Introduction

In this class: rings, fields

- Insolvability of ≥ 5 equations in radicals
- Fundamental theorem of algebra

Review

Definition: Recall that a **group** is a set G with operations $o : G \times G \to G$ (multiplication) and $(\cdot)^{-1} : G \times G \to G$ such that:

1. If $f, g, h \in G$, then $(fg)h = f(gh)$
2. There exists a unit $e \in G$ such that $e \circ g = g \circ e = g$ and $g \circ g^{-1} = g^{-1} \circ g = e$

Examples:

1. $(\mathbb{Z}, +), e = 0, (\cdot)^{-1} = -(\cdot)$
2. $D_n =$ dihedral group - group of symmetries of a regular n-gon
    - $e =$ identity transformation
3. $GL_n(\mathbb{R}) = n \times n$ matrices with determinant $\neq 0$
    - $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Definition: G is an **abelian group** if $g \circ h = h \circ g$ (commutativity).

4. $n \times n$ matrices with respect to addition is an abelian group

Rings

Definition: A **ring** R is a set with two operations **addition** and **multiplication** $(+, \cdot)$ such that

1. $(R, +)$ is an abelian group
2. $\cdot$ is associative: $a(bc) = (ab)c$
3. **Distributivity:** $a(b + c) = ab + ac$ and $(a + b)c = ab + ac$

Definition: R is a ring with **unit** if there exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for any a in the ring.

- Unit with respect to addition $+$ is usually denoted by 0
- Unit with respect to multiplication $\times$ is usually denoted by 1

Definition: R is a **commutative ring** if $ab = ba$ for all $a, b \in R$

In this class, we mostly work with commutative rings with unit, so "ring" will mean this.

Examples:

0. The "zero ring" $R = \{0\}$. All the operations are trivial: $0 + 0 = 0 \cdot 0 = 0$. In this case, $1 = 0$.

Exercise: if R is a ring such that $1 = 0$, then R is the "zero ring".

1. $(\mathbb{Z}, +, \cdot)$ is a ring
2. $(\mathrm{Mat}_{n\times n}(\mathbb{R}), +, \cdot)$ is a non-commutative ring with unit $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
3. **Polynomial ring** $(R[x], +, \cdot)$ with coefficients in R, where R is another ring (not necessarily commutative). x is a formal variable. Elements are of the form

$$\sum_{i=0}^{N} a_i x^i \leftrightarrow (a_0, a_1, \ldots, a_N) \quad a_i \in R$$

$+$ is component-wise. Multiplication is as follows:

$$\left(\sum_{i=0}^{N} a_i x^i\right) \cdot \left(\sum_{j=0}^{M} b_j x^j\right) = \sum_{k=0}^{N+M} \left(\sum_{i+j=k} a_i b_j\right) x^k$$

4. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings

Subrings

Definition: A **subring** of R is a subset closed under $+, \cdot$ and containing 1. We write $R' \leq R$ if R' is a subring of R.

$$\mathbb{Z} \leq R_1 \leq \mathbb{Q} \leq R_2 \leq \mathbb{R} \leq \mathbb{C}$$

Let's construct R_1 by adding $1/2$ to $\mathbb{Z}$.

If $n \in \mathbb{Z}$, then $n + 1/2 \in \mathbb{Z} + 1/2$, so R must contain all half-integers.

$$n \cdot \frac{1}{2} \in \mathbb{Z} \cup \left(\mathbb{Z} + \frac{1}{2}\right)$$

Also, $1/2 \cdot 1/2 = 1/4 \rightsquigarrow 1/2^k$ must be in R, so $n/2^k$ must be in R.

Definition:

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{n}{2^k} : n \in Z, k \in \mathbb{Z}_{\geq 0}\right\}$$

is the minimal subring of $\mathbb{Q}$ containing $1/2$.

Proof: $1 \in \mathbb{Z}[1/2] \implies \mathbb{Z} \subset \mathbb{Z}[1/2]$. You can keep multiplying by $1/2$ to get the $1/2^k$ factor. Finally, check that it is a ring:

$$\frac{n}{2^k} + \frac{m}{2^p} = \frac{2^p n + 2^k m}{2^{k+p}} \qquad \frac{n}{2^k} \cdot \frac{m}{2^p} = \frac{nm}{2^{kp}}$$

More generally, $\mathbb{Z}[1/n] \leq \mathbb{Q}$ is the minimal subring of $\mathbb{Q}$ containing $1/n$, where

$$\mathbb{Z}\left[\frac{1}{n}\right] = \left\{\frac{m}{n^k} : m \in \mathbb{Z}, k \in \mathbb{Z}_{\geq 0}\right\}$$

Exercise: prove that minimal subring containing $1/n$ and $1/m$ is $\mathbb{Z}[1/nm]$.

There exists $\mathbb{R}_3 \leq \mathbb{C}$ such that $R_3 \nleq \mathbb{R}$.

Example: The **Gaussian integers** $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$. Check this is a ring:

$$(a+ib)+(c+id) = (a+c)+i(b+d)$$
$$(a+ib)(c+id) = (ac-bd)+i(ad+bc)$$

$$R_2 = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

Check it's closed under multiplication:

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$$

Proposition: any nonzero element in $\mathbb{Q}(\sqrt{2})$ has an inverse in this ring:

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

Definition: A ring R is called a **field** if every nonzero $a \in R$ has a multiplicative inverse.