Math 361 lecture for Monday, Week 2

Algebraic numbers

Definition 1. The set of *algebraic numbers* is

$$\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

Example 2. Note that if $a \in \mathbb{Q}$, then a is a zero of the polynomial $x - a \in \mathbb{Q}[x]$. Hence, $\mathbb{Q} \subset \mathbb{A}$. Other algebraic numbers in include $\sqrt{2}$, $\sqrt[3]{5}$, and the complex n-roots of unity, $e^{2k\pi i/n}$ for $n \geq 1$ and $k = 0, \ldots, n$. These are the solutions to $x^n - 1$. Non-algebraic numbers are called *transcendental* numbers and include e and π, for example.

Proposition 3. $\mathbb{A}$ is a field.

Proof. It suffices to show that $\mathbb{A}$ is closed under addition and multiplication and that every nonzero element of $\mathbb{A}$ has a multiplicative inverse.

Let $\alpha, \beta \in \mathbb{A}$. Since α is algebraic over $\mathbb{Q}$, we saw in the last lecture that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite. Further, since β is algebraic over $\mathbb{Q}$, there is a polynomial p with coefficients in $\mathbb{Q}$ such that $p(\beta) = 0$. Regarding p as an element of $\mathbb{Q}(\alpha)[x]$, shows that β is algebraic over $\mathbb{Q}(\alpha)$. Therefore, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ is finite. It follows that

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha), \mathbb{Q}] < \infty.$$

Since $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] < \infty$, every element of $\mathbb{Q}(\alpha, \beta)$ is in $\mathbb{A}$. In particular, $\alpha + \beta$ and $\alpha\beta$ are algebraic numbers, and if $\alpha \neq 0$, then α^{-1} is an algebraic number. $\square$

Definition 4. A *number field* is a subfield $K \subseteq \mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$.

Theorem 5. (Primitive element theorem) If K is a number field, then there exists an algebraic number θ such that $K = \mathbb{Q}(\theta)$.

Proof. See our text, Theorem 2.2. $\square$

Our next goal is to fill in the box in the following diagram:

$$\begin{array}{ccc} K & — & \boxed{} \\ | & & | \\ \mathbb{Q} & — & \mathbb{Z} \end{array}\ .$$

In other words, we want to find a ring inside of K that plays the role of the ring of integers inside $\mathbb{Q}$. It will help to first discuss an algebraic structure called a *module*.

Modules. Roughly, a module is a vector space except that the scalars are elements of a ring rather than a field.

Definition 6. Let R be a ring. An *R-module* or *module over* R is an abelian group M and an operation

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto rm \end{aligned}$$

such that for all $r, s \in R$ and $m, n \in M$

- $(r + s)m = rm + sm$,
- $r(m + n) = rm + rn$,
- $r(sm) = (rs)m$, and
- $1 \cdot m = m$.

Example 7.

(a) If R is a field, then R-modules are exactly vector spaces over R.

(b) $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$ module (if $a \in \mathbb{Z}$ and $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$, then $a\bar{b} := \overline{ab} \in \mathbb{Z}/n\mathbb{Z}$).

(c) Let R be a ring, and let n be a positive integer. Define

$$R^n := \{(r_1, \ldots, r_n) : r_i \in R\},$$

the Cartesian product of R with itself n times. Then R^n is an R-module via

$$\begin{aligned} r(r_1, \ldots, r_n) &:= (rr_1, \ldots, rr_n) \\ (r_1, \ldots, r_n) + (s_1, \ldots, s_n) &:= (r_1 + s_1, \ldots, r_n + s_n) \end{aligned}$$

for all $r \in R$ and $(r_1, \ldots, r_n), (s_1, \ldots, s_n) \in R^n$. Letting $n = 1$, we see that R is, itself, and R-module. Finally, define $R^0 = \{0\}$, the *trivial* R-module.

(d) If R is a ring, then the ring of polynomials $R[x]$ is an R-module. For example, $\mathbb{Z}[x]$ is a $\mathbb{Z}$-module. Similarly, any polynomial ring in several variables over R is an R-module. For example, $\mathbb{Z}[x, y, z]$ is a $\mathbb{Z}$-module.

(e) If G is an abelian group, then G is a $\mathbb{Z}$-module as follows: If $g \in G$ and $n \in \mathbb{Z}_{>0}$, define

$$ng = \underbrace{g + \cdots + g}_{n-\text{times}}.$$

It $n \in \mathbb{Z}_{<0}$, define $ng = (-n)(-g)$, and finally, for $0 \in \mathbb{Z}$, define $0g = 0$, where the second 0 is the additive identity for G.

(f) (**Important**) If R is a ring, then an R-ideal is exactly a subset I of R such that I is an R-module with the natural operation: if $r \in R$ and $i \in I$, then ri is just multiplication in R. We could have defined the notion of an ideal in this way if we had the language of modules earlier.

Definition 8. An R-module M is *generated by* $X \subseteq M$ if each $m \in M$ is a finite R-linear combination of elements of X, i.e., if for all $m \in M$, we can write

$$m = \sum_{x \in X} r_x x$$

where each r_x is an element of R and $r_x = 0$ for all but finitely many x. If M is generated by X, we write

$$M = \sum_{x \in X} Rx.$$

We say M is *finitely generated* if it is generated by a finite set.

Definition 9. A *basis* for an R-module M is a subset $B \subseteq M$ such that every element of M can be written *uniquely* as a finite R-linear combination of B. (Equivalently, B is R-linearly independent and spans M.) A *free* R-module is an R-module with a basis.

