $1 \le i \le n$, $\dim(\ker(T^i)) = i$.*

(5) *$\dim(\ker(T)) = 1$.*

Proof. The implication (1) ⇒ (5) follows from the shape of the matrix (i.e., rank-nullity). Let us show (2) ⇒ (1). Indeed, the sought-for basis is given by $e_i = T^{n-i}v$.

Let us show (3) ⇒ (2). Let $v \in V$ be such that $T^{n-1}v \neq 0$. Let $a_0, \ldots, a_{n-1}$ be such that

$$a_0 \cdot v + a_1 \cdot Tv + \cdots + a_{n-1} \cdot T^{n-1}v = 0.$$

Assume for the sake of contradiction that not all a_i are zero. Let i be the minimal index such that $a_i \neq 0$. On the one hand,

$$T^{n-i-1}(a_i \cdot T^i v + \cdots + a_{n-1} \cdot T^{n-1}v) = 0.$$

On the other hand, for $j > i$, $T^{n-i-1}(a_j \cdot T^j v) = 0$. Hence,

$$a_i \cdot T^{n-1}v = 0,$$

which is a contradiction.

The implication (4) ⇒ (3) is tautological (take $i = n-1$). Let us show that (5) implies (4). By [Problem 2(a), MT1] we have

$$\dim(\ker(T^i)) \geq i.$$

So it suffices to show that opposite inequality. We shall argue by induction on i — note that the case of $i = 1$ is the assumption of (5).

By rank-nullity, we know that $\dim(\mathrm{Im}(T^i)) = n - i$, and we need to show that $\dim(\mathrm{Im}(T^{i+1})) \geq n - i - 1$. Consider the map

$$\mathrm{Im}(T^i) \to \mathrm{Im}(T^{i+1})$$

given by applying T. This map is surjective, and its kernel identifies with

$$\ker(T) \cap \mathrm{Im}(T^i).$$

In particular, $\dim(\ker(T) \cap \mathrm{Im}(T^i)) \leq \dim(\ker(T)) = 1$. Hence,

$$\dim(\mathrm{Im}(T^{i+1})) \geq \dim(\mathrm{Im}(T^i)) - 1 = n - i - 1.$$

□

14.2.4. As a corollary, we obtain:

Corollary 14.2.5. *Let $T : V \to V$ be regular nilpotent. Then for $n = \dim(V)$, we have*

$$\ker(T^i) = \mathrm{Im}(T^{n-i}), \quad 1 \leq i \leq n-1.$$

Proof. The inclusion

$$\mathrm{Im}(T^{n-i}) \subset \ker(T^i)$$

follows from the fact that $T^n = 0$. Now Proposition 14.2.3(3) implies that both subspaces have the same dimension. □

14.3. **The Jordan canonical form.**

14.3.1. We are going to prove the following theorem:

Theorem 14.3.2. *Let $T : V \to V$ be a nilpotent operator. Then there exists a direct sum decomposition*

$$V \simeq \underset{i=1,\dots,k}{\oplus} V_i,$$

where each V_i is T-invariant and $T|_{V_i}$ is regular. Furthermore, the collection of integers

$$n_i := \dim(V_i)$$

is independent of the choice of the decomposition.

14.3.3. We emphasize that the direct sum decomposition as in the theorem is *not* canonical. I.e., the same (T, V) can admit several different decompositions of this shape.

Week 7, HW Problem 8. *Let $V = k^3$ and T be given by $T(e_1) = T(e_2) = 0$ and $T(e_3) = e_2$. Set $V_1 = \mathrm{Span}(e_1)$. Find two different T-invariant subspaces V_2' and V_2'' such that $T|_{V_1}, T|_{V_2'}$, and $T|_{V_2''}$ are all regular, and*

$$V_1 \oplus V_2' \simeq V \text{ and } V_1 \oplus V_2'' \simeq V.$$

14.4. **Partitions.** First, we are going to prove the uniqueness part of Theorem 14.3.2.

14.4.1. For a positive integer n, a partition $\mathfrak{p}$ of n is a decomposition

$$n = n_1 + \cdots + n_k,\ n_i \geq n_{i+1},\ n_i > 0.$$

To a partition $\mathfrak{p}$ we assign a dual partition, $\mathfrak{p}^\vee$,

$$n = n_1^\vee + \cdots + n_\ell^\vee,$$

determined by the formula

$$n_j^\vee = \#\left|\{i \,|\, j \leq n_i\}\right| = \sum_{i=1}^{k} \begin{cases} 1, & j \leq n_i \\ 0, & j > n_i, \end{cases}$$

where j ranges from 1 to $\ell := n_1$. Check that $\mathfrak{p}^\vee$ is actually a partition of n!

Note that $(\mathfrak{p}^\vee)^\vee = \mathfrak{p}$ (do you see why?). Hence the partition and its dual determine each other. Note also that a partition $\mathfrak{p}$ can be recovered from the data of the partial sums

$$n_1 + \cdots + n_i, \quad 1 \leq i \leq k.$$

Finally, note that

$$n_1^\vee + \cdots + n_j^\vee = \sum_{i=1}^{k} \begin{cases} j, & j \leq n_i \\ n_i, & j > n_i. \end{cases}$$

14.4.2. Given a decomposition

$$V \simeq \bigoplus_{i=1}^{k} V_i,$$

we may assume that the indices $i = 1, \dots, k$ are arranged so that $n_i := \dim(V_i)$ form a partition $\mathfrak{p}$ of n.

We will show that the dual partition $\mathfrak{p}^\vee$ is given by

$$n_j^\vee = \dim(\ker(T^j)) - \dim(\ker(T^{j-1})).$$

I.e., we will show that for every j

$$\dim(\ker(T^j)) = \sum_{i=1}^{k} \begin{cases} j, & j \leq n_i \\ n_i, & j > n_i. \end{cases}$$

Now note that

$$\dim(\ker(T^j)) = \sum_{i=1}^{k} \dim(\ker(T^j|_{V_i})).$$

Hence it certainly suffices to show that, for every i and j,

$$\dim(\ker(T^j|_{V_i})) = \begin{cases} j, & j \leq n_i \\ n_i, & j > n_i. \end{cases}$$

But this follows from Proposition 14.2.3.

Week 7, HW Problem 9. *Let $T : V \to V$ be a nilpotent operator. Without assuming the existence of the Jordan canonical form, show that*

$$n_j^\vee := \dim(\ker(T^j)) - \dim(\ker(T^{j-1}))$$

satisfy

$$n_j^\vee \geq n_{j+1}^\vee.$$

Suggested strategy: consider the vector spaces $\ker(T^j)/\ker(T^{j-1})$.

14.5. Existence of the Jordan canonical form.

14.5.1. We prove Theorem 14.3.2 by induction on the dimension of V. The case of $V = 0$ is evident. (Similarly for $\dim V = 1$!)

Let n be the minimal integer such that $T^n = 0$. Choose a vector $v \in V$ such that $T^{n-1}v \neq 0$. Let

$$V' := \text{Span}(v, Tv, \dots, T^{n-1}v), \quad T' := T|_{V'}.$$

By Proposition 14.2.3, T' is regular.

Set $V'' := V/V'$, $T'' := T|_{V''}$. By the induction hypothesis, we have that

$$V'' \simeq \bigoplus_{i} V_i'',$$

with each V_i'' T''-stable and $T_i'' := T''|_{V_i''}$ regular.

14.5.2. To prove the theorem, it suffices to find a map

$$j : V'' \to V$$

such that $\pi \circ j = \mathrm{id}$ (here π denotes the projection $V \to V''$) and such that

$$T \circ j = j \circ T''.$$

(Indeed, recall the splitting lemma!)

Let $V_i := \pi^{-1}(V_i'')$ and $T_i := T|_{V_i}$. Let π_i denote the corresponding map $V_i \to V_i''$. Certainly it suffices to show that, for every i, there exists a map $j_i : V_i'' \to V_i$ such that $\pi_i \circ j_i = \mathrm{id}$ and

$$T_i \circ j_i = j_i \circ T_i''.$$

Note that $\ker(\pi_i) = V'$. This reduces to the situation when both T' and T'' are regular, $T^n = 0$, and $(T')^{n-1} \neq 0$.

14.5.3. Let m be the minimal integer such that $(T'')^m = 0$. Note that since $T^n = 0$, we have $m \leq n$.

By Proposition 14.2.3, there exists a vector $v'' \in V''$ such that

$$v'', T''(v''), \ldots, (T'')^{m-1}(v'')$$

forms a basis for V''.

Suppose that we can find a vector $v \in V$ such that $\pi(v) = v''$ and such that $T^m v = 0$. Given such a vector, we may define the sought-for map j by

$$j((T'')^k(v'')) := T^k v, \quad k = 0, \ldots, m-1.$$

Certainly $\pi \circ j = \mathrm{id}$ (by construction!). We claim that $T \circ j = j \circ T''$. To see this, we simply need to check that, for each $k = 0, \ldots, m-1$,

$$(T \circ j \circ (T'')^k)v'' = (j \circ T'' \circ (T'')^k)v''.$$

For $k < m-1$, this is tautological (namely, both sides are equal to $T^{k+1}v$). For $k = m-1$, the right-hand side is 0, while the left-hand side is $T^m v$, which is 0 by assumption.

14.5.4. Thus, it remains to show that such a v exists. Choose any $w \in V$ such that $\pi(w) = v''$ (of course, such a w exists by surjectivity). Consider $w' := T^m w$.

We have that

$$\pi(w') = \pi(T^m w) = (T'')^m(\pi(w)) = 0.$$

Note that

$$(T')^{n-m} w' = T^n w = 0.$$

Thus, since T' is regular, by Corollary 14.2.5, there exists $u \in V'$ such that

$$w' = T^m u.$$

Of course this implies that $T^m(w - u) = w' - w' = 0$.

So take $v := w - u$. We claim that this guy satisfies the required properties. Indeed,

$$\pi(v) = \pi(w) = v'',$$

since $u \in V'$. But we also just saw that $T^m v = 0$.

□

14.5.5. *The centralizer of a nilpotent element.* Let $T : V \to V$ be a nilpotent operator. Consider the vector subspace $Z(T) \subset \mathrm{End}(V)$, defined by

$$S \in Z(T) \iff T \circ S = S \circ T.$$

The subspace is called *the centralizer* of T.

Week 7, HW Problem 10. *Show that* $\dim(Z(T)) \geq \dim(V)$*.*

Hint: use the Jordan canonical form.

14.6. Mini-project: general regular operators.

14.6.1. Let $T : V \to V$ be nilpotent.

Bonus Problem 3, 2pts.

(a) *Show that, if T is regular, then $Z(T)$ equals* $\mathrm{Span}(\mathrm{Id}, T, T^2, \ldots, T^n)$*; in particular* $\dim(Z(T)) = \dim(V)$*.*

(b) *Show that, if* $\dim(Z(T)) = \dim(V)$*, then T is regular.*

14.6.2. Let now $T : V \to V$ be an arbitrary operator.

Bonus Problem 3, 1pt. *Assume that* $\min_T$ *is a product of linear factors. Show that* $\dim(Z(T)) \geq \dim(V)$*.*

Bonus Problem 4, 1pt. *Deduce that* $\dim(Z(T)) \geq \dim(V)$ *holds without the assumption that* $\min_T$ *is a product of linear factors.*

Suggested strategy: translate the assertion of the problem into one about finding solutions of a system of linear equations and then move to an appropriate field extension (— just like in our proof of Cayley-Hamilton).

We shall say that $T \in \mathrm{End}(V)$ is *regular* if

$$\dim(Z(T)) = \dim(V).$$

14.6.3. Let $T : V \to V$ be such that $\min_T$ is a product of linear factors.

Theorem 14.6.4. *The following conditions are equivalent:*

(a) *T is regular.*

(b) *For every $\lambda \in \mathrm{Spec}(T)$, the operator $T - \lambda \cdot \mathrm{id}|_{V^{(\lambda)}}$ is regular nilpotent.*

(c) $\min_T = \mathrm{ch}_T$.

(d) *There exists $v \in V$ such that the elements $v, Tv, \ldots, T^{n-1}v$ span V.*

(e) *The subspace $Z(T) \subset \mathrm{End}(V)$ equals the image of the map $\phi : k[t] \to \mathrm{End}(V)$.*

Bonus Problem 5, 5pts. *Prove Theorem 14.6.4.*

Bonus Problem 6, 1pt. *Show that T is simultaneously regular and diagonalizable if and only if T has $\dim V$ distinct eigenvalues.*

Bonus Problem 7, 4pts. *Deduce the equivalence of (a), (c), (d) and (e) in Theorem 14.6.4 without the assumption that* $\min_T$ *is a product of linear factors.*

15. Tuesday, Oct. 23

15.1. **Vector spaces with an inner form.** We now specialize to the case of the ground field k being $\mathbb{R}$ or $\mathbb{C}$.

15.1.1. Let V be a vector space. An inner form on V is a map

$$(-,-) : V \times V \to k,$$

that satisfies the following:

- $(v_1' + v_1'', v_2) = (v_1', v_2) + (v_1'', v_2)$;
- $(v_1, v_2) = (v_2, v_1)$ (if $k = \mathbb{R}$) and $(v_1, v_2) = \overline{(v_2, v_1)}$ (if $k = \mathbb{C}$).
- $(v, v) \in \mathbb{R}^{\geq 0}$ and $(v, v) = 0$ if and only if $v = 0$.

Notation: over $\mathbb{R}$, $\bar{\lambda} := \lambda$.

For $v \in V$ we set

$$||v|| = \sqrt{(v, v)} \in \mathbb{R}^{\geq 0}.$$

15.1.2. Here are a few basic lemmas:

Lemma 15.1.3 (The Pythagorean Theorem)**.** *Suppose that $(v, w) = 0$. Then*

$$||v + w||^2 = ||v||^2 + ||w||^2.$$

Proof. Expand out $(v + w, v + w)$ by linearity. □

Lemma 15.1.4. *Let $0 \neq v$ and w be two vectors. Then there exist unique $a \in k$ and $u \in V$ such that*

$$w = a \cdot v + u, \quad (v, u) = 0.$$

Proof. Take $a = \frac{(w,v)}{(v,v)}$ and $u = w - \frac{(w,v)}{(v,v)} \cdot v$. □

Lemma 15.1.5 (Cauchy-Schwartz)**.** *For any $v, w \in V$,*

$$|(v, w)| \leq ||v|| \cdot ||w||,$$

with equality if and only if $w = a \cdot v$ for $a \in k$.

Proof. Of course we may take $v \neq 0$. Write $w = a \cdot v + u$ as in Lemma 15.1.4. We have: $|(v, w)| = |a| \cdot ||v||^2$, while by Lemma 15.1.3

$$||w|| \geq |a| \cdot ||v||,$$

with equality if and only if $w = a \cdot v$. This implies the desired inequality. □

Lemma 15.1.6 (Triangle inequality)**.** *For any $v, w \in V$, we have*

$$||v + w|| \leq ||v|| + ||w||,$$

with the equality if and only if $w = a \cdot v$, $a \in \mathbb{R}^{\geq 0}$.

Proof. We simply need to show that

$$(v + w, v + w) \leq (v, v) + (w, w) + 2 \cdot ||v|| \cdot ||w||$$

(with equality only in the specified case). This is equivalent to

$$(v, w) + (w, v) \leq 2 \cdot ||v|| \cdot ||w||,$$

with equality only in the specified case. We have

$$(v, w) + (w, v) = 2 \cdot \mathrm{Re}(v, w) \leq 2 \cdot |(v, w)|,$$

with equality if and only if $(v, w) \in \mathbb{R}^{\leq 0}$. Now apply Cauchy-Shwartz. □

15.2. **Inner product and the dual vector space.**

15.2.1. If $k = \mathbb{C}$, we let $\overline{V}$ the $\mathbb{C}$-vector space which is the same as V as an abelian group, but where the action of $\mathbb{C}$ is different:

For $v \in \overline{V}$ and $a \in \mathbb{C}$ we let $a \cdot v$ be "the old" $\overline{a} \cdot v$, i.e. the action of $\bar{a}$ on v in V.

Note that the assignment $W \mapsto \overline{W}$ establishes a bijection between vector subspaces of V and of $\overline{V}$.

Furthermore, if $e_1, \ldots, e_n$ is a basis of V, then the same vectors form a basis of $\overline{V}$. In particular, if V is finite-dimensional,

$$\dim(V) = \dim(\overline{V}).$$

Notation: When $k = \mathbb{R}$, we will also write $\overline{V}$, in which case it just means V.

15.2.2. Consider a map

$$\Phi : \overline{V} \to V^*, \quad v \mapsto \xi_v, \quad \xi(w) = (w, v).$$

It is easy to see that Φ is a linear map. (The only reason we've written down $\overline{V}$ is because the same definition as a map $V \to V^*$ is *not* linear!)

Proposition 15.2.3. *Let V be finite-dimensional. Then Φ is an isomorphism.*

Proof. Since the two vector spaces have the same dimension, it is enough to show that Φ is injective. I.e., it suffices to show that for $v \neq 0$, the element $\xi_v \neq 0$. However,

$$\xi_v(v) = (v, v) \neq 0.$$

□

Corollary 15.2.4. *For every $\xi \in V^*$ there exists a unique $v \in V$ such that*

$$\xi(-) = (-, v).$$

15.3. The orthogonal complement.

15.3.1. Let $W \subset V$ be a vector subspace. We define

$$W^\perp \subset V$$

by

$$v \in W^\perp \iff (v, w) = 0, \forall w \in W.$$

15.3.2. Consider the corresponding vector subspace

$$\overline{W^\perp} \subset \overline{V}.$$

We claim:

Lemma 15.3.3. *The vector subspace $\overline{W^\perp}$ equals the kernel of the map*

$$\overline{V} \overset{\Phi}{\to} V^* \to W^*,$$

where $V^* \to W^*$ is the map dual to the embedding $W \to V$.

Proof. Tautology. □

Corollary 15.3.4. *Assume that V is finite-dimensional. Then*

$$\dim(W^\perp) = \dim(V) - \dim(W).$$

Proof. We have $\dim(W^\perp) = \dim(\overline{W^\perp})$. Since the map $V^* \to W^*$ is surjective, and Φ is an isomorphism, we have

$$\dim(W^\perp) = \dim(\overline{V}) - \dim(W^*) = \dim(V) - \dim(W),$$

as required. □

Lemma 15.3.5. *Let V be finite-dimensional. $(W^\perp)^\perp = W$.*

Proof. The inclusion $W \subset (W^\perp)^\perp$ is tautological. This inclusion is an equality because the two vector spaces have the same dimension, by Corollary 15.3.4. □

15.3.6. We now claim:

Proposition 15.3.7. *Let V be finite-dimensional. Then the map*

$$W \oplus W^\perp \to V$$

is an isomorphism.

