Graduate Algebra

1. Preliminaries

1.1. Notations

We reserve the following letters:

- $\mathbb{N}$ for the set of *natural numbers* $0, 1, 2, \ldots$
- $\mathbb{Z}$ for the set of *integers*, i.e. for all $\pm n$ for $n \in \mathbb{N}$
- $\mathbb{Q}$ for the set of *rational numbers* m/n for $m, n \in \mathbb{Z}$ with $n \neq 0$
- $\mathbb{R}$ for the set of *real numbers*, and
- $\mathbb{C}$ for the set of *complex numbers* $a + bi$ for $a, b \in \mathbb{R}$.

2. Recollection of some algebra

In this first lecture, I want to recall some of the main objects of study in algebra, including: groups, rings and fields. Ultimately, the goal today is to prove an analogue of Cayley's Theorem - see Theorem 2.5.1 and Theorem 2.6.1 about embedding arbitrary groups in some standard groups.

2.1. Groups

Recall that a group is a set G together with a binary operation $\cdot : G \times G \to G$ satifsying the following:

- associativity: $\forall x, y, z \in G, (xy)z = x(yz)$
- identity: $\exists e \in G, xe = ex = x$.
- inverses: $\forall x \in G, \exists y \in G, xy = yx = 1$.

Remark:

a. We usually write 1 or sometimes 1_G rather than e for the inverse element of G.
b. we usually write x^{-1} for the inverse of $x \in G$
c. A group is abelian if $\forall a, b \in G, ab = ba$
d. Sometimes we write groups additively; in that case, 0 is the identity element and and the inverse of $a \in G$ is $-a \in G$. We always insist that additive groups are abelian.

Definition 2.1.1: For groups G and H, a function $\varphi : G \to H$ is a group homomorphism provided that $\forall x, y \in G, \varphi(xy) = \varphi(x)\varphi(y)$.

Definition 2.1.2: Let $\varphi : G \to H$ be a group homomorphism. The kernel of φ is

$$\ker \varphi = \{g \in G \mid \varphi(g) = 1.\}$$

Remark: If $\varphi : G \to H$ is a group homomorphism, $\ker \varphi$ is a subgroup of G – i.e. $\ker \varphi$ is non-empty, and is closed under multiplication and under taking inverses.

Proposition 2.1.3: Let $\varphi : G \to H$ be a group homomorphism. Then φ is an injective (or one-to-one) function if and only if $\ker \varphi = \{1_G\}$.

2.2. Rings

Definition 2.2.1: A ring is an additive abelian group R together with a binary operation of multiplication

$$\cdot : R \times R \to R$$

which satisfies the following:

- multiplication is associative: $\forall a, b, c \in R, (ab)c = a(bc)$.
- there is a multiplicative identity: $\exists 1 \in R, \forall a \in R, 1a = a1 = a$.
- distribution laws: $\forall a, b, c \in R, a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

The ring R is commutative provided that $\forall a, b \in R, ab = ba$.

Example 2.2.2:

a. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings.
b. For a natural number $n > 1$, the ring $\mathrm{Mat}_n(\mathbb{Z})$ of $n \times n$ matrices with coefficients in $\mathbb{Z}$ is a non-commutative ring.

Definition 2.2.3: For a commutative ring R, an element $a \in R$ is a unit provided that $\exists v \in R, uv = vu = 1$.

The set $R^\times$ of units in R is a group under the multiplication of R.

2.3. Fields

Definition 2.3.1: A field is a commutative ring F such that $\forall a \in F, a \neq 0 \Rightarrow a$ is a unit.

Example 2.3.2: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field.

2.4. Linear Algebra

Definition 2.4.1: If F is a field, a vector space over F – or an F-vector space – is an additive abelian group V together with an operation of scalar multiplication

$$F \times V \to V$$

written $(t, v) \mapsto tv$, subject to the following:

- identity: $\forall v \in V, 1v = v$.
- associativity: $\forall a, b \in F$ and $v \in V, a(bv) = (ab)v$.
- distributive laws: $\forall a, b \in F$ and $v, w \in V, (a + b)v = av + bv$ and $a(v + w) = av + aw$.

Remark: Probably in a linear algebra class you saw results stated for vector spaces over $\mathbb{R}$ or $\mathbb{C}$; however, "most" results in linear algebra remain valid for vector space over F.

