NOVEMBER 7 NOTES

1. 7.1: Introduction to rings: basic definitions and examples

Some reminders from last week:

Definition 1.1. A **ring** R is a set with two binary operations, $+$ and $\times$ (called *addition* and *multiplication*) such that:

(1) $(R, +)$ is an abelian group, where we denote the identity element by 0 and the inverse of some $a \in R$ by $-a$,
(2) $\times$ is an associative binary operation, and
(3) the *distributive laws* hold: for all $a, b, c \in R$,
$$(a + b) \times c = (a \times c) + (b \times c)$$
and
$$a \times (b + c) = (a \times b) + (a \times c).$$

Definition 1.2. Let R be a ring. R is **commutative** if $\times$ is commutative. R is said to have an **identity** if there exists an element $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.

Definition 1.3. Let R be a ring with identity 1 where $1 \neq 0$. If every nonzero element $a \in R$ has a multiplicative inverse, i.e. for all $a \in R$ there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$, then R is called a **division ring**. If R is a commutative division ring, then R is called a **field**.

Definition 1.4. Let R be a ring.

(1) A nonzero element $a \in R$ is called a **zero divisor** if there exists some $b \in R$, $b \neq 0$, such that $ab = 0$ or $ba = 0$. A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has *no* zero divisors.
(2) If R has an identity $1 \neq 0$, an element $u \in R$ is called a **unit** if u has a multiplicative inverse $u^{-1} \in R$. The set of all units in a ring R are by definition a *group under multiplication*, so is called the **group of units** of R and denoted by $R^\times$.

Definition 1.5. Let R be a ring. A **subring** of R is a subgroup of R that is closed under multiplication (i.e. a subset of R that is also a ring).

Here is an example that we started last time:

Example 1.6. Let $D \in \mathbb{Q}$ be a rational number that is not a perfect square in $\mathbb{Q}$ (not the square of any rational number).

Let $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}\}$. This is called a **quadratic field.** It is a subring of $\mathbb{C}$ because it is a subgroup of $\mathbb{C}$ and $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D})$, so it is closed under multiplication. (In fact, if $\sqrt{D} \in \mathbb{R}$, it is a subring of $\mathbb{R}$.) It is also commutative and has identity $1 = 1 + 0\sqrt{D})$.

It turns out that $\mathbb{Q}(\sqrt{D})$ is also a field. If $a + b\sqrt{D}$ is a nonzero element, then $a^2 - b^2D \neq 0$ (this would imply that $D = a^2/b^2$ so is a perfect square) which them implies it has a multiplicative inverse given by $\frac{a - b\sqrt{D}}{a^2 - b^2D}$, which can be written as $c + d\sqrt{D}$ for $c, d \in \mathbb{Q}$.

One comment: we will often assume that D is actually a square-free integer, meaning it is not divisible by the square of any prime number. Indeed, if $D = \frac{a}{b} \in \mathbb{Q}$, then $D = \frac{s^2}{b^2}D'$ where $D' = \frac{a}{s^2}b$ where s^2 is the largest perfect square that divides a. If D is not a square and written in lowest form (so $(a,b)=1$), then D' is an integer that is square-free. Furthermore, $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'})$ because $\sqrt{D} = \frac{1}{b}\sqrt{D'}$, so $c + d\sqrt{D} = c + \frac{d}{b}\sqrt{D'}$. Therefore, in any example of quadratic field, we can assume without any loss of generality that D is a square-free integer.

From this example, we have several interesting subrings. The following example defines several of them:

Example 1.7. If D is a square-free integer, then $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{Q}(\sqrt{D})$.

If $D = -1$, then we have the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ which is called the **Gaussian integers.**

If $D = 1 \pmod 4$, we actually have a slightly larger interesting subring:

$$\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$$

(check that this is a subring!). These are interesting for several reasons and have names.