Proof. By Corollary 15.3.4, it is enough to show that the map in question is injective. I.e., that $W \cap W^\perp = 0$. If $w \in W \cap W^\perp$, we have $(w, w) = 0$, and hence $w = 0$. □

Thus, we obtain that every vector $v \in V$ can be uniquely decomposed as $w + u$, where $w \in W$ and $u \in W^\perp$.

Week 8, HW Problem 1. *Let $v = w + u$ be as above. Show that for all $w \neq w' \in W$, we have*

$$||v - w'|| > ||v - w||.$$

15.4. **Orthogonal collections.**

15.4.1. Let $\underline{v} := \{v_1, \ldots, v_n\}$ be a collection of non-zero elements of V. We shall say that $\underline{v}$ is an orthogonal collection if $(v_i, v_j) = 0$ for all $i \neq j$.

We shall say that $\underline{v}$ is *orthonormal* if it is orthogonal and $||v_i|| = 1$ for every i.

15.4.2. We have:

Lemma 15.4.3. *Let $\underline{v}$ be an orthogonal collection. Then it is linearly independent.*

Proof. Suppose that

$$a_1 \cdot v_1 + \cdots + a_n \cdot v_n = 0.$$

Then

$$(a_1 \cdot v_1 + \cdots + a_n \cdot v_n, v_i) = a_i \cdot (v_i, v_i) = 0,$$

which implies $a_i = 0$. □

Lemma 15.4.4. *Let $\underline{e}$ be an orthononormal collection. Then if*

$$v = a_1 \cdot v_1 + \ldots + a_n \cdot v_n,$$

we have

$$||v||^2 = |a_1|^2 + \cdots + |a_n|^2.$$

Proof. This follows from the Pythagorean theorem. □

15.4.5. *Gram-Schmidt.* Let $v_1, \ldots, v_n$ be a linearly independent collection. We have:

Proposition 15.4.6. *There exists a unique orthogonal collection $e_1, \ldots, e_n$ with the following properties:*

- *For every $1 \leq k \leq n$,* $\operatorname{Span}(e_1, \ldots, e_k) = \operatorname{Span}(v_1, \ldots, v_k)$*.*
- *For every $1 \leq k \leq n$, the images of v_k and e_k in*

$$\operatorname{Span}(e_1, \ldots, e_k)/\operatorname{Span}(e_1, \ldots, e_{k-1}) \simeq \operatorname{Span}(v_1, \ldots, v_k)/\operatorname{Span}(v_1, \ldots, v_{k-1})$$

coincide.

Proof. We proceed by induction on k, with $e_1 := v_1$. Suppose that $e_1, \ldots, e_k$ have been constructed. Set

$$W_k = \operatorname{Span}(e_1, \ldots, e_k) = \operatorname{Span}(v_1, \ldots, v_k).$$

Applying Proposition 15.3.7, we write

$$v_{k+1} = w + u,$$

where $w \in W_k$ and $u \in W_k^\perp$ are uniquely determined (since $v_{k+1} \neq 0$ by linear independence). By assumption, $v_{k+1} \notin W_k$, so $u \neq 0$. Set $e_{k+1} := u$.

□

Of course from this is it evident that we can produce an orthonormal collection by simply normalizing these e_i. Observe that this result also tells us that orthonormal bases exist in the first place!

16. Thursday, Oct 25

16.1. **Adjoint operators.**

16.1.1. Let $T : V_1 \to V_2$ be a linear operator, where both V_1 and V_2 are endowed with inner forms. For an element $v_2 \in V_2$ we define a linear functional

$$\xi_{T,v_2} : V_1 \to k$$

by setting

$$\xi_{T,v_2}(v_1) = (T(v_1), v_2).$$

By Corollary 15.2.4, there exists a unique element $w \in V_1$ such that

$$(v_1, w) = \xi_{T,v_2}(v_1).$$

Thus, the assignment

$$v_2 \mapsto w$$

defines a map of sets $V_2 \to V_1$. We denote this map by

$$T^{adj} : V_2 \to V_1.$$

Week 8, HW Problem 2. *Show that the following diagram commutes:*

$$\begin{tikzcd}
V_1^* & V_2^* \arrow[l, "T^*"'] \\
\overline{V_1} \arrow[u, "\Phi_1"] & \overline{V_2}. \arrow[l, "T^{adj}"] \arrow[u, "\Phi_2"']
\end{tikzcd}$$

Deduce that T^{adj} is a linear map.

We also have:

Lemma 16.1.2. *$(T^{adj})^{adj} = T$.*

Proof. Tautological. □

16.1.3. Here is an interpretation of the assignment $T \rightsquigarrow T^{adj}$ via matrices. Let $\underline{e}$ and $\underline{f}$ be *orthonormal* bases in V_1 and V_2, respectively.

Consider the matrices $M_{T,\underline{e},\underline{f}}$ and $M_{T^{adj},\underline{f},\underline{e}}$.

Week 8, HW Problem 3. *Show that the matrices $M_{T,\underline{e},\underline{f}}$ and $M_{T^{adj},\underline{f},\underline{e}}$ are related by*

$$M_{T^{adj},\underline{f},\underline{e}} = \overline{(M_{T,\underline{e},\underline{f}})^T}.$$

That is to say, one is the "conjugate transpose" of the other.

16.1.4. The following observation is useful:

Proposition 16.1.5.
(a) $(\mathrm{Im}(T))^{\perp} = \ker(T^{adj})$.
(b) $(\ker(T))^{\perp} = \mathrm{Im}(T^{adj})$.

Proof. First, note that by Lemmas 15.3.5 and 16.1.2, points (a) and (b) of the proposition are equivalent. Let us prove point (b). We have

$$\begin{aligned} v_2 \in (\mathrm{Im}(T))^{\perp} &\iff \forall v_2' \in \mathrm{Im}(T),\ (v_2', v_2) = 0 \\ &\iff \forall v_1 \in V_1,\ (T(v_1), v_2) = 0 \\ &\iff \forall v_1 \in V_1,\ (v_1, T^{adj}(v_2)) = 0 \\ &\iff T^{adj}(v_2) = 0 \\ &\iff v_2 \in \ker(T^{adj}). \end{aligned}$$

□

16.2. **Normal, self-adjoint and unitary/orthogonal operators.** Let $T : V \to V$, where V is endowed with an inner form. Consider the operator $T^{adj} : V \to V$.

Definition 16.2.1. *We shall say that T is* normal *if $T \circ T^{adj} = T^{adj} \circ T$.*

Definition 16.2.2. *We shall say that T is* self-adjoint *if $T = T^{adj}$.*

Evidently a self-adjoint operator is normal.

16.2.3.

Definition 16.2.4. *We shall say that T is* anti-self adjoint *if $T = -T^{adj}$.*

Evidently an anti-self adjoint operator is normal.

Week 8, HW Problem 4. *Show that any T can be uniquely written as a sum of a self-adjoint operator and an anti-self adjoint operator. Show also that T is normal if and only if its self-adjoint and anti-self adjoint parts commute with one another.*

16.2.5.

Definition 16.2.6. *We shall say that T is* unitary *(for $k=\mathbb{C}$) or* orthogonal *(for $k=\mathbb{R}$) if $T^{adj}=T^{-1}$ (in particular, T is invertible).*

Week 8, HW Problem 5. *Show that T is unitary/orthogonal if and only if for every $v,w\in V$ we have $(T(v),T(w))=(v,w)$, if and only if for every $v\in V$ we have $||T(v)||=||v||$.*

16.3. Diagonalization in the presence of an inner form.

16.3.1. Let $T:V\to V$ be as above.

Lemma 16.3.2. *The following conditions are equivalent:*

(a) *V admits an orthonormal basis consisting of T-eigenvectors.*

(b) *T is diagonalizable, and for $\lambda\neq\mu$, we have $V^\lambda\perp V^\mu$.*

Proof. The implication (b) ⇒ (a) is easy: choose orthonormal bases in each V^λ. The implication (a) ⇒ (b) follows from Proposition 9.3.8.

□

Definition 16.3.3. *We shall say that T is* diagonalizable in a way compatible with the inner form *if the equivalent conditions of Lemma 16.3.2 are satisfied.*

16.3.4. We shall now prove the following result:

Theorem 16.3.5. *Let V be a vector space over $\mathbb{C}$ endowed with an inner form, and $T:V\to V$ be an endomophism. Then the following conditions are equivalent:*

(a) *T is normal.*

(b) *T is diagonalizable in a way compatible with the inner form.*

Remark 16.3.6. *This theorem relies on the fact that the field $\mathbb{C}$ is algebraically closed.*

Proof. Assume (b). Write

$$V\simeq\underset{\lambda}{\oplus}V^\lambda,$$

where the V^λ are pairwise orthogonal, and $T|_{V^\lambda}=\lambda\cdot\mathrm{Id}_{V^\lambda}$.

Lemma 16.3.7. $T^{adj}|_{V^\lambda}=\overline{\lambda}\cdot\mathrm{Id}_{V^\lambda}$.

Note that Lemma 16.3.7 implies that T is normal.

Proof of Lemma 16.3.7. We need to show that for every $v\in V^\lambda$ and $w\in V$ we have

$$(w,T^{adj}(v))=(w,\overline{\lambda}\cdot v).$$

We rewrite the left-hand side as $(T(w),v)$ and the right-hand side as $\lambda\cdot(w,v)$.

It is enough to consider separately the following two cases: (1) $w\in V^\lambda$ and (2) $w\in V^\mu$, $\mu\neq\lambda$.

In case (1),

$$(T(w),v)=(\lambda\cdot w,v)=\lambda\cdot(w,v),$$

as required.

In case (2),

$$(T(w),v)=(\mu\cdot w,v)=\mu\cdot(w,v)=0,$$

while $\lambda \cdot (w, v)$ is also equal to 0.

□

Let us now assume (a). We shall argue by induction on $\dim(V)$, assuming that the assertion is true for vector spaces of smaller dimension.

Since $\mathbb{C}$ is algebraically closed, $\operatorname{Spec}(T) \neq \emptyset$. Hence, there exists $\lambda \in \mathbb{C}$ such that $V^\lambda \neq 0$. Consider the subspace $(V^\lambda)^\perp$.

Lemma 16.3.8. *The subspace $(V^\lambda)^\perp$ is T-invariant.*

Proof. By Proposition 16.1.5, we have $(V^\lambda)^\perp = \operatorname{Im}\left((T - \lambda \cdot \mathrm{Id})^{adj}\right)$. Note that

$$(T - \lambda \cdot \mathrm{Id})^{adj} = T^{adj} - \overline{\lambda} \cdot \mathrm{Id},$$

By normality T commutes with $T^{adj} - \overline{\lambda} \cdot \mathrm{Id}$. In particular, $\operatorname{Im}((T - \lambda \cdot \mathrm{Id})^{adj})$ is T-invariant.

□

By Proposition 15.3.7, the map

$$V^\lambda \oplus (V^\lambda)^\perp \to V$$

is an isomorphism. Thus, we obtain an orthogonal decomposition of V into a direct sum of two T-invariant subspaces.

Lemma 16.3.9. *If $V = V_1 \oplus V_2$, where $V_1 \perp V_2$ and V_1, V_2 are T-invariant, then they are also invariant with respect to T^{adj}. If T is normal, then so are $T|_{V_1}$ and $T|_{V_2}$.*

Proof. This follows from the definitions. □

Hence, we obtain that $T|_{(V^\lambda)^\perp}$ is normal. Applying the induction hypothesis, we obtain that $(V^\lambda)^\perp$ admits an orthonormal basis of T-eigenvectors. Concatenating with an arbitrary orthonormal basis of V^λ, we obtain the sought-for orthonormal basis of T-eigenvectors for V.

□

We continue working over $\mathbb{C}$.

Week 8, HW Problem 6. *Let T be normal. Show that it is self-adjoint if and only if all of its eigenvalues are real.*

Definition 16.3.10. *We shall say that T is* non-negative definite *if it is normal and for every $v \in V$, $(T(v), v)$ is a non-negative real number.*

Week 8, HW Problem 7. *Let T be normal. Show that it is non-negative definite if and only if all of its eigenvalues are non-negative real numbers.*

Week 8, HW Problem 8. *Let T be normal. Show that it is unitary if and only if all of its eigenvalues λ satisfy $|\lambda| = 1$.*

16.3.11. We will now prove:

Theorem 16.3.12. *Let V be a vector space over $\mathbb{R}$ endowed with an inner form, and $T : V \to V$ be an endomophism. Then the following conditions are equivalent:*

(a) *T is self-adjoint.*

(b) *T is diagonalizable in a way compatible with the inner form.*

Proof. The implication (b) $\Rightarrow$ (a) repeats the proof of the same impliaction in Theorem 16.3.5: note that the eigenvalues now are real, so $\overline{\lambda} = \lambda$ and we again use Lemma 16.3.7.

For the implication (a) $\Rightarrow$ (b) it suffices to show that $\text{Spec}(T) \neq \emptyset$ (the rest of the proof of Theorem 16.3.5 applies). We will give three different proofs. □

Proof 1. Let $\min_T \in \mathbb{R}[t]$ be a minimal polynomial of T. Let $p(t)$ be an irreducible factor of $\min_T$; in particular $p(T) \in \text{End}(V)$ is non-invertible.

Lemma 16.3.13. *Every monic irreducible polynomial over R is either of the form $t - a,\ a \in \mathbb{R}$, or of the form $(t + b)^2 + a,\ b \in \mathbb{R},\ a \in \mathbb{R}^{>0}$.*

The proof of the lemma is given below. Let us proceed with the proof of the theorem. If $p(t) = t - \lambda$, we obtain that $T - \lambda \cdot \text{Id}$ has a kernel, and we are done.

We claim that $p(t)$ cannot be of the form $(t + b)^2 + a,\ b \in \mathbb{R},\ a \in \mathbb{R}^{>0}$ if T is self-adjoint. Indeed, let

$$0 \neq v \in \ker\left((T + b \cdot \text{Id})^2 + a \cdot \text{Id}\right).$$

We have

$$0 = \left(\left((T + b \cdot \text{Id})^2 + a \cdot \text{Id}\right) v, v\right) = \left((T + b \cdot \text{Id})^2 v, v\right) + a \cdot (v, v).$$

Now, since T is self-adjoint, so is $T + b \cdot \text{Id}$, and hence

$$\left((T + b \cdot \text{Id})^2 v, v\right) = ((T + b \cdot \text{Id})v, (T + b \cdot \text{Id})v) \geq 0.$$

However, $a \cdot (v, v) > 0$, which is a contradiction. □

Proof of Lemma 16.3.13. Let λ be a root of $p(t)$ over $\mathbb{C}$. If $\lambda \in \mathbb{R}$, the polynomial $(t - \lambda)$ divides $p(t)$ by Bezout's theorem, and we are done.

Otherwise, since $p(t)$ has real coefficients, we obtain that $\overline{\lambda}$ is also a root of $p(t)$. Hence, $(t - \lambda) \cdot (t - \overline{\lambda})$ divides $p(t)$ *as a polynomial over* $\mathbb{C}$ (since the two factors are coprime, since $\lambda \neq \overline{\lambda}$). I.e.,

$$p(t) = (t - \lambda) \cdot (t - \overline{\lambda}) \cdot q(t), \quad q(t) \in \mathbb{C}[t].$$

Note, however that

$$(t - \lambda) \cdot (t - \overline{\lambda}) = t^2 - t \cdot (\lambda + \overline{\lambda}) + \lambda \cdot \overline{\lambda}$$

has real coefficients. From here it easily follows that $q(t)$ also has real coefficients. Hence

$$p(t) = (t - \lambda) \cdot (t - \overline{\lambda}),$$

by irreducibility.

Now, it is clear that irreducible quadratic polynomials over $\mathbb{R}$ have the specified form (they have no roots over $\mathbb{R}$, so look at the discriminant, and then complete the square).

□

Proof 2. We regard $V \simeq \mathbb{R}^n$ as a topological space (via a choice of basis), and define

$$S(V) = \{v \in V \, : \, ||v|| = 1\}.$$

This is a compact topological subspace of V. Define a function

$$f : S(V) \to \mathbb{R}$$

by

$$f(v) := (T(v), v).$$

This is a restriction of a continuous function from V (in fact it is quadratic in the coordinates of v once we have fixed a basis), so it is continuous. Let $v \in S(V)$ be a point at which $f(v)$ attains a maximum, which exists by compactness. We claim that v is an eigenvector of T. By Lemma 15.3.5, we need to show that

$$T(v) \in (\mathrm{Span(v)}^{\perp})^{\perp}.$$

I.e., if $(w, v) = 0$, then $(T(v), w) = 0$.

Let $g : \mathbb{R} \to S(V)$ be the map defined by

$$g(a) := \frac{v + a \cdot w}{||v + a \cdot w||}.$$

Of course this is definable in the first place since v and w are linearly independent (by orthogonality).

Consider the composition $h := f \circ g : \mathbb{R} \to \mathbb{R}$. Since f attains a maximum at $v \in S(V)$, we obtain that h attains a maximum at $0\,\mathbb{R}$.

We have:

$$\begin{aligned} h(a) &= \frac{(T(v + a \cdot w), v + a \cdot w)}{||v + a \cdot w||^2} \\ &= \frac{(T(v + a \cdot w), v + a \cdot w)}{(v + a \cdot w, v + a \cdot w)} \\ &= \frac{(T(v), v) + a^2 \cdot (T(w), w) + a \cdot ((T(v), w) + (T(w), v))}{(v, v) + a^2 \cdot (w, w) + a \cdot ((v, w) + (w, v))}. \end{aligned}$$

It is clear from the above expression that $h(a)$ is differentiable at $a = 0$. Since 0 is a global — hence local — maximum, the derivative of h at 0 must vanish. Let us compute this derivative.

Let's quickly simplify the expression for h using the facts that $(v, v) = (w, w) = 1$ (since they both lie on the unit sphere), $(v, w) = 0$ (by the assumption on w) and $(T(v), w) = (T(w), v)$ (since T is self-adjoint and we are working over the reals). Hence, we obtain:

$$h(a) = \frac{(T(v), v) + a^2 \cdot (T(w), w) + 2a \cdot (T(v), w)}{1 + a^2}.$$

We therefore see that $h'(a)|_{a=0} = 2 \cdot (T(v), w)$.

