27. 4/24

27.1. *Review* Last week, we introduced rings and fields. A ring is a set equipped with operations that generalize the usual addition and multiplication of integers. A field is a ring where every nonzero element is a unit, *i.e.*, has an inverse under multiplication.

We also discussed how some equations do not have solutions in a given ring, but do have solutions in a larger ring. For instance,

$$x^2 + 1 = 0$$

has no solutions in $\mathbf{R}$ or $\mathbf{Z}/3\mathbf{Z}$, but does in $\mathbf{C}$ and $\mathbf{Z}[i]/3\mathbf{Z}[i]$.

27.2. We say that a ring R is *algebraically closed* iff any polynomial equation of positive degree with coefficients in R can be solved in R. That is, for any integer $d \geq 1$ and $a_0, a_1, \ldots, a_d \in R$ such that $a_d \neq 0$, the equation

$$a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0 = 0$$

must always have a solution $x \in R$.

I claim that any algebraically closed ring must be a field. Why? We must be able to solve $ax - 1 = 0$ whenever $a \neq 0$. Then the solution x is the multiplicative inverse of a.

Example 27.1. We mentioned last time that $\mathbf{Z}/3\mathbf{Z}$ is a field. But it is not algebraically closed, because it does not contain solutions to $x^2 + 1 = 0$. It turns out that $\mathbf{Z}[i]/3\mathbf{Z}[i]$ is also a field, but it is not algebraically closed either, because it does not contain solutions to $x^3 - x - 1 = 0$.

How to check this? For any $x = a + bi$, where $a, b \in \mathbf{Z}$, we have

$$(a + bi)^3 \equiv a^3 + 3a^2(bi) + 3a(bi)^2 + (bi)^3 \equiv a^3 - b^3 i \pmod{3}.$$

Therefore $x^3 - x - 1 \equiv (a^3 - a - 1) - (b^3 + b)i \pmod{3}$. There is no way to pick $a \in \mathbf{Z}$ such that $a^3 - a - 1 \equiv 0 \pmod{3}$ as integers.

27.3. *The fundamental theorem of algebra* The main goal today is to prove:

Theorem 27.2. *The field of complex numbers* $\mathbf{C}$ *is algebraically closed.*

To this end, we need a little calculus, or more precisely, contour integration. How many people have seen contour integration before?

In high school, we learn to integrate over intervals of the real line: $[a, b] \subseteq \mathbf{R}$. In a similar way, if $\gamma : [0, 1] \to \mathbf{C}$ is a parametrized path in the complex plane, and f is a nice-enough function defined on an (open) domain containing γ, then we can integrate along γ using the parametrization:

$$\int_\gamma f(z)\, dz = \int_0^1 f(\gamma(t))\gamma'(t)\, dt.$$

By “nice-enough”, we really mean a condition called *holomorphicity*. It says that near any point α of our domain, we can Taylor-expand $f(z)$ as a power series in $z-\alpha$.

Away from γ, it could happen that f has a “pole”. For instance, if $\gamma(t) = e^{2\pi i t}$, then $f(z) = 1/z$ is holomorphic along γ, but undefined at $z = 0$. Note:

$$\int_\gamma \frac{1}{z}\,dz = \int_0^1 \frac{2\pi i e^{2\pi i t}}{e^{2\pi i t}}\,dt = 2\pi i.$$

In general, if γ parametrizes a *simple closed curve* (something we will not define in detail), then $\int_\gamma f\,dz$ is closely related to the poles of f in the interior of γ. This is the key idea we will use to prove Theorem 27.2.

27.4. *Residues and orders* We say that f is *meromorphic* around a complex number α iff, in some (open) disk centered (and punctured) at α, we have

$$f(z) = \sum_{k \geq N} c_k (z-\alpha)^k,$$

where $c_N \neq 0$.

The *residue* of f at α is $\mathrm{res}_\alpha(f) = c_{-1}$. The order of f at α is $\mathrm{ord}_\alpha(f) = N$. We say that f is *holomorphic* at α when its order at α is nonnegative.