Example 2.4.2: Let I be any set, and let V be the set of all functions $f : I \to F$ which have finite support. Recall that the support of f is $\{x \in I \mid f(x) \neq 0\}$.

Then V is a vector space. (The addition and scalar multiplication operations are define "pointwise" – see homework.)

Remark: Recall that a basis of a vector space is subset B of V which is linearly indepent and spans V.

The vector space of finitely supported functions $I \to F$ has a basis $B = \{\delta_i \mid i \in I\}$, where

$$\delta_i : I \to F$$

is the function defined by $\delta_i(j) = 0$ if $i \neq j$ and $\delta_i(i) = 1$.

Definition 2.4.3: If V and W are F-vector spaces, an F-linear map $\varphi : V \to W$ is a homomorphism of additive groups which satisfies the condition

$$\forall t \in F, \forall v \in V, \varphi(tv) = t\varphi(v).$$

Definition 2.4.4: If V is an F-vector space, the general linear group $\mathrm{GL}(V)$ is the set

$$\{\varphi : V \to V \mid \varphi \text{ is } F\text{-linear and invertible.}\}$$

$\mathrm{GL}(V)$ is a group whose operation is given by composition of linear transformations.

Remark: If V is finite dimensional, so that V is isomorphic to F^n as F-vector spaces, linear algebra shows that $\mathrm{GL}(V)$ is isomorphic to the group GL_n of $n \times n$ matrices with non-zero determinant, where $n = \dim_F V$ and where the operation in GL_n is given by matrix multiplication.

2.5. Cayley's Theorem

Let Ω be any set. The set $S(\Omega)$ of all bijective functions $\psi : \Omega \to \Omega$ is a group whose operation is composition of functions.

Theorem 2.5.1 (Cayley's Theorem): Let G be any group. Then G is isomorphic to a subgroup of $S(\Omega)$ for some Ω.

Proof: Let $\Omega = G$. For $g \in G$, define a mapping $\lambda_g : G \to G$ by the rule

$$\lambda_g(h) = gh.$$

We are going to argue that the mapping $g \mapsto \lambda_g$ defines an injective group homomorphism $G \to S(\Omega) = S(G)$.

First of all, we note that $\lambda_1 = \mathrm{id}$. Indeed, to check this identity of functions, let $h \in \Omega = G$. Then

$$\lambda_1(h) = 1h = h = \mathrm{id}(h);$$

this confirms $\lambda_1 = \mathrm{id}$.

Next, we note that for $g_1, g_2 \in G$, we have $(*) \quad \lambda_{g_1} \circ \lambda g_2 = \lambda_{g_1 g_2}$. Again, to confirm this identify of functions, we let $h \in \Omega = G$. Then

$$\big(\lambda_{g_1} \circ \lambda_{g_2}\big)h = \lambda_{g_1}\big(\lambda_{g_2}(h)\big)) = \lambda_{g_1}(g_2 h) = g_1(g_2 h) = (g_1 g_2)h = \lambda_{g_1 g_2}(h)$$

as required.

Now, using $(*)$ we see for $g \in G$ that $\lambda_g \circ \lambda_{g^{-1}} = \lambda_1 = \mathrm{id} = \lambda_{g^{-1}} \circ \lambda_g$, which proves that λ_g is bijective; thus indeed $\lambda_g \in S(\Omega) = S(G)$.

Moreover, $(*)$ shows that the mapping $\lambda : G \to S(G)$ given by $g \mapsto \lambda_g$ is a group homomorphism.

It remains to see that λ is injective. If $g \in \ker \lambda$, then $\lambda_g = \mathrm{id}$. Thus $1 = \mathrm{id}(1) = \lambda_g(1) = g1 = g$. Thus $g = 1$ so that $\ker \lambda = \{1\}$ which confirms that λ is injective by Proposition 2.1.3. This completes the proof. ■

2.6. A linear analogue of Cayley's Theorem.

Let F be a field.

Theorem 2.6.1: Let G be any group. Then G is isomorphic to a subgroup of $\mathrm{GL}(V)$ for some F-vector space V.

Proof: The proof is quite similar to the proof of Cayley's Theorem.