□

Week 8, HW Problem 9. *Adapt the above proof to the case when $k = \mathbb{C}$ to produce an alternative proof that a self-adjoint operator over $\mathbb{C}$ has a non-empty spectrum.*

Week 8, HW Problem 10. *Give yet another proof of the fact that, for a vector space V over $\mathbb{R}$ and a self-adjoint operator $T : V \to V$, the spectrum of T is non-empty, by deducing it from the complex case and [Problem 6, Week 8].*

Hint: use the strategy of the proof of Theorem 13.2.6.

16.4. **Mini-project: square roots of operators and factorizations.**

16.4.1. Let V be a vector space (over $\mathbb{R}$ or $\mathbb{C}$) with an inner form, and let $T : V \to V$ be a non-negative definite operator.

Write

$$V = \underset{\lambda}{\oplus} V^\lambda.$$

Recall [Problem 7, Week 8] that $\lambda \in \mathbb{R}^{\geq 0}$. Define

$$T^{1/2} : V \to V$$

by setting

$$T^{1/2}|_{V^\lambda} = \lambda^{1/2} \cdot \mathrm{Id}_{V^\lambda},$$

where $\lambda^{1/2} \in \mathbb{R}^{\geq 0}$.

Bonus Problem 8, 1pt. *Show that any operator that commutes with T commutes with $T^{1/2}$.*

Bonus Problem 9, 2pts. *Show that if S is a non-negative definite operator such that $S^2 = T$, then $S = T^{1/2}$.*

16.4.2. Let now $T : V \to V$ be an arbitrary operator. Note that

$$T \circ T^{adj}$$

is always non-negative definite.

Assume now that T is invertible.

Bonus Problem 10, 3pts. *Show that there is a unique way to write T as a product $T_1 \cdot T_2$, where T_1 is non-negative definite and T_2 is unitary/orthogonal. Show, moreover, that T is normal if and only if T_1 and T_2 commute.*

17. Tuesday, Oct. 30

17.1. **Products of groups.**

17.1.1. Let G_1 and G_2 be two groups. We are define their product $G_1 \times G_2$ to be the product of sets, and equip it with the unique group structure for which the the projections

$$p_i : G_1 \times G_2 \to G_i$$

are group homomorphisms. Concretely, $(g_1, g_2) \cdot (g_1', g_2') := (g_1 \cdot g_1', g_2 \cdot g_2')$.

17.1.2. The following assertion is proved in the same way as [Problem 1, Week 3]:

Lemma 17.1.3. *For a group G, the map*

$$\mathrm{Hom}(G, G_1 \times G_2) \to \mathrm{Hom}(G, G_1) \times \mathrm{Hom}(G, G_2)$$

that sends $\phi : G \to G_1 \times G_2$ to the pair (ϕ_1, ϕ_2), where $\phi_i = p_i \circ \phi$, is a bijection.

17.1.4. We now consider maps *out of* $G_1 \times G_2$. Let

$$i_1 : G_1 \to G_1 \times G_2 \text{ and } i_2 : G_2 \to G_1 \times G_2$$

be the maps

$$g_1 \mapsto (g_1, 1) \text{ and } g_2 \mapsto (1, g_2),$$

respectively.

For a group G, consider the map

$$\mathrm{Hom}(G_1 \times G_2, G) \to \mathrm{Hom}(G_1, G) \times \mathrm{Hom}(G_2, G), \quad \phi \mapsto (\phi \circ i_1, \phi \circ i_2). \tag{32}$$

The following is proved in a way similar to [Problem 2, Week 3]:

Lemma 17.1.5. *The map* (32) *is an injection. Its image consists of those elements*

$$(\phi_1, \phi_2) \in \mathrm{Hom}(G_1, G) \times \mathrm{Hom}(G_2, G)$$

for which

$$\forall\, g_1 \in G_1,\ \forall\, g_2 \in G_2 \text{ we have } \phi_1(g_1) \cdot \phi_2(g_2) = \phi_2(g_2) \cdot \phi_1(g_1).$$

Corollary 17.1.6. *If G is commutative, then the map* (32) *is an isomorphism.*

17.2. **Generation.**

17.2.1. Let G be a group, and let $g_\alpha \in G$ be elements where α runs over a set A.

Definition 17.2.2. *We say that $\{g_\alpha,\, \alpha \in A\}$ generate G if G does not contain a proper subgroup H such that $g_\alpha \in H$ for all $\alpha \in A$.*

Lemma 17.2.3. *The following conditions are equivalent:*

(a) *The elements $\{g_\alpha,\, \alpha \in A\}$ generate G.*

(b) *Every element of G can be written as a (finite) product*

$$g_{\alpha_1}^{\pm 1} \cdot \ldots \cdot g_{\alpha_n}^{\pm 1} \tag{33}$$

for some integer n and some map

$$\{1, \ldots, n\} \to A, \quad i \mapsto \alpha_i.$$

Proof. Suppose (b) holds. Let H be a subgroup of G that contains all the g_α. We want to show that $H = G$. Let g be an element of G. Write g as (33). Since all $g_{\alpha_i} \in H$ and H is a subgroup, we obtain that $g \in H$.

Suppose that (a) holds. Let $H \subset G$ be the set of elements of G that can be written as (33). It is easy to see that H is a subgroup. By construction, H contains all the g_α. The assumption in (a) says that $H = G$.

□

It is worth noting that within the proof we constructed the *subgroup generated by the g_α*, the minimal subgroup of G generated by the g_α.

Week 9, HW Problem 1. *Take $G = \mathbb{Z}/n\mathbb{Z}$ and consider the element $\overline{m}$ for a $m \in \mathbb{Z}^{\geq 1}$. Show the one element set $\{\overline{m}\}$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if m and n are coprime.*

17.3. **The order of an element.**

17.3.1. Let G be a (not necessarily finite) group, and let $g \in G$ be an element.

Definition 17.3.2.

(a) *We say that g is of finite order if there exists a positive integer n such that $g^n = 1$.*

(b) *If g is an element of finite order, its order, denoted* $\operatorname{ord}(g)$ *is the minimal positive integer n such that $g^n = 1$.*

By definition $\operatorname{ord}(g) = 1$ if and only if $g = 1$.

Lemma 17.3.3. *Let G be a group and $g \in G$ be an element of finite order. If for some positive integer n we have $g^n = 1$, then* $\operatorname{ord}(g) \,|\, n$.

Proof. Write $n = \operatorname{ord}(g) \cdot m + k$, where $k < \operatorname{ord}(g)$. If $k \neq 0$, we obtain

$$1 = g^n = g^{\operatorname{ord}(g) \cdot m + k} = (g^{\operatorname{ord}(g)})^m \cdot g^k = g^k,$$

which contradicts the minimality of $\operatorname{ord}(g)$. □

Proposition 17.3.4. *Let G be a group and $g \in G$ be an element of finite order. Let n be an integer.*

(a) $\operatorname{ord}(g) \,|\, n$ *if and only if there exists a homomorphism*

$$\phi : \mathbb{Z}/n\mathbb{Z} \to G$$

with $\phi(\overline{1}) = g$. If this happens, this homomorphism is unique.

(b) *The homomorphism ϕ in point* (a) *is injective if and only if* $\operatorname{ord}(g) = n$.

Proof. Do it yourself. □

Note that the image of such a homomorphism is the subgroup generated by g!

17.3.5. We also note:

Lemma 17.3.6. *An element g is of finite order if and only if g^{-1} is, and their orders are equal.*

Proof. For any n we have $(g^{-1})^n = (g^n)^{-1}$. □

Lemma 17.3.7. *Let g and h be two elements. Then g is of finite order if and only if $h \cdot g \cdot h^{-1}$ is, and their orders are equal.*

Proof. This follows from the fact that

$$g \mapsto h \cdot g \cdot h^{-1}, \quad G \to G$$

is an automorphism. □

17.3.8. Let g_1 and g_2 be two elements of G.

Lemma 17.3.9. *Suppose that $g_1 \cdot g_2 = g_2 \cdot g_1$. Then if g_1 is of (finite) order n_1 and g_2 is of (finite) order n_2, the element $g_1 \cdot g_2$ is of finite order and* $\operatorname{ord}(g_1 \cdot g_2)$ *divides $[n_1, n_2]$, the least common multiple of n_1 and n_2.*

Proof. By Lemma 17.3.3 we have to show that $(g_1 \cdot g_2)^{[n_1,n_2]} = 1$. However, the fact that $g_1 \cdot g_2 = g_2 \cdot g_1$ implies that

$$(g_1 \cdot g_2)^{[n_1,n_2]} = (g_1)^{[n_1,n_2]} \cdot (g_2)^{[n_1,n_2]},$$

and the assertion follows. □

Week 9, HW Problem 2. *Let n be the minimal positive integer such that $g^n = 1$ for all $g \in G$. Show that g is the least common multiple of* $\operatorname{ord}(g)$*, $g \in G$.*

17.4. **The order of a group.** From now, and until further notice, all groups will be assumed finite.

17.4.1. Let G be a (finite) group. Its order, denoted $|G|$, is its cardinality as a set. We will sometimes write $\#|G|$ for this size as well, if only to clear up notation.

Here is a basic result about group orders:

Proposition 17.4.2. *Let G be a group and $H \subset G$ a subgroup. Then*

$$|G| = |H| \cdot |G/H|.$$

Proof. Consider the map

$$\pi : G \to G/H.$$

It is enough to show that the preimage of every element $x \in G/H$ is of cardinality $|H|$. Each such preimage is a right coset of G with respect to H (see Sect. 2.3). I.e., if $x = \overline{g} = \pi(g)$, the corresponding coset is

$$g \cdot h, \quad h \in H.$$

It is manifestly in bijection with H. □

Corollary 17.4.3 (Lagrange's theorem)**.** *If H is a subgroup of G, we have $|H| \mid |G|$.*

17.4.4. We have:

Proposition 17.4.5. *Every element in a finite group is of finite order, and its order divides the order of the group.*

Proof. Consider the elements

$$1, g, g^2, \ldots.$$

These cannot all be distinct. Hence, there exist integers $n > m$ such that $g^m = g^n$. In this case $g^{n-m} = 1$, so g is of finite order.

Let $k = \operatorname{ord}(g)$. By Proposition 17.3.4, G contains a subgroup isomorphic to $\mathbb{Z}/k\mathbb{Z}$. By Corollary 17.4.3 we obtain that $k \mid |G|$.

□

See if you can do the following yourself:

Corollary 17.4.6 (Fermat's little theorem)**.** *Let p a prime and $n \in \mathbb{Z}$ not divisible by p. Then p divides $n^{p-1} - 1$.*

17.4.7. We define:

Definition 17.4.8. *Let p be a prime. We shall say that G is a p-group if $|G| = p^n$ for some n.*

Corollary 17.4.9. *Every element in a p-group is of order equal to a power of p.*

17.5. **Structure of finite abelian groups.** For abelian groups, we will write $A_1 \oplus A_2$ instead of $A_1 \times A_2$. We will use the symbol "+" for the group law.

17.5.1. Let A be a finite abelian group. We will prove the following theorems:

Theorem 17.5.2. *Let p be a prime.*

(a) *There exists a unique decomposition $A = A^{(p)} \oplus A^{(non\text{-}p)}$, such that every element of $A^{(p)}$ is of order equal to a power of p, and every element of $A^{(non\text{-}p)}$ is of order co-prime to p.*

(b) *For any subgroup $A' \subset A$, we have*

$$(A')^{(p)} = A' \cap A^{(p)} \text{ and } (A')^{(non\text{-}p)} = A' \cap A^{(non\text{-}p)}.$$

(c) *Every element of A of order equal to a power of p belongs to $A^{(p)}$, and every element of order co-prime to p belongs to $A^{(non\text{-}p)}$.*

Theorem 17.5.3.

(a) *There exists a unique decomposition*

$$A \simeq \underset{p}{\oplus} A^{(p)},$$

where each $A^{(p)}$ is as in Theorem 17.5.2.

(b) *Every element of A of order equal to a power of p belongs to $A^{(p)}$.*

Theorem 17.5.4. *Let A be an abelian p-group. There exists a (non-unique) decomposition*

$$A \simeq \underset{i}{\oplus} \mathbb{Z}/p^{n_i}\mathbb{Z}.$$

The collection of numbers n_i that appear only depends on A.

17.5.5. Here is a table of analogies between finite abelian groups and pairs $(V, T : V \to V)$ (over an algebraically closed field):

- $\mathrm{Spec}(T)$ corresponds to those primes for which $A^{(p)} \neq 0$.
- $\dim(V)$ corresponds to the integer $lg(A) := \underset{i}{\Sigma}\, n_i$, where $|A| = \underset{i}{\Pi}\, p_i^{n_i}$.
- If $T - \lambda \cdot \mathrm{Id}$ is regular nilpotent, this corresponds to A being isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$.
- If T is diagonalizable, this corresponds to A being isomorphic to $\underset{p}{\oplus} \mathbb{Z}/p\mathbb{Z}$.
- $\mathrm{ch}_T \in k[t]$ corresponds to $|A| \in \mathbb{Z}$.
- $\min_T \in k[t]$ corresponds to the minimal integer n such that $a^n = 0$ for any $a \in A$.

18. Thursday, Nov. 1

In this section all groups will be abelian and finite, unless explicitly specified otherwise.

18.1. **Orders of groups and elements.** We will use the additive notation. In particular for $n \in \mathbb{Z}$ and $a \in A$ we will write $n \cdot a$ rather than a^n. This is justified by [Problem 7, Week 2].

18.1.1. We claim:

Lemma 18.1.2. *Let A be a finite abelian group, and p a prime. The following are equivalent:*

(a) *The order of every $a \in A$ is a power of p.*

(b) *The endomorphism of A given by $a \mapsto p \cdot a$ is nilpotent (vanishes to some power).*

Proof. The implication (b) ⇒ (a) follows from Lemma 17.3.3. The implication (a) ⇒ (b) follows from [Problem 2, Week 9]. □

18.1.3. We also claim:

Lemma 18.1.4. *Let A be a finite abelian group, and p a prime. The following are equivalent:*

(a) *The order of every $a \in A$ is prime to p.*

(b) *The endomorphism of A given by $a \mapsto p \cdot a$ is invertible.*

Proof. Assume (b). Let, for contradiction, $a \in A$ be an element whose order is not prime to p. I.e., $\mathrm{ord}(a) = p \cdot n$. Consider the element $a' = n \cdot a$. We have $a' \neq 0$, since otherwise $\mathrm{ord}(a)$ would be $\leq n$. Now, $p \cdot a' = 0$, contradiction.

Assume (a). Since the set A is finite, it is enough to show that the map $a \mapsto p \cdot a$ is injective. Since the map in question is a group homomorphism, it is enough to show that its kernel is zero. However, $p \cdot a = 0$ implies $\mathrm{ord}(a) \,|\, p$. Hence $\mathrm{ord}(a) = 1$, i.e., $a = 0$.

□

18.1.5. We now claim:

Proposition 18.1.6. *Let A be a finite abelian group. Then $|A|$ divides $\prod\limits_a \mathrm{ord}(a)$.*

Proof. For an element $a \in A$, let

$$\phi_a : \mathbb{Z}/\mathrm{ord}(a)\mathbb{Z} \to A$$

be the homomorphism of Propisition 17.3.4. The resulting map

$$\underset{a \in A}{\oplus} \mathbb{Z}/\mathrm{ord}(a)\mathbb{Z} \to A$$

is surjective. I.e., A is isomorphic to a quotient group of $\underset{a \in A}{\oplus} \mathbb{Z}/\mathrm{ord}(a)\mathbb{Z}$. Hence, by Proposition 17.4.2, $|A|$ divides

$$\left| \bigoplus_{a \in A} \mathbb{Z}/\mathrm{ord}(a)\mathbb{Z} \right| = \prod_{a \in A} |\mathbb{Z}/\mathrm{ord}(a)\mathbb{Z}| = \prod_{a \in A} \mathrm{ord}(a).$$

□

Corollary 18.1.7. *Let A be a finite abelian group, and p a prime. The following are equivalent:*

(a) *A satisfies the equivalent conditions of Lemma 18.1.2.*

(b) *A is a p-group, i.e., $|A|$ is a power of p.*

Proof. The implication (b) $\Rightarrow$ (a) follows from Corollary 17.4.9. The converse implication follows from Proposition 18.1.6.

□

Corollary 18.1.8. *Let A be a finite abelian group, and p a prime. The following are equivalent:*

(a) *A satisfies the equivalent conditions of Lemma 18.1.4.*

(b) *A is a "non-p-group", i.e., $|A|$ is prime to p.*

Proof. The implication (b) $\Rightarrow$ (a) follows from Proposition 17.4.5. The converse implication follows from Proposition 18.1.6. □

18.2. **Proof of Theorem 17.5.2.** The proof will mimic the proof of Theorem 11.1.4.

18.2.1. For a finite abelian group, we denote by $lg(A)$ the integer $n_1 + \cdots + n_k$, where

$$|A| = \prod_i p_i^{n_i}, \quad p_i \text{ are prime.}$$

Week 9, HW Problem 3. *Let*

$$0 \to A_1 \to A \to A_2 \to 0$$

be a short exact sequence of finite abelian groups. Show that $lg(A) = lg(A_1) + lg(A_2)$.

18.2.2. For any integer n, we denote by $A[n]$ the kernel of multiplication by n, i.e.,

$$A[n] := \{a \in A \,|\, n \cdot a = 0\}.$$

Terminology: We call $A[n]$ the subgroup of *n-torsion elements* in A.

We have the following analogue of Theorem 8.4.2:

Proposition 18.2.3. *Let A be a finite abelian group, and p a prime. For any $N \geq lg(A)$, the inclusion*

$$A[p^{lg(A)}] \to A[p^N]$$

is an equality.

We shall denote by $n \cdot A$ the image of multiplication by n on A.

Corollary 18.2.4. *Let A be a finite abelian group, and p a prime. For any $N \geq lg(A)$,*

$$p^N \cdot A \subset p^{lg(A)} \cdot A$$

is an equality.

Week 9, HW Problem 4. *Prove Proposition 18.2.3 and Corollary 18.2.4.*

18.2.5. Denote:

$$A[p^\infty] := A[p^N] \text{ for any } N \geq lg(A),$$
$$p^\infty \cdot A := p^N \cdot A \text{ for any } N \geq lg(A).$$

We have the following analog of Theorem 8.6.8:

Proposition 18.2.6. *Let A be a finite abelian group, and p a prime.*

(a) *The canonical map*

$$A[p^\infty] \oplus p^\infty A \to A$$

is an isomorphism.