In what follows, let γ be a parametrized simple closed curve, and let Ω be an (open) domain containing the interior of γ.

Theorem 27.3 (Cauchy). *If f is meromorphic on Ω, and has neither zeros nor poles along γ, then*

$$\frac{1}{2\pi i}\int_\gamma f\,dz = \sum_{\textit{poles } \alpha \in \Omega \textit{ of } f} \mathrm{res}_\alpha(f).$$

Corollary 27.4. *If h is holomorphic on Ω, and h'/h has neither zeros nor poles along γ, then*

$$\frac{1}{2\pi i}\int_\gamma \frac{h'}{h}\,dz = \sum_{\textit{zeros } \alpha \in \Omega \textit{ of } h} \mathrm{ord}_\alpha(h).$$

Proof. If $f(z) = h'(z)/h(z)$, then the poles of f are the zeros of h, and if α is such a number, then $\mathrm{res}_\alpha(f) = \mathrm{ord}_\alpha(h)$. □

27.5. *Rouché’s principle* Informally, the *winding number* of a simple closed curve around α is the number of times that it circles α in a counter-clockwise direction before it stops. This is an integer, possibly zero or negative, since the “closed” condition means the curve returns to its starting point.

In what follows, we write $h \circ \gamma$ for the parametrized path defined by

$$(h \circ \gamma)(t) = h(\gamma(t)).$$

In the situation of Corollary 27.4, substituting $w = h(z)$ gives

$$\frac{1}{2\pi i}\int_\gamma \frac{h'}{h}\,dz = \frac{1}{2\pi i}\int_{h\circ\gamma}\frac{dw}{w} = \text{winding number of } h\circ\gamma \text{ around } 0.$$

Now imagine we perturb h to a function of the form

$$H(z) = h(z) + \varepsilon(z), \qquad \text{where } |h(z)| > |\varepsilon(z)| \text{ along } \gamma.$$

Then $H \circ \gamma$ must have the same winding number around 0 as $h \circ \gamma$. This is sometimes called Rouché's principle.

Proof of Theorem 27.2. We will show that if

$$H(z) = a_d z^d + a_{d-1}z^{d-1} + \cdots + a_1 z + a_0, \qquad \text{where } d \geq 1 \text{ and } a_d \neq 0,$$

then $\sum_{\text{zeros } \alpha \text{ of } H} \operatorname{ord}_\alpha(H) = d$. Indeed, set

$$\begin{aligned} h(z) &= a_d z^d, \\ \varepsilon(z) &= a_{d-1}z^{d-1} + \cdots + a_1 z + a_0. \end{aligned}$$

Let γ be a circle around zero large enough that $|h(z)| > |\varepsilon(z)|$ along γ. Then

$$\begin{aligned} \textstyle\sum_{\text{zeros } \alpha \text{ of } H} \operatorname{ord}_\alpha(H) &= \text{winding number of } H\circ\gamma \text{ around } 0 \\ &= \text{winding number of } h\circ\gamma \text{ around } 0 \\ &= \operatorname{ord}_0(h) \\ &= d, \end{aligned}$$

as claimed. □

28. 4/26

28.1. *Ring homomorphisms* If R and S are rings, then a map $f : R \to S$ is said to be a *homomorphism (of rings)* iff for all $x, y \in R$, we have

$$\begin{aligned} f(x + y) &= f(x) + f(y), \\ f(x \cdot y) &= f(x) \cdot f(y), \\ f(1_R) &= 1_S. \end{aligned}$$

(Above, we are using subscripts to disambiguate the identity elements of R and S.) Note that while $f(0_R) = 0_S$ is implied by the first condition, $f(1_R) = 1_S$ is not implied by the second condition.

If f is injective, then we say that $f(R)$ is a *subring* of R'. If f is surjective, then we say that $f(R)$ is a *quotient ring* of R. Finally, a bijective homomorphism of rings is called an *isomorphism*, just like the terminology for groups.

Example 28.1. We saw earlier that there are many group homomorphisms $\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$. Each is determined by where it sends 1.