Let $\mathcal{O} = \mathbb{Z}[\omega] \subset \mathbb{Q}(\sqrt{D})$ be the subring given by:

$$\omega = \sqrt{D} \text{ if } D = 2,3 \pmod 4 \qquad \omega = \frac{1+\sqrt{D}}{2} \text{ if } D = 1 \pmod 4.$$

This ring $\mathcal{O}$ is called the **ring of integers** in $\mathbb{Q}(\sqrt{D})$.

On the quadratic field, we have a function called a **norm**:

$$N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$$
$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D.$$

You can check the following facts about the norm:

(1) For any $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$, $N(\alpha)N(\beta) = N(\alpha\beta)$, and
(2) For $a + b\omega \in \mathcal{O} = \mathbb{Z}[\omega]$,

$$N(a+b\omega) = \begin{cases} a^2 - b^2 D & D = 2,3 \pmod 4 \\ a^2 + ab + (1-D)b^2/4 & D = 1 \pmod 4 \end{cases}$$

so for any $\alpha \in \mathcal{O}$, $N(\alpha) \in \mathbb{Z}$.

This actually allows us to compute the units in many rings $\mathcal{O}$! We can do this in both cases, but for now we just write the case that $D = 2,3 \pmod 4$. If $a + b\omega \in \mathcal{O}$ has $N(a + b\omega) = \pm 1$, then $(a + b\omega)^{-1} = \pm(a - b\omega)$, which is still an element of $\mathcal{O}$, so is a unit. If $\alpha \in \mathcal{O}$ is a unit, then for some $\beta \in \mathcal{O}$, $\alpha\beta = 1$ so $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$, but $N(\alpha)$ and $N(\beta)$ are integers, so this is possible only if $N(\alpha) = \pm 1$. Therefore, $\alpha \in \mathcal{O}$ is a unit if and only if $N(\alpha) = \pm 1$. (This is also true in the case $D = 1 \pmod 4$.)

Let's apply this: find the group of units in $\mathbb{Z}[i]$. The previous computation says $a + bi$ is a unit if and only if $N(a + bi) = a^2 + b^2 = 1$. Because a and b are integers, this is possible if and only if $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$. So, $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

2. 7.3: Ring Homomorphisms and Quotient Rings

A few more definitions.

Definition 2.1. Let R and S be rings.

(1) A **ring homomorphism** is a map $\phi : R \to S$ such that, for all $a, b \in R$, $\phi(a+b) = \phi(a)+\phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$.
(2) The **kernel** of ϕ is

$$\ker\phi = \{r \in R \mid \phi(r) = 0\}.$$

(3) An **isomorphism** is a bijective homomorphism.

Example 2.2. The function $\phi : \mathbb{Z} \to \mathbb{Z}_2$ given by $\phi(n) = n \pmod 2$ (equivalently, $\phi(n) = 0$ if n is even and $\phi(n) = 1$ if n is odd) is a homomorphism. The kernel is the set of even integers.

Example 2.3. Fix $r \in R$, where R is a ring. Let $ev_r : R[x] \to R$ be the function $ev_r(p(x)) = p(r)$ (called 'evaluation' of p at r). This is a ring homomorphism:

$$ev_r(p(x) + q(x)) = p(r) + q(r) = ev_r(p(x)) + ev_r(q(x))$$

and

$$ev_r(p(x)q(x)) = p(r)q(r) = ev_r(p(x))ev_r(q(x)).$$

The kernel is precisely the set of polynomials such that $p(r) = 0$, i.e. the polynomials for which r is a root.

A short proposition, whose proof we leave as an exercise:

Proposition 2.4. *Let R and S be rings and $\phi : R \to S$ a homomorphism. Then,*

(1) The image of ϕ is a subring of R, and
(2) The kernel of ϕ is a subring of R. Furthermore, if $a \in \ker \phi$ and $r \in R$ is any element, then $ar \in \ker \phi$.

This last comment on the kernel is an example of something called an *ideal*, which we will define next time.