(b) *For any subgroup $A' \subset A$, we have*

$$A'[p^\infty] = A' \cap (A[p^\infty]) \text{ and } p^\infty \cdot A' = A' \cap (p^\infty \cdot A).$$

Week 9, HW Problem 5. *Prove Proposition 18.2.6.*

Week 9, HW Problem 6. *Prove Theorem 17.5.2.*

Week 9, HW Problem 7. *Prove Theorem 17.5.3.*

19. Midterm Exam. Due: Saturday, Nov. 3 at 6pm, by email

Probem 1. 5pts Let G_1 and G_2 be two groups (not necessarily finite), and let $g_i \in G_i$ be elements. Show that the element $(g_1, g_2) \in G_1 \times G_2$ is of finite order if and only if g_1 amd g_2 are, and that in this case

$$\text{ord}(g_1, g_2) = lcm(\text{ord}(g_1), \text{ord}(g_2)).$$

Probem 2. 5pts. Let A be a finite abelian group.

(a) 3pts. Suppose that $|A| = p^n$, where p is a prime. Show that the following are equivalent:

(i) $A \simeq \mathbb{Z}/p^n\mathbb{Z}$.

(ii) There exists $a \in A$ such that $\{a\}$ generates A.

(iii) Multiplication by p^{n-1} on A is non-zero.

(iv) For every $1 \leq i \leq n$ we have $lg(A[p^i]) = i$.

(v) $\#|A[p]| = p$.

(b) 2pts. Write A as $\underset{p}{\oplus} A^{(p)}$, see Theorem 17.5.3. Show that the following are equivalent:

(i) $A \simeq \mathbb{Z}/n\mathbb{Z}$ for some n.

(ii) There exists $a \in A$ that generates it.

(iii) Each $A^{(p)}$ is as in point (a).

Probem 3. 5pts. Let A be a finite abelian group. Write

$$A \simeq \underset{p}{\oplus} A^{(p)},$$

see Theorem 17.5.3. Show that for every prime p there exists an integer n_p such that:

(i) $n_p \cdot a = a$ for $a \in A^{(p)}$.

(ii) $n_p \cdot a = 0$ for $a \in A^{(p')}$, $p' \neq p$.

20. Tuesday, Nov. 6

20.1. Leftover problem on finite abelian groups.

Week 10, HW Problem 1. *Prove Theorem 17.5.4.*

20.2. Group actions on sets.

20.2.1. Let G be a group. An action of G on a set X is a map

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

that satisfies:

- For any $x \in X$, we have $1 \cdot x = x$;
- For any $g_1, g_2 \in X$ and $x \in X$ we have $g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x$.

Terminology: If G acts on X we shall also say that X is a G-set.

We have:

Lemma 20.2.2. *Let X be a G-set. Then for any $g \in G$ the map $x \mapsto g \cdot x$ is an automorphism of X.*

Proof. The inverse map is given by $x \mapsto g^{-1} \cdot x$. □

20.2.3. Let X_1 and X_2 be two G-sets. A map of G-sets from X_1 to X_2 is a map of sets $\phi : X_1 \to X_2$ that makes the diagram

$$\begin{tikzcd}
G \times X_1 \arrow[r] \arrow[d, "\mathrm{id}_G \times \phi"'] & X_1 \arrow[d, "\phi"] \\
G \times X_2 \arrow[r] & X_2
\end{tikzcd}$$

commute.

In other words, for every $x_1 \in X_1$ and $g \in G$, we have

$$g \cdot \phi(x_1) = \phi(g \cdot x_1).$$

We denote the set of maps G-sets from X_1 to X_2 by $\mathrm{Hom}_G(X_1, X_2)$.

Lemma 20.2.4. *Let ϕ be a map of G sets which is bijective at the level of the underlying sets. Then its inverse is also a map of G-sets.*

Proof. Same as [Problem 2, Week 1]. □

20.2.5. If G acts on X, we define

$$X^G = \{x \in X \mid \forall g \in G,\, g \cdot x = x\}.$$

We call X^G the set of G-invariants.

20.2.6. *Examples.*

(i) For any group G, the one-element set $\{*\} =: \mathrm{pt}$ carries a unique G-action.

For any G-set X consider the map

$$\mathrm{Hom}_G(\{*\}, X) \to X$$

that sends $\phi : \{*\} \to X$ to $\phi(*) \in X$.

Week 10, HW Problem 2. *Show that the image of the above map is contained in X^G, and that the resulting map*

$$\mathrm{Hom}_G(\{*\}, X) \to X^G$$

is a bijection.

(ii) For any group G, the set $X = G$ carries a canonical G-action given by *left multiplication*. We call this G-set the *left-regular G-action*.

For any G-set consider the map

$$\mathrm{Hom}_G(G, X) \to X$$

that sends $\phi \in \mathrm{Hom}_G(G, X)$ to the element $\phi(1) \in X$.

Week 10, HW Problem 3. *Show that the above map is a bijection.*

(iii) For any group G, the set $X = G$ carries a canonical G-action given by *right multiplication by the inverse element*

$$g \underset{\mathrm{act}}{\cdot} g' = g' \cdot g^{-1}.$$

We call this G-set the *right-regular G-action*.

(iv) Combining Examples (ii) and (iii) we have an action of the group $G \times G$ on the set $X = G$ by

$$(g_1, g_2) \underset{\mathrm{act}}{\cdot} g' = g_1 \cdot g' \cdot g_2^{-1}.$$

(v) If G acts on X and $\phi : H \to G$ is a group homomorphism, we obtain an H action on X by composition.

(vi) We define the *adjoint* action of G on itself by

$$g \underset{\mathrm{act}}{\cdot} g' = g \cdot g' \cdot g^{-1}.$$

Week 10, HW Problem 4. *Show that the adjoint action is obtained from Examples (iv) and (v) via the diagonal homomorphism $G \to G \times G$. Show that the corresponding subset G^G of G-invariants under the adjoint action on G equals the* center $Z(G) \subset G$*, i.e., the set of all those elements of G that commute with every element of G.*

(vii) Let X be a set. Consider the group $G := \mathrm{Aut}_{\mathrm{Sets}}(X)$. We obtain a tautological action of G on x by

$$g \cdot x := g(x).$$

(viii) In the previous example, set $X := \{1, \ldots, n\}$. We define the symmetric group S_n to be $\mathrm{Aut}_{\mathrm{Sets}}(\{1, \ldots, n\})$. Thus, we obtain the tautological S_n-action on $\{1, \ldots, n\}$.

(ix) Let V be a vector space over a field k. We define the group $\mathrm{GL}(V)$ to be that of all k-linear automorphisms of V. We have a tautological action of $\mathrm{GL}(V)$ on V.

In fact, this is a combination of Examples (v) and (vii) since $\mathrm{GL}(V)$ is a subgroup of $\mathrm{Aut}_{\mathrm{Sets}}(V)$.

(x) Let V be a complex vector space with an inner form. We define $\mathrm{U}(V)$ to be a subgroup of $\mathrm{GL}(V)$ consisting of those $T : V \to V$ for which $(T(v_1), T(v_2)) = (v_1, v_2)$. We call $\mathrm{U}(V)$ the *unitary* group of V. From examples (v) and (ix) we obtain an action of $\mathrm{U}(V)$ on V.

The same works for real vector spaces; the corresponding subgroup of $\mathrm{GL}(V)$ is denoted $\mathrm{O}(V)$ and is called the *orthogonal group of* V.

(xi) Let V be a finite-dimensional vector space. Let $\mathrm{Fl}(V)$ be the set of *complete flags* in V, i.e., an element of $\mathrm{Fl}(V)$ is a sequence of vector subspaces

$$0 = V_0 \subset V_1 \subset \dots V_{n-1} \subset V_n = V, \quad \dim(V_i) = i.$$

Any k-linear automorphism T of V defines a map $\mathrm{Fl}(V) \to \mathrm{Fl}(V)$, by sending a flag as above to the flag of V defined by

$$V_i' := T(V_i).$$

It is easy to see that in this way we obtain an action of $\mathrm{GL}(V)$ on $\mathrm{Fl}(V)$.

20.3. Action on sets of cosets.

20.3.1. Let G be a group, and $H \subset G$ a subgroup. Recall that we introduced the set G/H of *right cosets* of G with respect to H. It was characterized by the property that we have a surjective map

$$\pi : G \to G/H$$

such that $\pi(g_1) = \pi(g_2)$ if and only if $g_1 = g_2 \cdot h$ with $h \in H$.

20.3.2. We now claim:

Proposition 20.3.3. *There exists a uniquely defined action of G on G/H such that π is a map of G-sets, where G acts on G by the left regular action.*

Week 10, HW Problem 5. *Deduce Proposition 20.3.3 from Proposition 2.2.13.*

20.3.4. Let H be a subgroup G. For a G-set X consider the map

$$\mathrm{Hom}_G(G/H, X) \to X \tag{34}$$

that sends $\phi : G/H \to X$ to the element $\phi(\overline{1})$.

Proposition 20.3.5. *The image of the map* (34) *belongs to the subset X^H, and the resulting map*

$$\mathrm{Hom}_G(G/H, X) \to X^H$$

is bijective. The inverse map sends $x \in X^H$ to the map ϕ uniquely characterized by the property that

$$\phi \circ \pi(g) = g \cdot x.$$

Week 10, HW Problem 6. *Prove Proposition 20.3.5.*

20.4. Stabilizers.

20.4.1. Let G act on X. For $x \in X$ we set

$$\mathrm{Stab}_G(x) := \{g \in G \,|\, g \cdot x = x\}.$$

Week 10, HW Problem 7. *Consider the adjoint action of G on itself. Show that the stablizer of $g' \in G$ is its centralizer, i.e. the set $\{g \in G \,|\, g \cdot g' = g' \cdot g\}$.*

Week 10, HW Problem 8.

(a) *Consider the canonical S_n-action on $\{1, \ldots, n\}$. Construct an isomorphism*

$$\mathrm{Stab}_{S_n}(n) \simeq S_{n-1}.$$

(b) *Let V be a finite-dimensional complex vector space with an inner form. Consider the canonical $\mathrm{U}(V)$-action on V. Let $v \in V$ be a non-zero vector. Construct an isomorphism between $\mathrm{Stab}_{\mathrm{U}(V)}(v)$ and $\mathrm{U}(W)$, where $W = (\mathbb{C} \cdot v)^\perp \subset V$.*

20.4.2. Recall the setting of Proposition 20.3.5. Let X be a set with a G-action, and let $x \in X$ be an element. Let $H \subset G$ be a subgroup. From Proposition 20.3.5 we obtain that if $H \subset \mathrm{Stab}_G(x)$, then there exists a unique map

$$\phi : G/H \to X$$

such that $\phi(\overline{1}) = x$.

Week 10, HW Problem 9. *Show that the map ϕ is injective if and only if the inclusion $H \subset \mathrm{Stab}_G(x)$ is an equality.*

20.5. **Transitivity.**

20.5.1. We shall say that the action of G on X is:

- *transitive* if for every $x_1, x_2 \in X$ there exists $g \in G$ such that $g \cdot x_1 = x_2$.
- *simple* if for every $x \in X$, we have $\mathrm{Stab}_G(x) = \{1\}$.
- *simply transitive* if it is both simple and transitive.

Week 10, HW Problem 10. *Which of the actions in Section 20.2.6 are transitive?*

These rather unfamiliar words take a good deal of time to get used to, perhaps because they are not so great descriptors of the formal properties they encode. Intuitively, a transitive action allows one to move from any given point to any other point with a group element — to make the "transit" from one to the other, so to speak. Perhaps simplicity refers to the fact that the action does not factor through a nontrivial quotient of the group. Soon you will see that the quotients of G are the only examples of sets with transitive actions (on choosing a "basepoint"), and the sets with simple actions of G are precisely disjoint unions of copies of G (on again choosing a basepoint in each!).

20.5.2. The above discussion suggests the following more precise claim:

Proposition 20.5.3. *Let G acts transitively on X, and let $x \in X$ be a point. Then there exists a unique isomorphism of G sets*

$$\phi : G/\operatorname{Stab}_G(x) \to X$$

such that $\phi(\overline{1}) = x$.

Proof. The existence and uniqueness of the map

$$\phi : G/\operatorname{Stab}_G(x) \to X$$

such that $\phi(\overline{1}) = x$ follows from 20.3.5. It is injective by Problem 9. It is surjective by Lemma 20.5.4 below. Hence, it is an isomorphism by Lemma 20.2.4. □

Lemma 20.5.4. *Let $\phi : X_1 \to X_2$ be a map of G-sets with $X_1 \neq \emptyset$ and the G-action on X_2 transitive. Then ϕ is surjective.*

Proof. We need to show that for any $x_2 \in X_2$ there exists $x_1 \in X_1$ such that $\phi(x_1) = x_2$. Let x_1' be any point of X_1. By transitivity, there exists $g \in G$ such that $g \cdot \phi(x_1') = x_2$. The sought-for x_1 is then just $g \cdot x_1'$. □

21. Thursday, Nov. 8

21.1. **Groups acting on sets, continued.**

21.1.1. Let G act on X. We define an equivalence relation $\sim$ on X by declaring that $x_1 \sim x_2$ if there exists $g \in G$ such that $g \cdot x_1 = x_2$. It is easy to see that this is indeed an equivalence relation.

Equivalence classes with respect to this equivalence relation are called *orbits.*

In other words, an obit of a G-action on X is a non-empty G-subset $\mathbf{O} \subset X$, such that the action of G on $\mathbf{O}$ is transitive.

It is clear that X is the disjoint union of its orbits.

21.1.2. Assume now that both G and X are finite sets. For each orbit $\mathbf{O}$ choose a point $x_{\mathbf{O}} \in \mathbf{O}$. We have:

Proposition 21.1.3.

$$|X| = \sum_{\mathbf{O}} \frac{|G|}{|\operatorname{Stab}_G(x_{\mathbf{O}})|}.$$

Proof. Clearly,

$$|X| = \textstyle\sum_{\mathbf{O}} |\mathbf{O}|.$$

For each orbit, by Proposition 20.5.3,

$$\mathbf{O} \simeq G/\operatorname{Stab}_G(x_{\mathbf{O}}).$$

Hence, we are done by Proposition 17.4.2.

□

21.1.4. Proposition 21.1.3 has the following remarkable corollary:

Corollary 21.1.5. *Let G be a p-group, and assume that $|X|$ is prime to p. Then $X^G \neq \emptyset$.*

Proof. We argue by contradiction. Assume that $X^G = \emptyset$. Then for each G-orbit $\mathbf{O} \subset X$ we have $|\mathbf{O}| > 1$. Since

$$|\mathbf{O}| = \frac{|G|}{|\operatorname{Stab}_G(x_{\mathbf{O}})|},$$

and since $|G|$ is a power of p, we obtain that $|\mathbf{O}|$ is divisible by p. Hence,

$$\sum_{\mathbf{O}} |\mathbf{O}|$$

is also divisible by p. Contradiction. □

21.1.6. Let us give some applications of Corollary 21.1.5.

Proposition 21.1.7. *Let G be a p-group. Then its center is non-trivial, i.e., $Z(G) \neq \{1\}$.*

Recall that the center of a group is the subset of those elements that commute with all other elements, i.e.,

$$Z(G) = \{g \in G \,|\, g \cdot g_1 = g_1 \cdot g, \ \forall g_1 \in G\}.$$

Proof. Consider the adjoint action of G on itself, see Example (vi) of Section 20.2.6. Note that $G^G = Z(G)$.

Set $X := G - \{1\}$. We need to show that $X^G \neq \emptyset$. However, this follows from the fact that $|X| = |G| - 1$ isn't divisible by p. □

Proposition 21.1.8. *Let G be a group of order p^2. Then G is commutative.*

Proof. We argue by contradiction. Suppose G isn't commutative, i.e., $Z(G) \neq G$. By Proposition 21.1.7, $1 < |Z(G)| < p^2$. Hence, $|Z(G)| = p$.

Choose an element $g \notin Z(G)$. Consider the subgroup

$$Z_G(g) := \{g_1 \in G \,|\, g_1 \cdot g = g \cdot g_1\}.$$

We have

$$Z(G) \subset Z_G(g),$$

while $Z_G(g) \neq G$. Hence, $|Z_G(g)| = p$. Hence $Z(G) = Z_G(g)$. However, $g \in Z_G(g)$. Contradiction.

□

A remark: the above theorem is sharp! For example, consider the following group of order 8: $\{\pm 1, \pm i, \pm j, \pm k\}$ (called the "quaternion group"), with $i^2 = j^2 = k^2 = ijk = -1$. Note that $ij = -ji \neq ji$, so the group is noncommutative. As another example, consider the group of symmetries of a regular n-gon in the plane, called D_{2n} (the "dihedral group" of order $2n$). It is generated by the clockwise rotation by $\frac{2\pi}{n}$ and reflection across e.g. the x-axis. Note that rotation and reflection do *not* commute! It also turns out that $|D_{2n}| = 2n$, whence taking $n = 4$ we find another noncommutative group of order 8. See if you can show that these are nonisomorphic! We will see that doing representation theory too naively will fail to tell these two groups apart, but that's for (much) later.

21.2. **Sylow's theorem.**

21.2.1. Let G be of finite group, and let p be a prime. Write $|G| = p^n \cdot m$, where m is prime to p.

Theorem 21.2.2.

(a) *There exists a subgroup $G_p \subset G$ of order p^n.*

(b) *If $H \subset G$ is a p-group, there exists an element $g \in G$ such that $g \cdot H \cdot g^{-1} \subset G_p$.*

The rest of this subsection is devoted to the proof of Theorem 21.2.2.

21.2.3. *Proof of point (b).* Let us assume point (a), i.e., the existence of G_p, and prove point (b). Consider $X := G/G_p$, with H acting by left multiplication: $h(gG_p) := (hg)G_p$. By assumption $|X|$ is prime to p. Since H is a p-group, by Corollary 21.1.5, we have $X^H \neq \emptyset$.

The assertion of the theorem follows now from the following general lemma:

Lemma 21.2.4. *Let G be a group and $H \subset G \supset G'$ two subgroups. Consider the action of H on G/G' via left multiplication and let $g \in G$ be such that $\overline{g} = \pi(g) \in G/G'$ is H-invariant. Then $g^{-1} \cdot H \cdot g \subset G'$.*

Proof. We need to show that for all $h \in H$ we have

$$g^{-1} \cdot h \cdot g \in G'.$$

By assumption, $h \cdot \overline{g} = \overline{g}$. However, $h \cdot \overline{g} = \overline{h \cdot g}$. We obtain that there exists $g' \in G'$ such that

$$g \cdot g' = h \cdot g.$$

Q.E.D. point (b).

