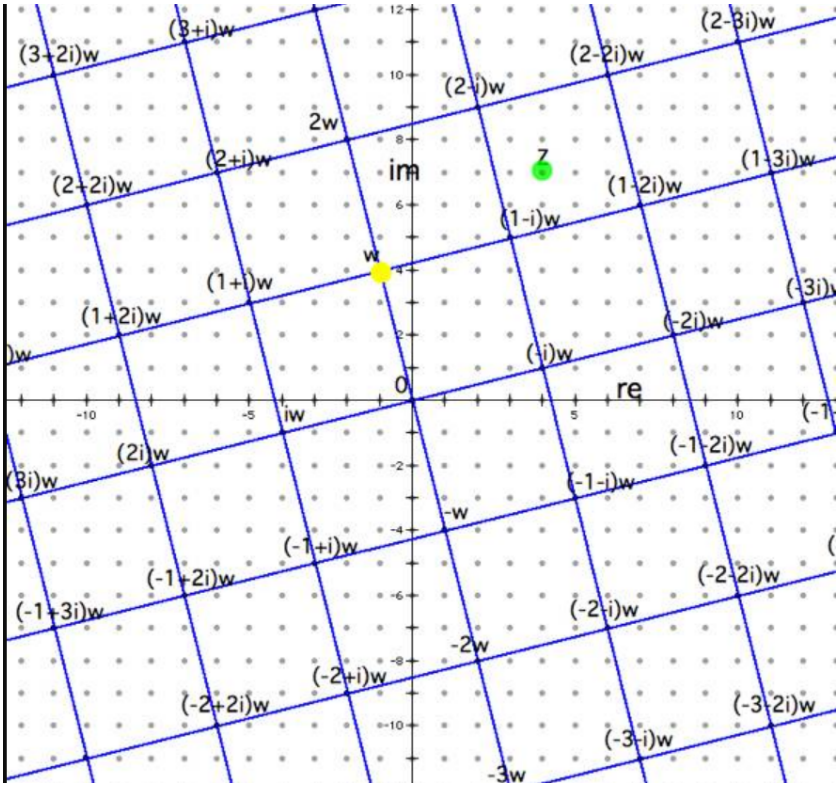

Notes: These are notes live-tex'd from a graduate course in Algebraic Number Theory taught by Paul Pollack at the University of Georgia in Spring 2021. As such, any errors or inaccuracies are almost certainly my own.

Algebraic Number Theory

Lectures by Paul Pollack. University of Georgia, Spring 2021

D. Zack Garza

D. Zack Garza
University of Georgia
dzackgarza@gmail.com

Last updated: 2021-01-19

Table of Contents

Contents

1 | Thursday, January 14

See website for notes on books, intro to class.

- Youtube Playlist: https://www.youtube.com/playlist?list=PLAOxtXqOUji8fjQysx4k8a6h-hOZ7x5ue
- Free copies of textbook: https://www.dropbox.com/sh/rv5j222kn74bjhm/AABZ1qcR1rOnpaBsa5CL3P_Ea?dl=0&lst=
- Course website: ?

Paul's description of the course:

"This course is an introduction to arithmetic"beyond $\mathbb{Z}$", specifically arithmetic in the ring of"integers" in a finite extension of $\mathbb{Q}$. (Among many other things) we'll prove three important theorems about these rings:

- Unique factorization into ideals.
- Finiteness of the group of ideal classes.
- Dirichlet's theorem on the structure of the unit group."

1.1 Motivation

Solving Diophantine equations, i.e. polynomial equations over $\mathbb{Z}$.

Example 1.1.1 ***(?):*** Consider $y^2 = x^3 + x$.

Claim: $(x, y) = (0, 0)$ is the only solution.

To see this, write $y^2 = x(x^2 + 1)$, which are relatively prime, i.e. no $D \in \mathbb{Z}$ divides both of them. Why? If $d \mid x$ and $d \mid x + 1$, then $d \mid (x^2 + 1) + (-x) = 1$. It's also the case that both $x^2 + 1$ and x^2 are squares (up to a unit), so $x^2, x^2 + 1$ are consecutive squares in $\mathbb{Z}$. But the gaps between squares are increasing: $1, 2, 4, 9, \cdots$. The only possibilities would be $x = 0, y = 1$, but in this case you can conclude $y = 0$.

Example 1.1.2 ***(Fermat):*** Consider $y^2 = x^3 - 2$.

Claim: $(3, \pm 5)$ are the only solutions.

Rewrite

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$$
$$\in \mathbb{Z}[\sqrt{-2}] \coloneqq \left\{ a + b\sqrt{-2} \;\middle|\; a, b, \in \mathbb{Z} \right\} \leq \mathbb{C}.$$

This is a subring of $\mathbb{C}$, and thus at least an integral domain. We want to try the same argument: showing the two factors are relatively prime. A little theory will help here:

Definition 1.1.3 ***(Norm Map)***
For $\alpha \in \mathbb{Z}[\sqrt{-2}]$ define $N\alpha = \alpha\overline{\alpha}$.

Lemma 1.1.4 ***(?).***
Let $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$. Then

1. $N(\alpha\beta) = N(\alpha)N(\beta)$
2. $N(\alpha) \in \mathbb{Z}_{\geq 0}$ and $N(\alpha) = 0$ if and only if $\alpha = 0$.
3. $N(\alpha) = 1 \iff \alpha \in R^\times$

Proof (?). 1. Missing, see video (10:13 AM).