By contrast, a ring homomorphism $R \to S$ must send 1_R to 1_S. So there is only one ring homomorphism $\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$: the map $a \mapsto a + m\mathbf{Z}$. Again, this map is surjective. Thus, $\mathbf{Z}/m\mathbf{Z}$ is not just a quotient group of $\mathbf{Z}$, but a quotient ring as well.

Example 28.2. Similarly, there is exactly one ring homomorphism $\mathbf{Z} \to \mathbf{Z}[i]$: the map $a \mapsto a$. This map is injective, but not surjective: $\mathbf{Z}$ forms a (strict) subring of $\mathbf{Z}[i]$.

28.2. It's natural to ask: Is there a ring homomorphism in the other direction, *i.e.*, $f : \mathbf{Z}[i] \to \mathbf{Z}$? I claim that the answer must be no.

The informal idea: There is no way to put i inside $\mathbf{Z}$. A formal explanation: If f were a ring homomorphism, then since $i^2 + 1 = 0$, we would have

$$0 = f(0) = f(i^2 + 1) = f(i)^2 + f(1) = f(i)^2 + 1.$$

But there is no <u>integer</u> $f(i)$ such that $f(i)^2 + 1 = 0$.

In general, if $f : R \to S$ is a ring homomorphism, and $a \in R$ satisfies some equation involving only addition and multiplication—in other words, a polynomial equation—then $f(a)$ must satisfy a similar equation.

28.3. When do we have a ring homomorphism

$$f : \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}?$$

It must send $f(1 + m\mathbf{Z}) = 1 + n\mathbf{Z}$, so we must have

$$m + n\mathbf{Z} = f(m + m\mathbf{Z}) = f(0 + m\mathbf{Z}) = 0 + n\mathbf{Z}.$$

So we require that $m \equiv 0 \pmod{n}$, or equivalently, that n divides m in $\mathbf{Z}$. In this case, there is exactly one possibility for f.

28.4. When do we have a ring homomorphism

$$f : \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}[i]/\mu\mathbf{Z}[i]?$$

By similar reasoning to the previous discussion, it requires that $m \equiv 0 \pmod{\mu}$, or equivalently, that μ divides m in $\mathbf{Z}[i]$, and in this case, there is exactly one possibility for f.

Example 28.3. Take $m = \mu$. In this case, f is injective, but not surjective, since

$$|\mathbf{Z}/m\mathbf{Z}| = m < m^2 = |\mathbf{Z}[i]/m\mathbf{Z}[i]|.$$

In other words, $\mathbf{Z}/m\mathbf{Z}$ forms a strict subring of $\mathbf{Z}[i]/m\mathbf{Z}[i]$.

Example 28.4. Take $m = 5$ and $\mu = 2 + i$. A discussion from the April 3 showed that in this case, the map f is an isomorphism of rings. The same argument works for $\mu = 2 - i$.

28.5. *Products of rings* If R and S are rings, then the cartesian product $R \times S$ forms a ring under coordinate-wise addition and multiplication:

$$(x, y) + (x', y') := (x + x', y + y'),$$
$$(x, y) \cdot (x', y') := (x \cdot x', y \cdot y').$$

The additive and multiplicative identity elements of $R \times S$ are given by

$$0_{R\times S} = (0_R, 0_S),$$
$$1_{R\times S} = (1_R, 1_S).$$

Example 28.5. We claim that the map

$$\begin{array}{rcl} \mathbf{Z}[i]/5\mathbf{Z}[i] & \to & \mathbf{Z}[i]/(2+i)\mathbf{Z}[i] \quad \times \quad \mathbf{Z}[i]/(2-i)\mathbf{Z}[i] \\ \alpha + 5\mathbf{Z}[i] & \mapsto & (\alpha + (2+i)\mathbf{Z}[i], \quad \alpha + (2-i)\mathbf{Z}[i]) \end{array}$$

is a ring isomorphism. The domain and range of F both have exactly 25 elements, so to prove bijectivity, it's enough to prove surjectivity. That is, we must show that for any $\beta \in \mathbf{Z}[i]/(2+i)\mathbf{Z}[i]$ and $\gamma \in \mathbf{Z}[i]/(2-i)\mathbf{Z}[i]$, we can find some $\alpha \in \mathbf{Z}[i]$ such that

$$\alpha \equiv \beta \pmod{2+i}, \qquad \alpha \equiv \gamma \pmod{2-i}.$$

But note that $2 + i$ and $2 - i$ are actually coprime in $\mathbf{Z}[i]$. So we can prove the existence of this α by an argument similar to that in the proof of the Chinese Remainder Theorem for integers.