□

21.2.5. In mathematics, when faced with producing an object with rather nice properties, if one is not so unlucky to find that there are *no* such objects, usually one finds oneself with the difficulty (yes, it is in fact a difficulty) of having *too many to choose from.* Indeed, in this case, there turn out to potentially be many Sylow p-subgroups (in fact their number is congruent to 1 modulo p, so if it is not 1 (i.e., the subgroup is nonnormal), it is at least $p+1$). To get around such difficulties, it is usually a very good idea to consider all such objects at once to prove that just one exists. (For instance, to show that a graph of certain nice properties exists, it is usually advisable to consider all such graphs of that particular type and show that there is nonzero probability of choosing one such when choosing among all possible graphs with some notion of randomness. This is called the probabilistic method of Erdos.)

So to prove point (a) we introduce the following set X equipped with an action of G. Namely, we let X be the set of *all subsets of G of cardinality p^n.* Inside X we will manage to find a very nice subset, namely a *subgroup.*

We let G act on X by left translations. I.e., if $x \in X$ corresponds to $S \subset G$, we let $g \cdot x$ correspond to the subset $g \cdot S$ (multiply all elements of S on the left by g).

The cardinality of X is

$$\binom{p^n m}{p^n},$$

and it is easy to see that it is prime to p. For instance, consider the polynomial $(t+1)^{p^n m}$ modulo p. Since $(a+b)^p = a^p + b^p$ modulo p (do you see why?), we have that this is $(t^{p^n}+1)^m$ modulo p. Now extract the coefficient of t^{p^n}: one the one hand, our original expression guarantees it is $\binom{p^n m}{p^n}$, and on the other our latter expression tells us it is $\binom{m}{1} = m$ modulo p. Now recall that p does not divide m.

Hence, there exists a G-orbit

$$\mathbf{O} \subset X,$$

such that $|\mathbf{O}|$ is prime to p.

Choose a point $S \in \mathbf{O}$. We have

$$|\mathbf{O}| = \frac{p^n \cdot m}{\mathrm{Stab}_G(S)}.$$

Hence, we obtain that $|\,\mathrm{Stab}_G(S)|$ is divisible by p^n. Set $H := \mathrm{Stab}_G(S)$. We will show that

$$|H| = p^n,$$

thereby proving point (a).

21.2.6. To say that S is H-invariant is to say that

$$\forall h \in H, g \in S \text{ we have } h \cdot g \in S.$$

I.e., we can regard S as a set with an H-action.

We claim that for every $g \in S$,

$$\mathrm{Stab}_H(g) = \{1\}.$$

Indeed, $h \cdot g = g$ means $h = 1$, since the action is given by left multiplication in the group G.

Applying Corollary 21.1.3 we obtain that $|S|$ is divisible by $|H|$.

However, $|S| = p^n$. Hence, $|H|$ both divides and is divisible by p^n. Therefore $|H| = p^n$. Q.E.D. point (a).

□

21.3. **Applications of Sylow's theorem.** A subgroup $G_p \subset G$ given by Theorem 21.2.2 is called a *p-Sylow subgroup.*

Corollary 21.3.1. *Any two p-Sylow subgroups of G are conjugate. I.e., if G'_p and G''_p are two subgroups of order p^n, then there exists an element $g \in G$ such that*

$$g \cdot G'_p \cdot g^{-1} = G''_p.$$

Proof. Immediate from Theorem 21.2.2(b) and comparing cardinalities. □

Corollary 21.3.2. *A p-Sylow subgroup is normal if and only if it is the unique p-Sylow subgroup.*

Proof. Immediate from the previous corollary. □

Corollary 21.3.3. *Let $g' \in G$ be an element of order p^m. Then there exists $g \in G$ such that $g \cdot g' \cdot g^{-1} \in G_p$.*

Proof. Consider the subgroup H of G equal to the image of $\phi : \mathbb{Z}/p^m\mathbb{Z} \to G$ with $\phi(\overline{1}) = g'$. Now apply Theorem 21.2.2(b).

□

Corollary 21.3.4. *Suppose every element of G is of order prime to p. Then $|G|$ is of order prime to p.*

Proof. We argue by contradiction. Suppose $|G|$ is not prime to p, i.e., $|G| = p^n \cdot m$ with $n \neq 0$ and m prime to p. By 21.2.2(a), G contains a subgroup G_p of order p^n. Now, every non-unit element of G_p is of order a power of p by Proposition 17.4.5. □

Corollary 21.3.5. *Suppose every element of G is of order a power p. Then $|G|$ is a p-group.*

Proof. We argue by contradiction. Write $|G| = p^n \cdot m$ with $m \neq 1$. Let p' be a prime factor of m. Then by Theorem 21.2.2(a), G contains a subgroup $G_{p'}$ of order a power of p'. Now, every non-unit element of $G_{p'}$ is of order a power of p' by Proposition 17.4.5. □

Remark 21.3.6. *Note that the last two corollaries generalize Corollaries 18.1.7 and 18.1.8 to the non-abelian case.*

21.4. **Group representations.** Historically, groups were first defined as sets of matrices satisfying some properties (invertibility and closure under multiplication and inversion, as you may have guessed). As with many notions in mathematics, it was soon realized that one should separate the definition of an object and its construction — in this case, groups were defined axiomatically and then realized as sets of matrices. For instance, the trivial group (with one element, the identity) is of course the same whether viewed as the identity element inside invertible 1×1 matrices over $\mathbb{Q}$ or as the identity element inside invertible 1728×1728 matrices over $\mathbb{C}$.

But it still remains rather useful to realize groups as linear objects: i.e., subgroups of matrices. It turns out to be more useful to realize a given group *and its quotients* as subgroups of matrices, as we will see. That is to say, to allow for arbitrary homomorphisms to the invertible linear operators of a vector space over a field k.

So let G be a group. We fix a field k and consider vector spaces over k.

21.4.1. A representation of G is a pair $\pi := (V, \phi)$, where V is a k-vector space, and ϕ denotes an action of G on V *as a vector space.* I.e., V is a G-set, such that for every $g \in G$, the map

$$v \mapsto g \cdot v$$

is k-linear.

We can equivalently view the data of ϕ as a group homomorphism $G \to \mathrm{GL}(V)$.

21.4.2. For a representation $\pi = (V, \phi)$, we let π^G be the vector space

$$\{v \in V \mid g \cdot v = v \text{ for all } g \in G\}.$$

We call π^G *the set of G-invariants in π.*

21.4.3. Let $\pi_1 := (V_1, \phi_1)$ and $\pi_2 := (V_2, \phi_2)$ be two G-representations. A map of G-representations $\pi_1 \to \pi_2$ is a map of G-sets $T : V_1 \to V_2$ such that T is k-linear as a map of vector spaces.

Equivalently, T is a linear map $V_1 \to V_2$ which respects the action of G, i.e., for every $v_1 \in V_1$ we have

$$g \cdot T(v_1) = T(g \cdot v_1).$$

We denote the set of maps of G-representations $\pi_1 \to \pi_2$ by

$$\mathrm{Hom}_G(\pi_1, \pi_2).$$

As in [Problem 8, Week 3], it is easy to see that $\mathrm{Hom}_G(\pi_1, \pi_2)$ has a natural structure of vector space.

21.4.4. *Examples.*

(0) The zero representation. We take the zero vector space. Any action on it is trivial.

(i) The trivial representation. We take the vector space k, and the trivial action of G. We shall denote this representation by triv_G, or just triv.

(ii) Let G act on a set X. Take the vector space $\mathrm{Fun}(X, k)$ of *all* k-valued functions on X. We define a G-action on $\mathrm{Fun}(X, k)$ as follows: for $g \in G$ and $f \in \mathrm{Fun}(X, k)$ we define a new function $g \cdot f$ by

$$(g \cdot f)(x) = f(g^{-1} \cdot x).$$

Observe that, for X finite, $\mathrm{Fun}(X, k)$ has a canonical basis as a k-vector space: $\{\delta_x\}_{x \in X}$, where $\delta_x(y) = 0$ unless $x = y$, in which case it is 1. Note that, for $g \in G$, $g \cdot \delta_x = \delta_{g \cdot x}$, which is perhaps easier to remember.

(iii) Take in the previous example $G = S_n$ and $X = \{1, \ldots, n\}$. We can identify $\mathrm{Fun}(X, k)$ with k^n. We obtain an action of S_n on k^n by "permutation of coordinates." We call this representation the *reflection representation* and denote it by refl. The reason for this name is simple: the elements of S_n are products of transpositions (i.e., permutations simply switching two points and leaving everything else fixed), and a transposition (ij) is sent to the reflection switching the i and j coordinates (i.e., through the line spanned by $e_i + e_j$, for $\{e_k\}$ the standard basis). Hence the image of an element of S_n is a product of reflections.

22. Tuesday, Nov. 13

Week 11, HW Problem 1. *Let π be a representation of G. Construct a canonical isomorphism of vector spaces*

$$\pi^G \simeq \mathrm{Hom}_G(\mathrm{triv}_G, \pi).$$

Week 11, HW Problem 2. *Verify that Example (ii) in Sect. 21.4.4 is indeed a group representation.*

22.1. **Characters.**

22.1.1. The word "character" is used in the context of representation theory in two different ways. This can lead to confusion. A compounding factor is that these two notions are related.

Today we will introduce one of these notions. The other one will be deferred until Math 123.

22.1.2. A character of G with values in $k^\times$ is a group homomorphism

$$\chi : G \to k^\times,$$

where $k^\times := k - \{0\}$ is a group under the field multiplication.

22.1.3. To a character we assign a representation, denoted $k^\chi = (k, \chi)$. I.e., we take the vector space to be k, and $\phi : G \to \mathrm{GL}(k)$ to be given by χ, where we note that

$$\mathrm{GL}(k) = \mathrm{GL}_1(k) \simeq k^\times.$$

22.1.4. *Examples.*

(i) Take $k = \mathbb{C}$ and $G = \mathbb{Z}/n\mathbb{Z}$. We have a canonical homomorphism

$$\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$$

given by sending $\overline{k} \in \mathbb{Z}$ to $e^{\frac{2\pi i k}{n}}$ (do you see why this only depends on k mod n?).

(ii) We take k to be any field and $G = S_n$. Note that $k^\times$ always contains the subgroup $\{\pm 1\} \subset k^\times$. We define the *sign* homomorphism

$$S_n \to \{\pm 1\} \to k^\times$$

that sends $g \in S_n$ to $\mathrm{sign}(g)$, the sign of the permutation corresponding to g.

(That is to say, the map taking the value -1 for transpositions (ij), and extending by multiplicativity. It is not a priori obvious that this definition actually makes sense (e.g. a permutation might be written as a product of an odd *and* an even number of transpositions at the same time), but it is a miracle of science that it does. Alternatively, one could take the reflection representation (but over $\mathbb{Z}$) (— which is legitimate, since the entries of the matrices are only 0 or 1 —) defined above, and compose with the determinant map: $S_n \to \mathrm{GL}_n(\mathbb{Z}) \xrightarrow{\det} \mathrm{GL}_1(\mathbb{Z}) \simeq \mathbb{Z}^\times = \{\pm 1\}$. Then the canonical map $\mathbb{Z} \to k$ for any field k gives the desired representation.)

Another way to define the sign homomorphism is to take $\mathrm{sign}(g)$ to be the parity of the number of pairs $1 \leq i < j \leq n$ such that $g(i) > g(j)$. It is easy to see that the assignment

$$g \mapsto \mathrm{sign}(g), \quad S_n \to \{\pm 1\}$$

is a group homomorphism (i.e., the product of two odd permutations is an even permutation, etc.). As an aside, the *alternating group* A_n is defined to be the kernel of this homomorphism (i.e., the subgroup of *even* permutations).

22.2. **Inner Hom.**

22.2.1. Let $\pi_1 = (V_1, \phi_1)$ and $\pi_2 = (V_2, \phi_2)$ be representations of G. We define a new representation, denoted $\underline{\mathrm{Hom}}_G(\pi_1, \pi_2)$ and called the *internal Hom from* π_1 *to* π_2, as follows.

Let the underlying vector space of $\underline{\mathrm{Hom}}_G(\pi_1, \pi_2)$ be $\mathrm{Hom}_k(V_1, V_2)$, the vector space of all linear maps $V_1 \to V_2$.

Let the action of G on $\mathrm{Hom}_k(V_1, V_2)$ be as follows. For $g \in G$ and $T \in \mathrm{Hom}_k(V_1, V_2)$ we define a new element $T^g \in \mathrm{Hom}_k(V_1, V_2)$ by the rule

$$T^g = \phi_2(g) \circ T \circ \phi_1(g^{-1}). \tag{35}$$

Week 11, HW Problem 3. *Verify that the formula in* (35) *indeed defines a representation.*

22.2.2. We now claim:

Lemma 22.2.3. *For two representations* π_1 *and* π_2*, the vector spaces*

$$\left(\underline{\mathrm{Hom}}_G(\pi_1, \pi_2)\right)^G \text{ and } \mathrm{Hom}_G(\pi_1, \pi_2)$$

are canonically isomorphic.

Proof. By definition (i.e., by Sect. 21.4.2), $(\underline{\mathrm{Hom}}_G(\pi_1, \pi_2))^G$ is the subspace of $\mathrm{Hom}_k(V_1, V_2)$ consisting of those $T : V_1 \to V_2$ for which

$$\phi_2(g) \circ T \circ \phi_1(g^{-1}) = T \ \forall g \in G. \tag{36}$$

By definition (i.e., by Sect. 21.4.3), $\mathrm{Hom}_G(\pi_1, \pi_2)$ is the subspace of $\mathrm{Hom}_k(V_1, V_2)$ consisting of those $T : V_1 \to V_2$ for which

$$\phi_2(g) \circ T = T \circ \phi_1(g) \ \forall g \in G. \tag{37}$$

Now observe that conditions (36) and (37) are equivalent.

□

22.3. **Group representations as modules over a ring.** The material of this subsection wasn't in the lecture. Nonetheless, you need to study it, as a crucial HW problem is based on it.

22.3.1. Let G be a group. It turns out that, much like vector spaces with an endomorphism could be interpreted as modules over the polynomial ring in one variable over the base field, k-representations of G can be interpreted as modules over another ring, called the *group ring* of G. Let's get to defining this guy, who we will call $k[G]$, then.

As a vector space, $k[G]$ is the space of finite linear combinations of elements of G with coefficients in k: i.e., symbols of shape $\sum_{g \in G} a_g[g]$, with all but finitely many $a_g = 0$. We will also write δ_g for $[g]$, since these sums have evident interpretations as k-valued functions (with finite support) on G.

22.3.2. We called the thing the group *ring*, so there should probably be a multiplication somewhere. In fact it is the evident one: certainly $[g] \cdot [h]$ should be $[gh]$ — so we define $[g] \cdot [h] := [gh]$. Moreover, the multiplication should distribute over addition, so we simply extend it by linearity. That is to say,

$$\left(\sum_{g \in G} a_g[g]\right) \cdot \left(\sum_{g \in G} b_g[g]\right) := \sum_{g \in G} \sum_{g' \in G} a_g b_{g'} [gg']. \tag{38}$$

Actually such a thing is called a *k-algebra*, since it admits a canonical map from k, namely $a \mapsto a[1]$. So we will also call $k[G]$ the *group algebra* of G over k.

Week 11, HW Problem 4. *Show that formula* (38) *gives rise to a uniquely defined structure of ring on $k[G]$, with the unit being $[1] = \delta_1$.*

Week 11, HW Problem 5.

(a) *Show that a datum of a G-representation over a field k is equivalent to that of a $k[G]$-module.*

(b) *Show that, for two representations π_1 and π_2, we have a canonical isomorphism*

$$\mathrm{Hom}_G(\pi_1, \pi_2) \simeq \mathrm{Hom}_{k[G]}(\pi_1, \pi_2),$$

where we are interpreting G-representations as $k[G]$-modules via point (a)[3].

22.3.3. The interpretation of G-representations as modules over a particular ring allows us to transport all the notions from the general theory of R-modules to the realm of representations.

So, for instance, we automatically have the notion of direct sum of representations (along with its universal properties of mapping in and mapping out, see [Problems 1 and 2, Week 3]).

In addition, we have the notion of subrepresentation, quotient representation, and the universal property of quotient representations (see Proposition 5.1.4).

22.3.4. *Subrepresentaions.* Let $\pi = (V, \phi)$ be a representation.

Week 11, HW Problem 6. *Show that subrepresentations $\pi' \subset \pi$ are in bijection with subspaces $V' \subset V$ that are G-invariant.*

22.3.5. Here are some examples of subrepresentations. Let G act on a finite set X. Consider the representation π on the vector space $V := \mathrm{Fun}(X, k)$, see Example (ii) in Sect. 21.4.4.

We define the subrepresentation $\pi' \subset \pi$ as the vector subspace

$$V' \subset \mathrm{Fun}(X, k)$$

that consists of *constant* functions. I.e.,

$$V' = \{f \in \mathrm{Fun}(X, k) \mid f(x_1) = f(x_2) \text{ for all } x_1, x_2 \in X\}.$$

Week 11, HW Problem 7. *Show that the subspace V' is G-invariant and that the corresponding sub-representation π' is canonically isomorphic to* triv_G.

[3] Recall the notation $\mathrm{Hom}_R(M_1, M_2)$ from Sect. 4.3.2.

22.3.6. We take π to be the same representation as above. We define a vector subspace

$$V'' \subset \mathrm{Fun}(X,k)$$

by

$$V'' := \{f \in \mathrm{Fun}(X,k) \,|\, \sum_{x\in X} f(x) = 0\}.$$

Week 11, HW Problem 8. *Show that the subspace V'' is G-invariant and that the resulting quotient representation π/π'' is canonically isomorphic to* triv_G.

22.4. **Irreducibility.**

22.4.1. Let R be a ring and M an R-module. We shall say that M is irreducible if it is nonzero and does not contain any proper non-zero ("nontrivial") submodules.

(For example, take $R = \mathbb{Z}$ and M a finite abelian group. M is irreducible if and only if it is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.)

22.4.2. By Sect. 22.3.3, we automatically obtain the notion of irreducible representation.

By Problem 6, a representation $\pi = (V, \phi)$ is irreducible if and only if V does not contain any proper non-zero G-invariant subspaces. Alternatively, π is irreducible if and only if span of the G-orbit of any nonzero vector $v \in V$ is all of V!

22.4.3. In general, given a complicated object (like a representation), we'd like to write it as a direct sum of simpler objects. We have seen two instances where this has given us considerable strength over a particular class of objects: Jordan canonical form and the classification of finite abelian groups.

Note that it is *not* true for a general ring R that any R-module is isomorphic to the direct sum of a bunch of irreducible modules. E.g., for $R = \mathbb{Z}$, the module $\mathbb{Z}/p^2\mathbb{Z}$ is not isomorphic to a direct sum of $\mathbb{Z}/p\mathbb{Z}$'s.