Example 10. Unlike vector spaces, modules do not necessarily have bases. For example, $\mathbb{Z}$-module $\mathbb{Z}/5\mathbb{Z}$ has no basis. To see this, let B be any subset of $\mathbb{Z}/5\mathbb{Z}$. If $B = \emptyset$ or $B = \{0\}$, then $\operatorname{Span}_{\mathbb{Z}} B = \{\overline{0}\}$, and hence B does not span. Otherwise, let $x \in B$ with $x \neq 0$. Since 5 is a nonzero element of $\mathbb{Z}$, we have the nontrivial $\mathbb{Z}$-linear relation $5 \cdot x = \overline{0}$. So B is not linearly independent.

Definition 11. A *homomorphism* of R-modules M and N is a mapping $\phi \colon M \to N$ that preserves addition and scalar multiplication, i.e., for all $u, v \in M$ and $r \in R$:

$$\begin{aligned} \phi(u+v) &= \phi(u) + \phi(v) \\ \phi(ru) &= r\phi(u). \end{aligned}$$

A homomorphism is an *isomorphism* if it is bijective (in which case, the inverse is a homomorphism (exercise!)). The *kernel* of a homomorphism ϕ is

$$\ker(\phi) := \phi^{-1}(0) := \{m \in M : \phi(m) = 0\},$$

and the *image* is

$$\operatorname{im}(\phi) := \phi(M) := \{\phi(m) : m \in M\}.$$

Exercise 12. Show that an R-module homomorphism $\phi \colon M \to N$ is injective if and only if $\ker(\phi) = 0$.

Definition 13. A *submodule* of an R-module M is a subset $N \subseteq M$ that is itself an R-module (under the operations inherited from M). (Exercise: N is a submodule if and only if it is nonempty and closed under addition and scalar multiplication).

Definition 14. Let M be an R-module with submodule N. The *quotient module* M/N is the set of *cosets*

$$m + N := \{m + n : n \in N\}$$

with addition and scalar multiplication defined by

$$(m+N)+(m'+N):=(m+m')+N \quad \text{and} \quad r(m+N):=(rm)+N$$

for all $m, m' \in M$ and $r \in R$. (Exercise: these operations are well-defined and under them, M/N is an R-module.)

Remark 15. As usual, we can think of the quotient module M/N as the module M except that elements of N are set equal to 0. Also, as usual, we could have defined M/N as the set of equivalence classes under the equivalence $m \sim m'$ if m and m' differ be an element of N, i.e., $m - m' \in N$.

Example 16. Some examples of $\mathbb{Z}$-modules (all but the first are finitely-generated):

$$\begin{aligned} \mathbb{Z}[x] &\quad \text{generating set:}\{1, x, x^2, \ldots\} \\ \mathbb{Z}[i] &\quad \text{generating set:}\{1, i\} \\ \mathbb{Z} &\quad \text{generating set:}\{1\} \\ \mathbb{Z}[x,y]/(x^2,y^2) &\quad \text{generating set:}\{1, x, y, xy\}. \end{aligned}$$

In the final example, (x^2, y^2) is the ideal ($\mathbb{Z}$-submodule) of $\mathbb{Z}[x,y]$ generated by x^2 and y^2:

$$(x^2, y^2) = \{ax^2 + by^2 : a, b \in \mathbb{Z}[x,y]\}.$$

Modding out by this ideal sets $x^2 = y^2 = 0$ in $\mathbb{Z}[x,y]$. So, for instance, in $\mathbb{Z}[x,y]/(x^2,y^2)$, we have

$$1 + 2x + 3y + 4x^2 + 5xy + 6y^2 + 7x^3 + 8xy^3 = 1 + 2x + 3y + 5xy.$$

since x^2, y^2, x^3 and xy^3 are in the ideal (x^2, y^2).

Proposition 17. A finitely-generated R-module M is free if and only if it is isomorphic to R^n for some $n \geq 0$.

Proof. Suppose M has basis $B = \{b_1, \ldots, b_n\}$. Then we get an isomorphism $\phi\colon M \to R^n$ determined by letting $\phi(b_i) = e_i$ and extending linearly, i.e.,

$$\phi(\textstyle\sum_{i=1}^n r_i b_i) := \sum_{i=1}^n r_i \phi(b_i) = \sum_{i=1}^n r_i e_i = (r_1, \ldots, r_n) \in R^n.$$

Here, e_i is the i-th standard basis vector of R^n, i.e., e_i is the vector whose components are all 0 except its i-th component, which is 1.

Since B spans M, we have thus defined $\phi(m)$ for every element $m \in M$. Not that $\phi(m)$, as defined, depends upon how we express m as a linear combination of B. However, since B is a basis, this linear combination is unique. So ϕ is well-defined.

Conversely, suppose that $\phi\colon M \to R^n$ is an isomorphism. For $i = 1, \ldots, n$, define $b_i = \phi^{-1}(e_i)$. Then it is straightforward to check that $\{b_1, \ldots, b_n\}$ is a basis for M, and hence, M is free. $\square$

Example 18. We have the $\mathbb{Z}$-module isomorphism

$$\begin{aligned} \mathbb{Z}[i] &\to \mathbb{Z}^2 \\ a + bi &\mapsto (a, b), \end{aligned}$$

determined by $1 \mapsto (1, 0)$ and $i \mapsto (0, 1)$.