28.6. We can also restate the Chinese Remainder Theorem in a new way:

Theorem 28.6 (Chinese Remainder)**.** *If $m, n \in \mathbf{N}$ are coprime, then*

$$\begin{array}{rcl} \mathbf{Z}/(mn)\mathbf{Z} & \to & \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \\ a + mn\mathbf{Z} & \mapsto & (a + m\mathbf{Z}, a + n\mathbf{Z}) \end{array}$$

is an isomorphism of rings.

This statement implies the isomorphism of unit groups. More generally, if $f : R \to S$ is a ring isomorphism, then f restricts to a group isomorphism $f^\times : R^\times \to S^\times$.

29. 4/28

29.1. Last time we talked about ring homomorphisms and quotient rings. You can think of quotient rings as a vast generalization of congruence classes and congruence arithmetic.

We saw several examples of homomorphisms to quotient rings:

$$\begin{aligned} \mathbf{Z} &\to \mathbf{Z}/m\mathbf{Z}, && \text{where } m \in \mathbf{Z}, \\ \mathbf{Z}[i] &\to \mathbf{Z}[i]/\mu\mathbf{Z}[i], && \text{where } \mu \in \mathbf{Z}[i], \\ \mathbf{Z}/m\mathbf{Z} &\to \mathbf{Z}/n\mathbf{Z}, && \text{where } n \text{ divides } m. \end{aligned}$$

There are sillier examples: If $R \to R'$ is a ring isomorphism, then it is necessarily surjective, so R' is a quotient ring of R. And the zero ring $\{0\}$ is necessarily a quotient ring of every ring.

A ring homomorphism $f : R \to R'$ is always a homomorphism of the underlying abelian groups, since $f(x + y) = f(x) + f(y)$. In particular, if R' is a quotient ring of R, then it is necessarily a quotient group of R with respect to addition.

Is the converse true? Namely: If R is a ring and R' is a quotient group of $(R, +)$, then is it necessarily true that R' is a quotient ring of R? No:

Example 29.1. We know that $\mathbf{Z}[i]$ forms a ring. As a group under addition, $\mathbf{Z}[i]$ contains the subgroup $\mathbf{Z}$. But I claim that the quotient group $\mathbf{Z}[i]/\mathbf{Z}$ cannot be a quotient ring of $\mathbf{Z}[i]$. Recall that by definition,

$$\mathbf{Z}[i]/\mathbf{Z} = \{\alpha + \mathbf{Z} \mid \alpha \in \mathbf{Z}[i]\}.$$

The group homomorphism that expresses it as a quotient group of $\mathbf{Z}[i]$ is the map $\alpha \mapsto \alpha + \mathbf{Z}$.

If $\mathbf{Z}[i]/\mathbf{Z}$ were a quotient ring, then $1 + \mathbf{Z}$ would be the identity element for multiplication. But $1 + \mathbf{Z} = 0 + \mathbf{Z}$, and the latter is the identity element for addition. We observed on April 19 that the identity elements for addition and multiplication can only match in the zero ring.

So in order to form a quotient ring of R, it's not enough to have a quotient group. In other words: In order for R/S to be a quotient ring of R, it's not enough to start with an additive subgroup $S \subseteq R$.

In fact, the example we just discussed shows that it's not enough to start with a subring $S \subseteq R$.

29.2. *Kernels* To understand this better, let's take a step back to something more general.

If $f : (G, \star) \to (H, *)$ is a homomorphism of groups, then the *kernel* of f is

$$\ker(f) = \{g \in G \mid f(g) = e_H\}.$$

That is, the kernel of f is the preimage in G of the identity element of $(H, *)$.