However, we shall see that we are much luckier in the context of representations: every finite-dimensional representation of a group G over a field k admits such a direct sum decomposition, at least under certain conditions on G and k.

This phenomenon is called *complete reducibility.*

22.4.4. *Examples.* Any 1-dimensional representation is automatically irreducible. Proof: if $\dim(V) = 1$, there is no room for nontrivial subspaces of V.

Consider the group $G = S_n$ and the representation $\pi = \mathrm{refl}$. Let $\mathrm{refl}_0 \subset \mathrm{refl}$ be the subrepresentation corresponding to π'' of Sect. 22.3.6.

Week 11, HW Problem 9. *Take $n = 3$. And assume that $k = \mathbb{C}$.*[4] *Show that* refl_0 *is irreducible.*

Suggested strategy: there is no strategy. This is an explcit hands-on analysis.

Week 11, HW Problem 10. *Let k be algebraically closed and let G be abelian. Show that any irreducible finite-dimensional representation of G is of the form k^χ for some character χ.*

Hint: Use [Problem 4, Week 7].

[4] What is important here is that the *characteristic* of k is different from 3, see next lecture.

22.4.5. We have the following general assertion:

Lemma 22.4.6. *Let $T : M_1 \to M_2$ be a non-zero map of modules over a ring R.*

(a) *If M_1 is irreducible, then T is injective.*

(b) *If M_2 is irreducible, then T is surjective.*

(c) *If both M_1 and M_2 are irreducible, then T is an isomorphism.*

23. Tuesday, Nov. 14

Week 11, HW Problem 11. Let G be a group and H a subgroup. Consider the G-set $X := G/H$, and assume that X is finite. Consider the representation of G on $\mathrm{Fun}(X, k)$, see Example (ii) in Sect. 21.4.4. Construct an isomorphism of vector spaces

$$\mathrm{Hom}_G(\mathrm{Fun}(X, k), \pi) \simeq \pi^H$$

for any G-representation π.

Hint: compare with [Problem 6, Week 10].

Week 11, HW Problem 12. *Let X be a finite G-set, and consider the representation of G on $\mathrm{Fun}(X, k)$, see Example (ii) in Sect. 21.4.4. Show that $(\mathrm{Fun}(X, k))^G$ admits a basis formed by* characteristic functions *of G-orbits on X. I.e., for each orbit $\mathbf{O}$, we take the function $\delta_{\mathbf{O}} : X \to k$ defined by*

$$\delta_{\mathbf{O}}(x) = \begin{cases} 1 & \text{if } x \in \mathbf{O}, \\ 0 & \text{if } x \notin \mathbf{O}. \end{cases}$$

23.1. **Characteristic of a field.**

23.1.1. Note that any ring R receives a canonical homomorphism $\phi_{can,R} : \mathbb{Z} \to R$,

$$n \mapsto \underbrace{1 + \ldots + 1}_{n}.$$

Note that for a ring homomorphism $\psi : R_1 \to R_2$ we have

$$\psi \circ \phi_{can,R_1} = \phi_{can,R_2}. \tag{39}$$

23.1.2. Let k be a field. We would like to write things like $\frac{4}{5} + 2p^2 + \frac{1}{101^{100}} \in k$, which we can certainly do via this canonical map from $\mathbb{Z}$ — that is, so long as the denominators of our expressions are nonzero! There is a rather easy way to encode precisely which denominators we must avoid, called the *characteristic of k*.

We shall say that the characteristic of k is *zero* if $\phi_{can,k}$ is injective.

We shall say that characteristic of k is n if $\phi_{can,k}$ is not injective, but has kernel $n\mathbb{Z}$. In general we will call fields k for which $\phi_{can,k}$ is not injective fields of *positive characteristic.*

23.1.3. Note that if k has characteristic zero, the homomorphism $\phi_{can,k}$ uniquely extends to a homomorphism

$$\mathbb{Q} \to k, \quad \frac{m}{n} \mapsto \frac{\phi_{can,k}(m)}{\phi_{can,k}(n)}.$$

Moreover, we have:

Lemma 23.1.4. *A field k has characteristic zero if and only if there exists a field homomorphism $\mathbb{Q} \to k$.*

Proof. If k has characteristic zero, a homomorphism $\mathbb{Q} \to k$ was constructed above. If $\mathbb{Q} \to k$ exists, it is automatically injective (any homomorphism from a field to a ring is injective: do you see why?), and the assertion follows from (39), by looking at the composition

$$\mathbb{Z} \to \mathbb{Q} \to k.$$

□

23.1.5. Suppose now that k has positive characteristic. Consider $\ker(\phi_{can,k})$. This is an ideal on $\mathbb{Z}$, and hence is of the form $n\mathbb{Z} \subset \mathbb{Z}$ for a a unique positive integer n.

Lemma 23.1.6. *The integer n is a prime number.*

Proof. If $n = n_1 \cdot n_2$, we have

$$\phi_{can,k}(n_1) \cdot \phi_{can,k}(n_2) = \phi_{can,k}(n) = 0 \in k,$$

and since k is a field, either $\phi_{can,k}(n_1) = 0$ or $\phi_{can,k}(n_2) = 0$. Hence n divides either n_1 or n_2. □

We hence write p, rather than n (which usually stands for a random integer), for the characteristic of a field of positive characteristic.

By construction, if k is of characteristic p, the map $\phi_{can,k}$ uniquely factors through an automatically injective field homomorphism

$$\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to k.$$

Notation: we denote the field $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$.

As in Lemma 23.1.4 we prove:

Lemma 23.1.7. *A field k has characteristic p if and only if there exists a field homomorphism $\mathbb{F}_p \to k$.*

23.2. **Complete reducibilty of representations.** From now on, unless specified otherwise, we will assume that G is a finite group.

23.2.1. Our goal is prove the following theorem:

Theorem 23.2.2 (Maschke)**.** *Let G be such that* $\text{char}(k)$ *does not divide $|G|$. Then any finite-dimensional representation π of G is isomorphic to a direct sum of irreducible representations.*

We will deduce Theorem 23.2.2 from the next result:

Theorem 23.2.3. *Let G be such that* $\text{char}(k)$ *does not divide $|G|$. Then any short exact sequence*

$$0 \to \pi' \to \pi \to \pi'' \to 0$$

of finite-dimensional representations of G splits (see Sect. 5.2.5).

23.2.4. Let us show how Theorem 23.2.3 implies Theorem 23.2.2:

Proof of Theorem 23.2.2. We proceed by induction on $\dim \pi$. If π is irreducible, there is nothing to prove. Otherwise, let π' be a non-zero subrepresentation of π of minimal degree. By minimality, π' is irreducible. Set $\pi'' := \pi/\pi'$.

By 23.2.3 there exists an isomorphism

$$\pi \cong \pi' \oplus \pi''.$$

(This via considering $0 \to \pi' \to \pi \to \pi'' \to 0$.)

By the induction hypothesis, π' is isomorphic to a direct sum of irreducible representations. Hence so is π upon adding on π'. □

23.2.5. In fact, we can also deduce Theorem 23.2.3 *from* Theorem 23.2.2:

Week 11, HW Problem 13. *Let R be a ring, and M an R-module which is isomorphic to a finite direct sum of irreducible R-modules. Show that every short exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

of R-modules splits.

NB: this problem is not very easy, but it is certainly important to solve it since a close cousin will likely be on the final.

23.2.6. Let us show why the assumption that $|G|$ not be divisible by $\text{char}(k)$ is important. Take $G := S_2 \simeq \mathbb{Z}/2\mathbb{Z}$, and let π be the representation refl. Consider the short exact sequence

$$0 \to \text{refl}_0 \to \text{refl} \xrightarrow{T} \text{triv} \to 0,$$

where T is the map

$$f \mapsto f(1) + f(2).$$

We claim that the above short exact sequence does not split if $\text{char}(k) = 2$. Indeed, by Problem 1, such a splitting would produce an S_2-invariant element f in refl such that $T(f) = 1$. However, S_2-invariance of f means precisely that $f(1) = f(2)$, while

$$T(f) = f(1) + f(2) = f(1) \cdot (1 + 1) = f(1) \cdot 0 = 0,$$

because $\text{char}(k) = 2$.

Note that we can also see the breakdown of our complete reducibility theorem (i.e., Maschke's theorem) from before in this example. Suppose otherwise. Then the tautological injection $\text{refl}_0 \to \text{refl}$ would imply (by our results about nontrivial maps between irreducible modules necessarily being isomorphisms) that a direct sum decomposition must contain refl_0. But the above shows that this is impossible (since refl_0 having a direct sum complement is precisely equivalent to the relevant short exact sequence splitting). Alternatively, refl literally has four elements, so there isn't exactly much choice for irreducible subrepresentations to form a direct sum.

23.2.7. We will deduce 23.2.3 from yet another theorem:

Theorem 23.2.8. *Let G be such that* $\mathrm{char}(k)$ *does not divide* $|G|$. *Let* $T : \rho_1 \to \rho_2$ *be a surjective map of G-representations. Then the induced map*

$$\rho_1^G \to \rho_2^G$$

is also surjective.

23.2.9. Let us show how Theorem 23.2.8 implies 23.2.3:

Proof of Theorem 23.2.3. We need to show that if $T : \pi_1 \to \pi_2$ is a surjection of representations, then it admits a right inverse. This is equivalent to showing that the element $\mathrm{Id} \in \mathrm{Hom}_G(\pi_2, \pi_2)$ lies in the image of the map

$$\mathrm{Hom}_G(\pi_2, \pi_1) \to \mathrm{Hom}_G(\pi_2, \pi_2). \tag{40}$$

We will show that the map (40) is surjective.

Set $\rho_1 := \underline{\mathrm{Hom}}_G(\pi_2, \pi_1)$ and $\rho_2 := \underline{\mathrm{Hom}}_G(\pi_2, \pi_2)$. It is easy to see (check this!) that composition with T gives a map of G-representations

$$\rho_1 \to \rho_2,$$

precisely because T is a map of representations.

We claim that the above map $\rho_1 \to \rho_2$ is surjective. Indeed, let V_i, $i = 1, 2$, be the vector space underlying π_i. Recall that the vector space underlying $\underline{\mathrm{Hom}}_G(\pi_2, \pi_1)$ is $\mathrm{Hom}_k(V_2, V_1)$ and the vector space underlying $\underline{\mathrm{Hom}}_G(\pi_2, \pi_2)$ is $\mathrm{Hom}_k(V_2, V_2)$. Note that if $T : V_1 \to V_2$ is a surjective map of vector spaces, and W is a finite-dimensional vector space, then the map

$$\mathrm{Hom}_k(W, V_1) \to \mathrm{Hom}_k(W, V_2)$$

is surjective (indeed, choose a basis of W, etc.). Taking $W = V_2$, we obtain that $\rho_1 \to \rho_2$ is indeed surjective.

Applying Theorem 23.2.8, we obtain that the map

$$\rho_1^G \to \rho_2^G$$

is surjective.

The surjectivity of (40) follows now from Lemma 22.2.3.

□

23.2.10. *Proof of Theorem 23.2.8.* The proof uses a new idea: that of an averaging operator.

Let G be a finite group, such that $\mathrm{char}(k)$ does not divide $|G|$. Let $\rho = (V, \phi)$ be a representation of G. We define a map

$$\mathrm{Av}_G : V \to V$$

by

$$\mathrm{Av}_G(v) = \frac{1}{|G|} \sum_{g \in G} g \cdot v.$$

Note that $\frac{1}{|G|}$ makes sense as an element of k, since

$$|G| = \underbrace{1 + \ldots + 1}_{|G|} \neq 0.$$

Week 11, HW Problem 14.

(a) *Show that the image of* Av_G *is contained in* $\rho^G \subset V$.

(b) *Show that the restriction of* Av_G *to* $\rho^G \subset V$ *is the identity operator.*

(c) *Deduce that* $\mathrm{Av}_G \circ \mathrm{Av}_G = \mathrm{Av}_G$.

(d) *Show that if* V *is a vector space and* S *is an endomorphism such that* $S^2 = S$, *then* $V = \mathrm{Im}(S) \oplus \mathrm{Im}(\mathrm{Id} - S)$.

(e) *Show that* ρ *as a representation splits canonically as* $\rho^{\mathrm{inv}} \oplus \rho^{\text{non-inv}}$, *where the action of* G *on* $\rho^{\mathrm{inv}} := \rho^G$ *is trivial, and* $(\rho^{\text{non-inv}})^G = 0$.

(f) *Show that if* $\rho_1 \to \rho_2$ *is map of representations, then* ρ_1^{inv} *gets mapped to* ρ_2^{inv} *and* $\rho_1^{\text{non-inv}}$ *gets mapped to* $\rho_2^{\text{non-inv}}$.

Week 11, HW Problem 15. *Deduce the assertion of Theorem 23.2.8 from Problem 14.*

Having had the idea to average over each element of G, we can now give a completely equivalent but much more direct proof of the original assertion. Certainly by induction it suffices to show that a surjection of finite dimensional representations

$$\pi \to \pi' \to 0$$

splits. Certainly it splits on the level of vector spaces — i.e.,

$$V_\pi \to V_{\pi'} \to 0$$

splits (upon choosing a basis, etc.). Let

$$T : V_{\pi'} \to V_\pi$$

be such a splitting (so that $V_{\pi'} \xrightarrow{T} V_\pi \to V_{\pi'}$ is the identity map). Unfortunately for us, T isn't guaranteed to be a map of representations. But we can force it to be via this averaging idea: consider

$$S := \frac{1}{|G|} \sum_{g \in G} gTg^{-1} : v \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot T(g^{-1} \cdot v).$$

Check that this is indeed a map of representations $\pi' \to \pi$ such that $\pi' \xrightarrow{S} \pi \to \pi'$ is the identity!

24. Tuesday, Nov. 27

24.1. **Schur's lemma.**

24.1.1. Let G be an arbitrary group and π a G-representation. Note that we have a tautological map of vector spaces

$$k \to \mathrm{Hom}_G(\pi, \pi). \tag{41}$$

We claim:

Theorem 24.1.2 (Schur's lemma)**.** *Suppose that* k *is algebraically closed and* π *is irreducible and finite dimensional. Then the map* (41) *is an isomorphism.*

Proof. Let T be a non-zero element of $\mathrm{Hom}_G(\pi, \pi)$. Let V denote the vector space that underlies π, so T is an endomorphism of V. Since k is algebraically closed, T admits an eigenvalue. Let V^λ be the corresponding eigenspace, i.e.,

$$V^\lambda = \ker(T - \lambda) \neq 0.$$

Observe that $(T - \lambda) \in \mathrm{Hom}_G(\pi, \pi)$. Hence V^λ is G-invariant. But π was irreducible! Hence $V^\lambda = V$. Hence $T = \lambda \cdot \mathrm{Id}$. □

24.1.3. Note that Schur's lemma breaks down if k is not algebraically closed. For example, take $k := \mathbb{R}$, $G := \mathbb{Z}/3\mathbb{Z}$, and π the representation of G on $\mathbb{R}^2 \simeq \mathbb{C}$ via rotation by multiples of $\frac{2\pi}{3}$. Then

$$\mathrm{End}_G(\pi) \simeq \mathbb{C}.$$

24.2. **Corollaries of Schur's lemma.**

24.2.1. From now until the end of the semester we will impose the following assumptions:

- G is finite;
- k is algebraically closed;
- $\mathrm{char}(k)$ does not divide $|G|$.

(Hence we may freely use Maschke and Schur!)

24.2.2. Let us fix a choice of irreducible representation in each isomorphism class. We will denote the resulting set by $\mathrm{Irrep}(G)$. In other words, $\mathrm{Irrep}(G)$ is a set whose elements are representations of G such that:

- for every $\rho \in \mathrm{Irrep}(G)$, the representation ρ is non-zero and irreducible;
- for every irreducible representation π of G, there exists $\rho \in \mathrm{Irrep}(G)$ and an isomorphism $\pi \cong \rho$.
- for any two distinct elements $\rho_1 \neq \rho_2 \in \mathrm{Irrep}(G)$, the representations ρ_1 and ρ_2 are non-isomorphic.

24.2.3. Acoording to Maschke's theorem, any finite-dimensional representation π of G is isomorphic to a direct sum of irreducible representations.

Hence, we can write

$$\pi \cong \bigoplus_{\rho \in \mathrm{Irrep}(G)} \underbrace{\rho \oplus \ldots \oplus \rho}_{n_\rho}. \tag{42}$$

Proposition 24.2.4. *The vector spaces* $\mathrm{Hom}_G(\rho, \pi)$ *and* $\mathrm{Hom}_G(\pi, \rho)$ *both identify canonically with* k^{n_ρ}*, where* n_ρ *is as in* (42).

Week 12, HW Problem 1. *Prove Proposition 24.2.4.*

Corollary 24.2.5. $n_\rho = \dim \mathrm{Hom}_G(\rho, \pi) = \dim \mathrm{Hom}_G(\pi, \rho)$.

24.2.6. Let now π^1 and π^2 be two finite-dimensional representations. For each $\rho \in \mathrm{Irrep}(G)$ postcomposition defines a map

$$\mathrm{Hom}_G(\pi^1, \pi^2) \to \mathrm{Hom}_k(\mathrm{Hom}_G(\rho, \pi^1), \mathrm{Hom}_G(\rho, \pi^2)). \tag{43}$$

Hence, we obtain a map

$$\mathrm{Hom}_G(\pi^1, \pi^2) \to \bigoplus_{\rho \in \mathrm{Irrep}(G)} \mathrm{Hom}_k(\mathrm{Hom}_G(\rho, \pi^1), \mathrm{Hom}_G(\rho, \pi^2)). \tag{44}$$

(Note that in the right hand side we have a finite direct sum, by Corollary 24.2.5 there are at most finitely many ρ's for which $\mathrm{Hom}_G(\rho, \pi) \neq 0$. [5])

Proposition 24.2.7. *The map* (44) *is an isomorphism.*

Week 12, HW Problem 2. *Prove Proposition 24.2.4.*

24.2.8. Let now π^1 and π^2 be two finite-dimensional representations, and let n^1_ρ and n^2_ρ be the corresponding integers.