Let V be the vector space of all finitely supported functions $f : G \to F$. Recall that V has a basis $B = \{\delta_g \mid g \in G.\}$

We are going to define an injective group homomorphism $G \to \mathrm{GL}(V)$.

For $g \in G$, we may define an F-linear mapping $\lambda_g : V \to V$ by defining the value of λ_g at each vector in B. We set $\lambda_g(\delta_h) = \delta_{gh}$.

Recall that a typical element v of V has the form

$$v = \sum_{i=1}^{n} t_i \delta_{h_i}$$

for scalars $t_i \in F$ and elements $g_i \in G$; since λ_g is F-linear, we have

$$\lambda_g(v) = \sum_{i=1}^{n} t_i \delta_{g h_i}.$$

We now show that $\lambda_1 = \mathrm{id}$. To prove this, since the functions $V \to V$ are linear, it is enough to argue that the functions agree at each element of the basis B of V. Well, for $h \in G$,

$$\lambda_1(\delta_h) = \delta_{1h} = \delta_h = \mathrm{id}(\delta_h)$$

as required.

We next show for $g_1, g_2 \in G$ that $(*)$ $\lambda_{g_1} \circ \lambda_{g_2} = \lambda_{g_1 g_2}$. Again, it suffices to argue that these functions agree at each element δ_h of B. For $h \in G$ we have:

$$\left(\lambda_{g_1} \circ \lambda_{g_2}\right)(\delta_h) = \lambda_{g_1}\left(\lambda_{g_2}\delta_h\right) = \lambda_{g_1}\left(\delta_{g_2 h}\right) = \delta_{g_1(g_2 h)} = \delta_{(g_1 g_2)h} = \lambda_{g_1 g_2}\delta_h$$

as required.

Now, for $g \in G$ we see that by $(*)$ that

$$\mathrm{id} = \lambda_1 = \lambda_g \circ \lambda_{g^{-1}}$$

which proves that λ_g is invertible and hence in $\mathrm{GL}(V)$.

Moreover, $(*)$ shows that the assignment $\lambda : G \to \mathrm{GL}(V)$ given by the rule $g \mapsto \lambda_g$ is a group homomorphism.

It remains to argue that λ is injective. Suppose that $x \in \ker \lambda$, so that $\mathrm{id} = \lambda_x$.

Then $\delta_1 = \mathrm{id}(\delta_1) = \lambda_x(\delta_1) = \delta_{x1} = \delta_x$. This implies that $1 = x$ so that indeed the kernel of λ is trivial and thus λ is injective by Proposition 2.1.3.

■

3. Quotients

3.1. The Quotient of a set by an equivalence relation

Let S be a set and let R be a relation on S. Formally, R is an assignment $R : S \times S \to \text{Prop}$ – in other words, for $a, b \in S$, $R(a,b)$ is the proposition that a and b are related; of course $R(a,b)$ may or may not hold. We often use a symbol $\sim$ or $\underset{R}{\sim}$ to indicate this proposition; thus $R(a,b) \Leftrightarrow a \underset{R}{\sim} b$. We often refer to the relation using the symbol $\underset{R}{\sim}$ or simply $\sim$ rather than R.

Definition 3.1.1: The relation $\sim$ is an equivalence relation if the following properties hold:

- reflexive: $\forall s \in S, s \sim s$.
- symmetric: $\forall s_1, s_2 \in S, s_1 \sim s_2 \Rightarrow s_2 \sim s_1$
- transitive: $\forall s_1, s_2, s_3 \in S, s_1 \sim s_2$ and $s_2 \sim s_3 \Rightarrow s_1 \sim s_3$

Definition 3.1.2: If $\sim$ is an equivalence relation on the set S, a quotient of S by $\sim$ is a set $\bar{S}$ together with a surjective function $\pi : S \to \bar{S}$ with the following properties:

(Quot 1) $\forall a, b \in S, a \sim b \Rightarrow \pi(a) = \pi(b)$

(Quot 2) Let T be any set and let f be any function $f : S \to T$ such that $\forall a, b \in S, a \sim b \Rightarrow f(a) = f(b)$. Then there is a function $\bar{f} : S \to T$ for which $f = \bar{f} \circ \pi$.