Lemma 29.2. *Above,* $\ker(f)$ *is a subgroup of* $(G, \star)$.

Proof. It's enough to check that $\ker(f)$ is closed under the binary operation $\star$ and under inversion (as together, these imply that it contains the identity element). First, if $x, y \in \ker(f)$, then

$$f(x \star y) = f(x) * f(y) = e_H * e_H = e_H,$$

proving that $x \star y \in \ker(f)$. Next,

$$f(x^{\star -1}) = f(x)^{*-1} = e_H^{*-1} = e_H,$$

proving that $x^{\star -1} \in \ker(f)$. □

Lemma 29.3. *f is injective if and only if* $\ker(f) = \{e_G\}$.

Proof. The "only if" direction is immediate from the definition of injectivity. As for the "if" direction: Suppose that $\ker(f) = \{e_G\}$. We must show that if some $x, y \in G$ satisfy $f(x) = f(y)$, then $x = y$. Notice that

$$f(x \star y^{\star -1}) = f(x) * f(y)^{*-1} = e_H.$$

Therefore $x \star y^{\star -1} \in \ker(f)$. Therefore $x \star y^{\star -1} = e_G$, whence $x = y$. □

Let $K = \ker(f)$ for convenience. There is a group operation on $G/K = \{x \star K \mid x \in G\}$ given by

$$(x \star K) \circ (y \star K) = (x \star y) \star K,$$

as in our discussion of quotient groups.

Theorem 29.4. *Any group homomorphism $f : (G, \star) \to (H, *)$ can be factored as a composition*

$$(G, \star) \to (G/K, \circ) \xrightarrow{\bar{f}} (H, *),$$

where the first map is $x \mapsto x \star K$ and the second is $\bar{f}(x \star K) = f(x)$. Moreover, the first map is surjective and the second is injective.

Proof. First, $\bar{f}$ is well-defined because if $x \star K$ and $y \star K$ are two ways to write the same coset, then $x \in y \star K$, whence $x = y \star k$ for some $k \in K$, whence

$$\bar{f}(x \star K) = f(x) = f(y \star k) = f(y) * e_H = f(y) = \bar{f}(y \star K).$$

Next, the map $G \to G/K$ is surjective by construction. Finally, to show that $\bar{f}$ is injective: By Lemma 29.3, it's enough to show that $\ker(\bar{f})$ consists of the identity element of G/K, which is $e_G \star K = K$. By definition,

$$\begin{aligned} \ker(\bar{f}) &= \{x \star K \mid \bar{f}(x \star K) = e_H\} \\ &= \{x \star K \mid f(x) = e_H\} \\ &= \{x \star K \mid x \in \ker(f) = K\} \\ &= \{K\}, \end{aligned}$$

as desired. □

Remark 29.5. In books on abstract algebra, the result above is often called the "First Homomorphism Theorem".

29.3. *Ideals* Now suppose that R, R' are rings.

Lemma 29.6. *Let $f : R \to R'$ be a homomorphism of the underlying additive groups, and let $K = \ker(f)$.*

If $f : R \to R'$ is a homomorphism of rings, not just groups, then K is contagious *under multiplication, in the sense that*

$$\textit{for all } a \in K \textit{ and } x \in R, \textit{ we have } a \cdot x \in K.$$

Proof. Let $a \in K$ and $x \in R$. If f is a homomorphism of rings, then

$$f(a \cdot x) = f(a) \cdot f(x) = 0_{R'} \cdot f(x) = 0_{R'}.$$

Thus $ax \in K$. □

Motivated by Lemma 29.6, we say that a subset $I \subseteq R$ is an *ideal* of R iff the following properties hold:

(1) I is a subgroup of the group formed by R under addition.
(2) I is contagious under multiplication.

Next time, we will show a weak converse to the lemma: Namely, if I is an ideal of R, then R/I forms a ring, and the surjective group homomorphism $R \to R/I$ is in fact a ring homomorphism. In particular, R/I is a quotient ring of R.