Corollary 24.2.9.

$$\mathrm{Hom}_G(\pi^1, \pi^2) \simeq \bigoplus_{\rho \in \mathrm{Irrep}(G)} \mathrm{Mat}_{n^1_\rho, n^2_\rho}.$$

Proof. Combine Propositions 24.2.4 and 24.2.7. □

Corollary 24.2.10. *A representation π is irreducible if and only if*

$$\dim \mathrm{End}_G(\pi) = 1.$$

Proof. This follows from Corollary 24.2.9. □

And yet another corollary:

Corollary 24.2.11. *Let π^1 and π^2 be such that* $\dim \mathrm{Hom}_G(\pi^1, \pi^2) = 1$. *Let T be a non-zero map $\pi^1 \to \pi^2$. Then* $\mathrm{Im}(T)$ *is irreducible.*

Proof. It follows from Proposition 24.2.9 that there exists a unique irreducible representation ρ_0 such that $n^1_{\rho_0}$ and $n^2_{\rho_0}$ are both nonzero. In fact this also implies that $n^1_{\rho_0} = n^2_{\rho_0} = 1$. Then, up to a non-zero scalar, T equals

$$\pi^1 \cong \bigoplus_{\rho \in \mathrm{Irrep}(G)} \underbrace{\rho \oplus \ldots \oplus \rho}_{n^1_\rho} \twoheadrightarrow \rho_0 \hookrightarrow \bigoplus_{\rho \in \mathrm{Irrep}(G)} \underbrace{\rho \oplus \ldots \oplus \rho}_{n^2_\rho} \cong \pi^2.$$

□

24.3. Decomposition of the regular representation.

[5] We shall soon see that the set $\mathrm{Irrep}(G)$ is in fact finite.

24.3.1. We introduce some notation. Let π_1 and π_2 be representations of G. Recall that we have the vector space $\mathrm{Hom}_G(\pi_1\pi_2)$ and the G-representation $\underline{\mathrm{Hom}}_G(\pi_1, \pi_2)$.

We now introduce yet another object, namely, $\underline{\underline{\mathrm{Hom}}}_G(\pi_1, \pi_2)$, which will be a representation of $G \times G$. The vector space underlying $\underline{\underline{\mathrm{Hom}}}_G(\pi_1, \pi_2)$ is $\mathrm{Hom}_k(V_1, V_2)$, where V_i is the vector space underlying π_i.

The action of $G \times G$ on $\mathrm{Hom}_k(V_1, V_2)$ is defined as follows: for $(g', g'') \in G \times G$ and $T \in \mathrm{Hom}_k(V_1, V_2)$, we set

$$T^{(g',g'')} = \phi_2(g') \circ T \circ \phi_1\left((g'')^{-1}\right).$$

Note that $\underline{\mathrm{Hom}}_G(\pi_1, \pi_2)$ identifies with the restriction of $\underline{\underline{\mathrm{Hom}}}_G(\pi_1, \pi_2)$ under the diagonal embedding $G \xrightarrow{\Delta} G \times G$.

24.3.2. We now let $\mathrm{Reg}(G)$ denote the representation of $G \times G$ on the vector space $\mathrm{Fun}(G, k)$, corresponding to the action of the group $G \times G$ on the set G,

$$(g', g'') \cdot g = g' \cdot g \cdot (g'')^{-1},$$

see Example 21.4.4(ii).

We let $\mathrm{Reg}^l(G)$, $\mathrm{Reg}^r(G)$, $\mathrm{Reg}^{conj}(G)$ denote the representation of G obtained by restricting $\mathrm{Reg}(G)$ along the maps $G \to G \times G$ given by

$$g \mapsto (g, 1), \quad g \mapsto (1, g), \quad g \mapsto (g, g),$$

respectively.

24.3.3. The main structure theorem about representations of finite groups (under the assumptions of Sect. 24.2.1) says:

Theorem 24.3.4. *There exists an isomorphism of $G \times G$-representations*

$$\mathrm{Reg}(G) \cong \bigoplus_{\rho \in \mathrm{Irrep}(G)} \underline{\underline{\mathrm{Hom}}}_G(\rho, \rho).$$

24.3.5. Let us derive some corollaries of this theorem before we prove it:

Corollary 24.3.6.

$$|G| = \sum_{\rho \in \mathrm{Irrep}(G)} \dim(\rho)^2.$$

Proof. Compare the dimensions of the two sides of the theorem. □

Corollary 24.3.7. *The set* $\mathrm{Irrep}(G)$ *is finite.*

Proof.

$$|G| = \sum_{\rho \in \mathrm{Irrep}(G)} \dim \rho^2 \geq |\,\mathrm{Irrep}(G)|.$$

□

Corollary 24.3.8. *The cardinality of* $\mathrm{Irrep}(G)$ *equals the number of conjugacy classes in G (i.e., G-orbits on G with respect to the action by conjugation).*

Proof. Restricting the isomorphism of the theorem to G along the diagonal embedding, we obtain an isomorpism of G-representations:

$$\mathrm{Reg}^{conj}(G) \cong \bigoplus_{\rho \in \mathrm{Irrep}(G)} \underline{\mathrm{Hom}}_G(\rho, \rho).$$

Taking G-invariants on both sides, we obtain:

$$(\mathrm{Reg}^{conj}(G))^G \cong \bigoplus_{\rho \in \mathrm{Irrep}(G)} (\underline{\mathrm{Hom}}_G(\rho, \rho))^G \simeq \bigoplus_{\rho \in \mathrm{Irrep}(G)} \mathrm{Hom}_G(\rho, \rho) \simeq \bigoplus_{\rho \in \mathrm{Irrep}(G)} k,$$

where the last isomorphism follows from Schur's lemma.

The dimension of the right-hand side is $|\,\mathrm{Irrep}(G)|$. The dimension of the left-hand side is, by [Problem 12, Week 11], equal to the number of conjugacy classes in G. □

24.3.9. *Examples: abelianness via representations.*

Corollary 24.3.10. *Let G be abelian. Then the number of characters $\chi : G \to k^\times$ equals $|G|$.*

Proof. By [Problem 10, Week 11], all irreducible representations of G are of the form k^χ for χ a character $G \to k^\times$. Furthermore, it is clear that different characters correspond to non-isomorphic representations (prove this!). Hence, the set $\mathrm{Irrep}(G)$ is in a bijection with the set of characters of G.

Now, the assertion follows from Corollary 24.3.6, since for every $\rho \in \mathrm{Irrep}(G)$, we have $\dim(\rho) = 1$. □

(Alternatively, for G abelian, the number of conjugacy classes in G is just $|G|$. Alternatively still, we could write $G \cong \oplus_i \mathbb{Z}/n_i\mathbb{Z}$ and then verify the claim for cyclic groups (i.e., $\mathbb{Z}/n\mathbb{Z}$s). But there the claim is evident since to give a map $\mathbb{Z}/n\mathbb{Z} \to k^\times$ is precisely to give an n-th root of unity (i.e., a $\zeta \in k^\times$ for which $\zeta^n = 1$), and our field is algebraically closed, so it contains all n of these guys.)

Corollary 24.3.11. *Suppose that every irreducible representation of G is one-dimensional. Then G is abelian.*

Proof. From Corollary 24.3.6 we obtain that

$$|G| = |\,\mathrm{Irrep}(G)|.$$

Hence, from Corollary 24.3.8, we obtain that the number of conjugacy classes in G equals $|G|$. This can only happen if every element of G is its own conjugacy class. This is equivalent to G being abelian. □

24.3.12. *Examples: representations of small symmetric groups.* Let us classify all irreducible representations of S_3. We already know three: triv, k^{sign} and refl_0 (see [Problem 9, Week 11]). We claim that this exhausts the list of irreducible representations of S_3. Indeed, this follows from Corollary 24.3.6, since

$$6 = |S_3| = 1 + 1 + 2^2.$$

Week 12, HW Problem 3. *Show that the representation* refl_0 *of S_n is irreducible for any n.*

Hint: Use induction.

Let us now classify representations of S_4. Again, we know three: triv, k^{sign} and refl_0, whose dimensions are 1, 1 and 3 respectively. We claim that the number of conjugacy classes in S_4 equals 5 (see Sect. 24.3.13 below). Hence, there are two more irreducible representations, ρ_1 and ρ_2 such that

$$\dim(\rho_1)^2 + \dim(\rho_2)^2 = 24 - 1 - 1 - 3^2 = 13.$$

From here we see that, without loss of generality, we are forced to have $\dim(\rho_1) = 2$ and $\dim(\rho_2) = 3$.

Actually we will see later on that we can determine much more than just the dimensions of the ρ_i from this sort of data. We will introduce certain functions that classify representations up to isomorphism, and we will see that we are in a position to almost determine these functions for every one of these representations without even knowing two out of the five irreducible representations of our group!

24.3.13. *Digression: conjugacy classes in S_n.* We will establish a bijection between the set of conjugacy classes in S_n and partitions of n:

$$n = n_1 + \cdots + n_k, \quad n_1 \geq \cdots \geq n_k.$$

Namely, to each partition we attach an element that rotates the elements in each segment of the partition by a cycle (e.g., $1 \mapsto 2, 2 \mapsto 3, \ldots, n_1 - 1 \mapsto n_1, n_1 \mapsto 1$ would be the first cycle).

Vice versa, given an element $g \in S_n$, there is a unique group homomorphism $\mathbb{Z} \to S_n$ that sends $1 \mapsto g$. Consider the resulting action of $\mathbb{Z}$ on the set $\{1, \ldots, n\}$. Divide $\{1, \ldots, n\}$ according to the orbits of this action.

Week 12, HW Problem 4. *Show that by replacing g by a conjugate element, we can arrange that the above orbits are the segments of a partition.*

Week 12, HW Problem 5. *Show that the above establishes a bijection between the set of partitions of n and the set of conjugacy classes in S_n.*

25. Thursday, Nov. 29

25.1. **Proof of Theorem 24.3.4.** We have run out of ways to put off the proof of the theorem. So let us begin.

25.1.1. *Step 1.* We are going to first directly prove Corollary 24.3.6 (and in particular the fact that $\text{Irrep}(G)$ is finite).

Consider the G-representation $\text{Reg}^l(G)$. Decompose it as a direct sum of irreducibles:

$$\text{Reg}^l(G) \simeq \bigoplus_{\rho \in \text{Irrep}(G)} \underbrace{\rho \oplus \ldots \oplus \rho}_{n_\rho}.$$

It is enough to show that for every $\rho \in \text{Irrep}(G)$, we have $n_\rho = \dim(\rho)$. By Corollary 24.2.9, it is enough to show that for every ρ, the vector space $\text{Hom}_G(\text{Reg}^l(G), \rho)$ is isomorphic to the vector space underlying ρ. However, this follows from [Problem 11, Week 11].

25.1.2. *Step 2.* Let π be a representation of G. We will construct a map of $G \times G$-representations

$$\mathrm{Reg}(G) \to \underline{\underline{\mathrm{Hom}}}_G(\pi, \pi).$$

Recall our old friend $k[G]$ (see Sect. 22.3). By [Problem 5, Week 11] we have a canonical map of vector spaces

$$A_\pi : k[G] \to \mathrm{Hom}_k(V, V), \tag{45}$$

where V is the vector space underlying π.

Note that we have a canonical isomorphism of vector spaces

$$k[G] \simeq \mathrm{Fun}(G, k),$$

that sends δ_g to the (Kronecker) δ function at g (i.e., the function that takes the value 1 at g and 0 everywhere else). Hence the notation!

So we obtain a map of vector spaces

$$\mathrm{Fun}(G, k) \to \mathrm{Hom}_k(V, V). \tag{46}$$

Week 12, HW Problem 6. *Show that the map* (46) *is in fact a map of $G \times G$-representations, where on the left-hand side the structure of $G \times G$-representation is that of* $\mathrm{Reg}(G)$*, and on the right-hand side the structure of $G \times G$ representation is that of* $\underline{\underline{\mathrm{Hom}}}_G(\pi, \pi)$*.*

Week 12, HW Problem 7. *Let us view $k[G]$ as a module over itself, and hence as a G-representation via [Problem 5, Week 11]. Show that as such it is isomorphic to* $\mathrm{Reg}^l(G)$*.*

25.1.3. *Step 3.* Let us apply the construction from Step 2 for each $\rho \in \mathrm{Irrep}(G)$. Taking the direct sum of these maps, we obtain a map

$$\mathrm{Reg}(G) \to \bigoplus_{\rho \in \mathrm{Irrep}(G)} \underline{\underline{\mathrm{Hom}}}_G(\rho, \rho). \tag{47}$$

The claim is that this map is an isomorphism. By Step 1, the two sides have the same dimension. Hence it suffices to show that the map in (47) is injective. For this we forget the structure of $G \times G$-representations and simply consider the underlying map of vector spaces

$$k[G] \to \bigoplus_{\rho \in \mathrm{Irrep}(G)} \mathrm{Hom}_k(V_\rho, V_\rho), \tag{48}$$

where V_ρ denotes the vector space underlying ρ.

Let $f \in k[G]$ be an element lying in the kernel of the map (48). I.e.,

$$f \in \ker(A_\rho), \quad \forall \rho \in \mathrm{Irrep}(G),$$

where the notation A_ρ is an in (45).

We claim that in this case $f \in \ker(A_\pi)$ for any representation π. Indeed, if $f \in \ker(A_{\pi_1})$ and $f \in \ker(A_{\pi_2})$, then $f \in \ker(A_{\pi_1 \oplus \pi_2})$. Now use the fact that every π is a sum of elements from $\mathrm{Irrep}(G)$.

Taking π to be the G-representation corresponding to $k[G]$, regarded as a module over itself, we obtain that $f \in \ker(A_{k[G]})$. However, by definition, for any $f' \in k[G]$, the element $A_{k[G]}(f') \in \mathrm{End}_k(k[G])$ is takes $f'' \in k[G]$ to $f' \cdot f''$. In particular, taking $f'' = \delta_1$, we have

$$0 = (A_{k[G]}(f))(\delta_1) = f \cdot \delta_1 = f,$$

since δ_1 is the unit in the ring $k[G]$. Hence we conclude that $f = 0$.

□

25.2. **Representations of S_n.**

25.2.1. *Multiplying representations by a character.* Let G be *any* group, π be a G-representation, and $\chi : G \to k^\times$ be a character.

We define a new representation π^χ as follows. It occurs on the same vector space as π. However, the action of G is modified:

$$\phi^\chi(g) = \chi(g) \cdot \phi(g).$$

I.e., we simply multiply the operator $\phi(g)$ by the scalar $\chi(g)$.

Week 12, HW Problem 8. *Show that π is irreducible if and only if π^χ is.*

Week 12, HW Problem 9.

(a) *Let $G = S_3$. Show that* $\mathrm{refl}_0^{\mathrm{sign}}$ *is isomorphic to* refl_0*.*

Hint: compute $\mathrm{Hom}_{S_3}(\mathrm{refl}, \mathrm{refl}_0^{\mathrm{sign}})$ via [Problem 11, Week 11].

(b) *Let $G = S_4$. Show that* $\mathrm{refl}_0^{\mathrm{sign}}$ *is not isomorphic to* refl_0*.*

25.2.2. *Order relation on partitions.* We fix an integer $n > 2$ (the representation theory of the groups $S_1 = \{1\}$ and $S_2 \simeq \mathbb{Z}/2\mathbb{Z}$ is already available to us!) such that $\mathrm{char}(k) \nmid n! = |S_n|$. Note that in positive characteristic this is equivalent to $\mathrm{char}(k) > n$. By a partition, we will mean a partition of n.

Let $\mathfrak{p}^1$ and $\mathfrak{p}^2$ be a partitions. We shall say that $\mathfrak{p}^1 \geq \mathfrak{p}^2$ if (writing $\mathfrak{p}^i = n_1^i \geq n_2^i \geq \cdots$) we have, for every $k \geq 1$,

$$\sum_{j=1}^k n_j^1 \geq \sum_{j=1}^k n_j^2.$$

I.e., if we write $\mathfrak{p}^i$ as a Young diagram, with n_j^i being the height of the j-th column, then $\mathfrak{p}^1 \geq \mathfrak{p}^2$ if for every $k \geq 1$, the number of blocks in the first j columns in $\mathfrak{p}^1$ is at least the number of blocks in the first j columns in $\mathfrak{p}^2$. The point is that we can obtain $\mathfrak{p}^1$ from $\mathfrak{p}^2$ by taking the extra blocks that occur after $\mathfrak{p}^1$ finishes summing up to n and sprinkling them on top of the corresponding columns of $\mathfrak{p}^2$ in a smart way. Alternatively, were the two partitions racing to get up to n, $\mathfrak{p}^1$ would never lose the lead.

The following is elementary:

Lemma 25.2.3. $\mathfrak{p}^1 \leq \mathfrak{p}^2$ *if and only if* $(\mathfrak{p}^1)^\vee \geq (\mathfrak{p}^2)^\vee$.

25.2.4. To a partition $\mathfrak{p} = n_1 + n_2 + \cdots + n_k$ of n we attach a subgroup of S_n:

$$S_{\mathfrak{p}} := S_{n_1} \times S_{n_2} \times \ldots \times S_{n_k}.$$

I.e., $\mathfrak{p}$ divides the set $\{1, \ldots, n\}$ into clusters, and elements of $S_{\mathfrak{p}}$ are those that permute elements within each cluster (or respect this decomposition, so to speak).

Let $\pi_{\mathfrak{p}}$ denote the representation of S_n on $\mathrm{Fun}(S_n/S_{\mathfrak{p}}, k)$. We will prove the following theorem:

Theorem 25.2.5.

(a) *If* $\mathrm{Hom}_{S_n}(\pi_{\mathfrak{p}}, \pi^{\mathrm{sign}}_{\mathfrak{q}^\vee}) \neq 0$*, then* $\mathfrak{p} \leq \mathfrak{q}$*.*

(b) $\dim_k \mathrm{Hom}_{S_n}(\pi_{\mathfrak{p}}, \pi^{\mathrm{sign}}_{\mathfrak{p}^\vee}) = 1$.

25.2.6. Before proving Theorem 25.2.5, we will use it to deduce a classification of irreducible representations of S_n.

Let $\mathfrak{p}$ be a partition. By Corollary 24.2.11, the image of the (unique, up to a scalar) nonzero map

$$\pi_{\mathfrak{p}} \to \pi^{\mathrm{sign}}_{\mathfrak{p}^\vee}$$

is an irreducible representation. Denote this representation by $\rho_{\mathfrak{p}}$.

Week 12, HW Problem 10. *Assuming Theorem 25.2.5, show that* $\rho^{\mathrm{sign}}_{\mathfrak{p}} \simeq \rho_{\mathfrak{p}^\vee}$*.*

We claim:

Theorem 25.2.7.