Proposition 3.1.3: Suppose that $\left(\bar{S}_1, \pi_1\right)$ and $\left(\bar{S}_2, \pi_2\right)$ are two quotients of the set S by the equivalence relation $\sim$. Let

$$\bar{\pi_2} : \bar{S}_1 \to \bar{S}_2$$

be the mapping determined by the quotient property for $\left(\bar{S}_1, \pi_1\right)$ using

$$T = \bar{S}_2 \quad \text{and} \quad f = \pi_2 : S \to \bar{S}_2,$$

and let

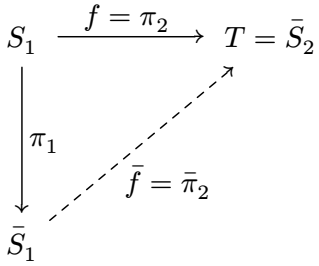
$$\bar{\pi}_1 : \bar{S}_2 \to \bar{S}_1$$

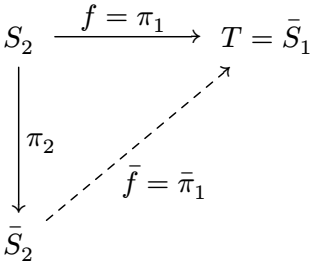
be the mapping determined by the quotient property for $\left(\bar{S}_2, \pi_2\right)$ using

$$T = \bar{S}_1 \quad \text{and} \quad f = \pi_1 : S \to \bar{S}_2.$$

Then the maps $\pi_2' : \bar{S}_1 \to \bar{S}_2$ and $\pi_{1'} : \bar{S}_2 \to \bar{S}_1$ are inverse to one another, and in particular π_1' and π_2' are bijections.

Proof: By the definition of quotients, we have commutative diagrams





In particular, we have $\pi_2 = \bar{\pi}_2 \circ \pi_1$ and $\pi_1 = \bar{\pi}_1 \circ \pi_2$

Substitution now yields

$$\pi_1 = \bar{\pi}_1 \circ \bar{\pi}_2 \circ \pi_1$$

and

$$\pi_2 = \bar{\pi}_2 \circ \bar{\pi}_1 \circ \pi_2$$

Since π_1 and π_2 are surjective, we conclude that $\mathrm{id} = \bar{\pi}_1 \circ \bar{\pi}_2$ and $\mathrm{id} = \bar{\pi}_2 \circ \bar{\pi}_1$ so indeed the indicated functions are inverse to one another. ■

Remark: The point of the Proposition is that a quotient is completely determined by the property indicated in the definition – this property is an example of what is known as a universal property or sometimes as a universal mapping property. The conclusion of the Proposition shows that any two ways of constructing a quotient are equivalent in a strong sense.

One way of constructing the quotient is by considering equivalence classes, as follows:

Definition 3.1.4: For an equivalence relation $\sim$ on a set S, the equivalence class $[s]$ of an element $s \in S$ is the subset of S defined by

$$[s] = \{x \in S \mid x \sim s\}.$$

Proposition 3.1.5: Equivalence classes for the equivalence relation $\sim$ have the following properties for arbitrary $s, s' \in S$:

a. $s \sim s' \Leftrightarrow [s] = [s']$
b. $[s] \neq [s'] \Leftrightarrow [s] \cap [s'] = \emptyset$

Proof: Review! ■

Theorem 3.1.6 (*Existence of quotients*): For any equivalence relation $\sim$ on a set S, there is a quotient $\left(\bar{S}, \pi\right)$.

Proof: We consider the set $\bar{S} = \{[s] \mid s \in S\}$ of equivalence classes and the mapping $\pi : S \to \bar{S}$ given by the rule $\pi(s) = [s]$.

Proposition 3.1.5 confirms condition (a) of Definition 3.1.2.

For condition (b) of Definition 3.1.2 suppose that T is a set and that $f : S \to T$ is a function with the property that $\forall a, b \in S, a \sim b \Rightarrow f(a) = f(b)$. We must exhibit a function $\bar{f} : \bar{S} \to T$ with the property $f = \bar{f} \circ \pi$. If $\bar{f}$ exists, it must satisfy $\bar{f}([a]) = a$ for $a \in S$. On the other hand, in view of Proposition 3.1.5 (a), the rule $[a] \mapsto f(a)$ indeed determines a well-defined function $\bar{f} : \bar{S} \to T$. Moreover, the identity $f = \bar{f} \circ \pi$ evidently holds.

■

3.2. Examples of quotients