(a) *The representations* $\rho_{\mathfrak{p}}$ *are pairwise nonisomorphic.*

(b) *Every irreducible representation of* S_n *is isomorphic to* $\rho_{\mathfrak{p}}$ *for a unique* $\mathfrak{p}$*.*

(c) *Write*

$$\pi_{\mathfrak{p}} \simeq \bigoplus_{\mathfrak{p}'} \underbrace{\rho_{\mathfrak{p}'} \oplus \ldots \oplus \rho_{\mathfrak{p}'}}_{n_{\mathfrak{p}'}}.$$

Then $n_{\mathfrak{p}} = 1$*, and if* $n_{\mathfrak{p}'} \neq 0$*, then* $\mathfrak{p}' \geq \mathfrak{p}$*.*

Proof. To prove point (a), suppose that $\rho_{\mathfrak{p}_1} \simeq \rho_{\mathfrak{p}_2}$. We obtain a non-zero map

$$\pi_{\mathfrak{p}_1} \twoheadrightarrow \rho_{\mathfrak{p}_1} \simeq \rho_{\mathfrak{p}_2} \hookrightarrow \pi^{\mathrm{sign}}_{\mathfrak{p}_2^\vee}.$$

Hence, by Theorem 25.2.5(a), we have $\mathfrak{p}_1 \leq (\mathfrak{p}_2^\vee)^\vee = \mathfrak{p}_2$.

Symmetrically, we obtain that $\mathfrak{p}_2 \leq \mathfrak{p}_1$. Hence, $\mathfrak{p}_1 = \mathfrak{p}_2$.

Point (b) of the theorem follows from point (a), combined with [Problem 5] and Corollary 24.3.8.

Let us prove point (c). The fact that the multiplicity of $\rho_{\mathfrak{p}}$ in $\pi_{\mathfrak{p}}$ is one follows from 25.2.5(b) and Corollary 24.2.9. Assume that the multiplicity of $\rho_{\mathfrak{p}'}$ on $\pi_{\mathfrak{p}}$ is non-zero. We obtain that

$$\mathrm{Hom}_{S_n}(\pi_{\mathfrak{p}}, \pi^{\mathrm{sign}}_{(\mathfrak{p}')^\vee}) \neq 0.$$

By 25.2.5(a), we obtain that $\mathfrak{p} \leq \mathfrak{p}'$, as desired.

□

25.3. **Proof of Theorem 25.2.5.**

25.3.1. The idea is to apply [Problem 11, Week 11]. That is to say, we will calculate

$$\left(\mathrm{Fun}(S_n/S_{\mathfrak{q}^\vee},k)^{\mathrm{sign}}\right)^{S_{\mathfrak{p}}}, \tag{49}$$

and we will show that it is non-zero only when $\mathfrak{p} \leq \mathfrak{q}$ and one-dimensional when $\mathfrak{p} = \mathfrak{q}$.

We will deduce this from the following combinatorial statement:

Proposition 25.3.2.

(a) *Suppose that $\mathfrak{p} \not\leq \mathfrak{q}$. Then for every $g \in S_n$ there exists a transposition $\sigma_{i,j} \in S_{\mathfrak{p}}$ such that $\sigma_{i,j} \cdot g = g \cdot h$ for $h \in S_{\mathfrak{q}^\vee}$.*

(b) *Suppose that $\mathfrak{p} = \mathfrak{q}$. Then there exists a unique $S_{\mathfrak{p}}$ orbit $\mathbf{O} \in S_n/S_{\mathfrak{p}^\vee}$, such that:*

(i) *The action of $S_{\mathfrak{p}}$ on $\mathbf{O}$ is simple (see Sect. 20.5.1).*

(ii) *For every $g \in S_n$ such that $\bar{g} \in S_n/S_{\mathfrak{p}^\vee}$ does not belong to $\mathbf{O}$, there exists a transposition $\sigma_{i,j} \in S_{\mathfrak{p}}$ such that $\sigma_{i,j} \cdot g = g \cdot h$ for $h \in S_{\mathfrak{p}^\vee}$.*

Let us deduce Theorem 25.2.5 from Proposition 25.3.2.

Proof. Suppose $\mathfrak{p} \not\leq \mathfrak{q}$. Let f be an element in $\mathrm{Fun}(S_n/S_{\mathfrak{q}^\vee},k)$ that is invariant with respect to $S_{\mathfrak{p}}$ under the usual action twisted by sign. We need to show that $f = 0$, i.e., that $f(\bar{g}) = 0$ for every $g \in S_n$.

So fix such a $g \in S_n$. Let $\sigma_{i,j}$ be as in Proposition 25.3.2(a) — that is, so that $\sigma_{i,j} \cdot g \equiv g \pmod{S_{\mathfrak{q}^\vee}}$. Observe that, by $S_{\mathfrak{p}}$-invariance, we have that

$$\mathrm{sign}(\sigma_{i,j}) \cdot f^{\sigma_{i,j}} = f.$$

Let's evaluate this equality on $\bar{g}$. We get:

$$-f(\overline{\sigma_{i,j} \cdot g}) = f(\bar{g}).$$

But by definition

$$\overline{\sigma_{i,j} \cdot g} = \bar{g}.$$

Hence $f(\bar{g}) = 0$. (This because $n > 2$ so $\mathrm{char}\, k \neq 2$.)

Suppose now that $\mathfrak{p} = \mathfrak{q}$. Let f be an element in $\mathrm{Fun}(S_n/S_{\mathfrak{p}^\vee},k)$, which is invariant with respect to $S_{\mathfrak{p}}$, where the action is the natural action, multiplied by the sign character. Immediately we claim that the value of f on $\bar{g} \notin \mathbf{O}$ is zero. The proof is the same as above, now using point b.ii of Proposition 25.3.2 instead.

Now we claim that there exists a unique (up to scalar) nonzero $S_{\mathfrak{p}}$-invariant function f on $\mathbf{O}$. Indeed, choosing any point $x \in \mathbf{O}$, since the action of $S_{\mathfrak{p}}$ is simply transitive, the map

$$g \mapsto g \cdot x$$

defines an isomorphism $S_{\mathfrak{p}} \to \mathbf{O}$. If $f(x) = 1$, then the value of f at any other point of $\mathbf{O}$ is given by the formula

$$f(g \cdot x) = \mathrm{sign}(g).$$

(For uniqueness, observe that, were $f(x) = 0$, we would find that $f = 0$ identically. Hence f is specified entirely by its value on x.)

□

25.3.3. It remains to prove Proposition 25.3.2. (What follows will require the use of your imagination. So get ready to think!)

25.3.4. Let us call an element $g \in S_n$ "good" if there *does not exists* of a permutation $\sigma_{i,j} \in S_{\mathfrak{p}}$ such that

$$\sigma_{i,j} \cdot g = g \cdot h, \quad h \in S_{\mathfrak{q}^\vee}.$$

Let X denote the set $\{1, ..., n\}$, and we regard $\mathfrak{q}^\vee$ and $\mathfrak{p}$ as two ways to represent it as a disjoint union of subsets

$$\underset{i}{\sqcup} X'_i \simeq X \simeq \underset{j}{\sqcup} X''_j.$$

An element $g \in S_n$ is an automorphism of X.

25.3.5. Let is view the union $\underset{i}{\sqcup} X'_i$ as a set X', and the union $\underset{j}{\sqcup} X''_j$ as a set X'', and let view the element g as an isomorphism of sets $\Phi : X' \to X''$. We will view the decomposition

$$X' = \underset{i}{\sqcup} X'_i$$

as a partition according to $\mathfrak{q}^\vee$, where the blocks are positioned horizontally. We will view the decomposition

$$X'' = \underset{j}{\sqcup} X'_j$$

as a partition according to $\mathfrak{p}$, where the blocks are positioned vertically. Note that the latter can also be thought as a partition according to $\mathfrak{p}^\vee$, where the blocks are positioned horizontally.

Let us call a map $\Phi : X' \to X''$ "good" if for every row $X'_i \subset X'$, its elements get sent by means of Φ to elements of X'' having distinct latitudes.

It is easy to see that "goodness" of $g \in S_n$ is equivalent to the "goodness" of the corresponding map Φ.

Furthermore, multiplication of g on the left (resp., right) by an element of $S_{\mathfrak{p}}$ (resp., $S_{\mathfrak{q}}$) corresponds to composing (resp., pre-composing) Φ with an automorphism of X'' (resp., X') that acts along the columns (resp., rows).

25.3.6. Let us call an element $\Phi : X' \to X''$ "superb" if it is "good", and the following additional condition holds:

For every index i (numbering the rows in X') and every $x' \in X'_i$, the element $\Phi(x')$ is such that all elements underneath it in its column in X'' *are of the form $\Phi(\widetilde{x}')$ for $\widetilde{x}' \in X'_{\widetilde{i}}$ with $\widetilde{i} < i$.*

We have:

Lemma 25.3.7. *For a given "good" map Φ there exists a unique element $h'' \in S_{\mathfrak{p}}$ such that the map*

$$\Phi_s := h'' \circ \Phi$$

is "superb."

The proof of the lemma is given below. Let us assume it, and finish the proof of the proposition.

25.3.8. Let us prove point (a) of the proposition. We need to show that if there exists a good map $\Phi : X' \to X''$, then $\mathfrak{p}^\vee \geq \mathfrak{q}^\vee$, i.e., that for every i, the volume of the first i rows of X' is $\leq$ than the volume of the first i *rows* of X''.

By Lemma 25.3.7, with no restriction of generality, we can assume that Φ is "superb." However, for a"superb" map, the first i rows of X' get sent to the first i rows of X''. Hence, our assertion follows from the pigeonhole principle.

25.3.9. Let us prove point (b) of the proposition. In this case X' and X'' have the same shape, and there exists a distinguished "good" map $\Phi_0 : X' \to X''$, namely the identity map. We need to show that every other "good" Φ can be uniquely written as

$$h'' \circ \Phi_0 \circ h'$$

where h'' acts along the columns of X'' and h' acts along the rows of X'.

By Lemma 25.3.7, with no restriction of generality, we can assume that Φ is "superb." In this we need to show that Φ can be uniquely written as

$$\Phi_0 \circ h',$$

where h' acts along the rows of X'.

However, for X' and X'' having the same shape, a "superb" map sends the ith row of X' bijectively to the ith row of X'', and the assertion is manifest.

□

Proof of Lemma 25.3.7. We define the map Φ_s (and hence the corresponding element h'') inductively on i. Suppose that Φ_s has been defined on the rows $X'_1 \sqcup \ldots \sqcup X'_{i-1}$. With no restriction of generality, we can assume that Φ and Φ_s are equal on the above rows.

For every element $x \in X_i$ consider the transposition $\sigma_x \in S_\mathfrak{p}$ along the column to which $\Phi(x)$ belongs, that puts it in the *lowest position not occupied by elements* $\Phi(\widetilde{x}')$ *for* $\widetilde{x}' \in X'_{\widetilde{i}}$ *with* $\widetilde{i} < i$.

We define Φ_s on X_i by

$$\left(\underset{x \in X_i}{\Pi} \sigma_x\right) \cdot \Phi.$$

Note that the order of the product in $\underset{x \in X_i}{\Pi} \sigma_x$ does not matter, because the "goodness" of Φ implies that all of the σ_x's act along distinct columns, and hence, commute.

The resulting element Φ_s satisfies the condition of being superb on the first i rows bu construction. The uniquness of Φ_s also follows from the construction.

□

26. Final Exam

Problem 1. 5pts. Let G be a finite group, and let $\pi = (V, \phi : G \to GL(V))$ be a finite-dimensional representation of G over the field $\mathbb{C}$. Show that there exists a (positive-difinite) inner form $(-,-)$ on V, which is G-invariant, i.e. such that $(g \cdot v_1, g \cdot v_2) = (v_1, v_2)$ for any $v_1, v_2 \in V$ and $g \in G$.

Hint: use averaging.

Problem 2. 5pts. Let R be a ring and $M_1, ..., M_k$ be irreducible pairwise non-isomorphic R-modules. Let N be an R-module, and T a map

$$N \to M_1 \oplus \ldots \oplus M_k.$$

Assume that for every $i = 1, ..., k$, the composition

$$N \to M_1 \oplus \ldots \oplus M_k \to M_i$$

is surjective. Show that the initial map T is surjective.

Problem 3. 5pts. Let A be a finite abelian group, and k an algebraically closed field of characteristic prime to $|A|$. Let $\widehat{A} := \mathrm{Char}(A, k)$ denote the set of characters $A \to k^\times$.

(a) 2pts. Consider the map of vector spaces

$$\Phi : \mathrm{Fun}(A, k) \to \mathrm{Fun}(\widehat{A}, k)$$

defined as follows. It sends a function f on A to the function $\Phi(f)$ on $\widehat{A}$ whose value on a character $\chi \in \widehat{A}$ is

$$\sum_{a \in A} \chi(a) \cdot f(a).$$

Show that Φ is an isomorphism of vector spaces.

(b) 2pts. Show that the map Φ sends a character χ, viewed as a function on A with values in k, i.e., an element of $\mathrm{Fun}(A, k)$ to

$$|A| \cdot \delta_{\chi^{-1}} \in \mathrm{Fun}(\widehat{A}, k),$$

where χ^{-1} is the character obtained from χ by taking inverse values, and $\delta_{\chi^{-1}}$ is Kronecker's δ at χ^{-1}.

(c) 1pt. Deduce that the characters of A, viewed as functions on A, form a basis of $\mathrm{Fun}(A, k)$.

Problem 4. 5pts. Let A be as in Problem 3. We consider the set $\widehat{A}$ as an abelian group via the operation of product of characters:

$$(\chi_1 \cdot \chi_2)(a) := \chi_1(a) \cdot \chi_2(a).$$

Consider the map of sets $A \to \widehat{\widehat{A}}$ that sends $a \in A$ to the character

$$\widehat{A} \to k^\times, \quad \chi \mapsto \chi(a).$$

(a) 1pt. Show that the above map $A \to \widehat{\widehat{A}}$ is a group homomorphism.

(b) 4pts. Show that the above map $A \to \widehat{\widehat{A}}$ is an isomorphism.

Problem 5. Bonus 10pts. Let G_1 and G_2 be finite groups, and k an algebraically closed field with $\mathrm{char}(p) \nmid |G_1|$, $\mathrm{char}(p) \nmid |G_2|$. For a representation $\pi_1 = (V_1, \phi_1)$ of G_1 and a representation $\pi_2 = (V_2, \phi_2)$ of G_2 consider the representation $\underline{\underline{\mathrm{Hom}}}_{G_1 \times G_2}(\pi_1, \pi_2)$ of $G_1 \times G_2$ on the vector space $\mathrm{Hom}_k(V_1, V_2)$ defined by

$$T^{g_1, g_2} = \phi_2(g_2) \cdot T \circ \phi_1(g_1^{-1}), \quad T : V_1 \to V_2$$

Show that if π_1 and π_2 are irreducible, then so is $\underline{\underline{\mathrm{Hom}}}_{G_1\times G_2}(\pi_1,\pi_2)$, and that if (π_1,π_2) and (π_1',π_2') are two such pairs (all reps are irredicuble) then

$$\underline{\underline{\mathrm{Hom}}}_{G_1\times G_2}(\pi_1,\pi_2)\simeq \underline{\underline{\mathrm{Hom}}}_{G_1\times G_2}(\pi_1',\pi_2')$$

if and only if $\pi_1\simeq\pi_1'$ and $\pi_2\simeq\pi_2'$.

27. Solutions of the final

27.1. **Problem 1.** Choose any inner form $(-,-)$ on V and define

$$(v_1,v_2)':=\sum_{g\in G}(g\cdot v_1,g\cdot v_2).$$

Then it is easy to see that $(-,-)'$ has all the required properties.

27.2. **Problem 2.** By induction on k, we can assume that the composed map (denote it T')

$$N\to M\to M/M_k\simeq M_1\oplus ...\oplus M_{k-1}$$

is surjective.

Consider $N':=\ker(T')$, and consider the restriction of the map T to N', call it T''. By definition, T'' is a map from $N'\to M_k$.

Claim: $T''\neq 0$.

Proof. Assume the contrary. Then $T|_{N'}=0$. We obtain that T factors as

$$N\to N/N'\to M,$$

where the resulting map $S:N/N'\to M$ inherits the property that its composition with each projection $\pi_i:M\to M_i$ is surjective.

However,

$$N/N'\simeq\mathrm{Im}(T')\simeq M_1\oplus ...\oplus M_{k-1}.$$

In particular, we obtain that S yields a surjective map

$$M_1\oplus ...\oplus M_{k-1}\to M_k,$$

which contradicts the assumption that $M_i\neq M_k$ for $i<k$.

□

We obtain a map of short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & N' \arrow[r] \arrow[d, "T''"'] & N \arrow[r] \arrow[d, "T"'] & N/N' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M_k \arrow[r] & M \arrow[r] & M_1\oplus ...\oplus M_{k-1} \arrow[r] & 0
\end{tikzcd}$$

where the right vertical arrow is surjective (in fact, isomorphism), and the left vertical arrow non-zero, and hence surjective since M_k is irreducible.

Hence, T is surjective.

27.3. **Problem 3.**

27.3.1. *Part (a).* Follows immediately from [Probem 10, Week 11] and from Step 3 of the proof of Theorem 24.3.4.

Alternatively, the two sides have the same dimension by Corollary 24.3.10. So, isomorphism is equivalent to surjectivity, which is proved in part (b) below.

27.3.2. *Part (b).* The fact that the value of $\Phi(\chi)$ at χ^{-1} is $|A|$ is immediate. The fact that it vanishes at any other character follows from the next claim:

Claim: *If G is a finite group and $\chi : G \to k^*$ a* non-trivial *character, then* $\underset{g\in G}{\Sigma} \chi(g) = 0$.

Proof. Let $g_0 \in G$ be such that $\chi(g_0) \neq 1$. Then

$$\chi(g_0) \cdot (\underset{g\in G}{\Sigma} \chi(g)) = \underset{g\in G}{\Sigma} \chi(g_0) \cdot \chi(g) = \underset{g\in G}{\Sigma} \chi(g_0 \cdot g) = \underset{g\in G}{\Sigma} \chi(g),$$

where the latter equality holds by re-indexing.

□

Hence,

$$(\chi(g_0) - 1) \cdot (\underset{g\in G}{\Sigma} \chi(g)) = 0,$$

implying the desired.

27.3.3. *Part (c).* From (b), we obtain that the characters of A, regarded as elements of $\text{Fun}(A, k)$ get mapped by means of Φ to a basis of $\text{Fun}(\widehat{A}, k)$. By (a), the map Φ is an isomorphism. Hence, the characters of A were a basis of $\text{Fun}(A, k)$.

27.4. **Problem 4.** Part (a) is straightforward.

To prove part (b), we note that both groups have the same order. So, it is enough to show that the map in question is injective. The latter says that if $a \in A$ is such that $\chi(a) = 1$ for all characters χ, then $a = 1$.

However, for such a, we have $\delta_a - \delta_1 \in \ker(\Phi)$, where Φ is from Problem 3. Since Φ is injective, we are done.