2. $N(\alpha) = a^2 + 2b^2 \geq 0$, so this equals zero if and only if $\alpha = \beta = 0$
3. Write $1 = \alpha\overline{\alpha}$ if $N(\alpha) = 1 \in R^\times$. Conversely if $\alpha \in R^\times$ write $\alpha\beta = 1$, then

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta) \in \mathbb{Z}_{\geq 0},$$

which forces both to be 1.

■

Claim: The two factors $y \pm \sqrt{2}$ are *coprime* in $\mathbb{Z}[\sqrt{-2}]$, i.e. every common divisor is a unit.

Proof (?).
Suppose $\delta \mid y \pm \sqrt{-2}$, then $y + \sqrt{-2} = \delta\beta$ for some $\beta \in \mathbb{Z}[\sqrt{-2}]$. Take norms to obtain $y^2 + 2 = N\delta N\beta$, and in particular

- $N\delta y^2 + 2$
- $\delta \mid (y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2}$ and thus $N\delta \mid N(2\sqrt{-2}) = 8$.

In the original equation $y^2 = x^3 - 2$, if y is even then x is even, and $x^3 - 2 \equiv 0 - 2 \pmod 4 \equiv 2$, and so $y^2 \equiv 2 \pmod 4$. But this can't happen, so y is odd, and we're done: we have $N\delta \mid 8$ which is even or 1, but $N\delta \mid y^2 + 2$ which is odd, so $N\delta = 1$.

■

We can identify the units in this ring:

$$\mathbb{Z}[\sqrt{-2}]^\times = \left\{ a + b\sqrt{-2} \;\middle|\; a^2 + 2b^2 = 1 \right\}$$

which forces $a^2 \leq 1, b^2 \leq 1$ and thus this set is $\{\pm 1\}$.

So we have $x^3 = ab$ which are relatively primes, so a, b should also be cubes. We don't have to worry about units here, since ± 1 are both cubes. So e.g. we can write

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}.$$

Comparing coefficients of $\sqrt{-2}$ yields

$$1 = b(3a^2b - 2b^2) \in \mathbb{Z} \implies b \mid 1,$$

and thus $b \in \mathbb{Z}^\times$, i.e. $b \in \{\pm 1\}$. By cases:

- If $b = 1$, then $1 = 3a^2 - 2 \implies a^2 = 1 \implies a = \pm 1$. So

  $$y = \sqrt{-2} = (\pm 1 + \sqrt{-2})^3 = \pm 5 + \sqrt{-2},$$

  which forces $y = \pm 5$, the solution we already knew.

- If $b = -1$, then $1 = -(3a^2 - 1)$ which forces $1 = 3a^2 \in \mathbb{Z}$, so there are no solutions.

Example 1.1.5 ***(?):*** Consider $y^2 = x^3 - 26$. Rewrite this as

$$x^3 = y^2 + 26 = (y + \sqrt{-26})(y - \sqrt{-26}),$$

then the same lemma goes through with 2 replaced by 26 everywhere where the RHS factors are still coprime. Setting $y + \sqrt{-26} = (a + b\sqrt{-26})^3$ and comparing coefficients, you'll find $b = 1, a = \pm 3$. This yields $x = 35, y = \pm 207$. But there are more solutions: $(x, y) = (3, \pm 1)$! The issue is that we used unique factorization when showing that ab is a square implies a or b is a square (say by checking prime factorizations and seeing even exponents). In this ring, we can have ab a cube with *neither* a, b a cube, even up to a unit.

Question 1.1.6
When does a ring admit unique factorization? Do you even *need* it?

This will lead to a discussion of things like the **class number**, which measure the failure of unique factorization. In general, the above type of proof will work when the class number is 3!

2 | Lecture 2 (Tuesday, January 19)

Today: Ch.2 of the book, "Cast of Characters". Note that all rings will be commutative and unital in this course.

Last time: looked at factorization in $\mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{26}]$. Where do rings like this come from?

Definition 2.0.1 (Number Field)
A **number field** is a subfield $K \subseteq \mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$.

Remark 2.0.2: Some authors don't require $K \subseteq \mathbb{C}$, but any finite extension of $\mathbb{Q}$ will embed into $\mathbb{C}$ so there's no harm in this extra requirement.

Example 2.0.3 *(?):* $\mathbb{Q}[\sqrt[3]{2}, \mathbb{Q}[\sqrt{2}, \sqrt[5]{7}]$ or $\mathbb{Q}(\theta)$ where θ is a root of $x^5 - x - 1$ (which you can check is irreducible. Now that the round vs. square brackets here won't make a difference, since we're adjoining algebraic numbers.

Proposition 2.0.4 *(?).*
Let $K_{/\mathbb{Q}}$ be a finite extension, say of degree $n \coloneqq [K : \mathbb{Q}]$. Then there are n distinct embeddings [a] of K into $\mathbb{C}$

[a] An injective ring morphism.

Proof (?).
We have $K_{/\mathbb{Q}}$, which is necessarily separable since $\mathrm{ch}(\mathbb{Q}) = 0$. By the primitive element theorem, we can write $K = \mathbb{Q}(\theta)$ where θ is a root of some degree n irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Since $\mathbb{C}$ is algebraically closed, f splits completely over $\mathbb{C}$ as $f = \prod_{i=1}^{n}(x - \theta_i$ which each $\theta_i \in CC$ distinct since f was irreducible and we're in characteristic zero. Then for each i there is an embedding $K = \mathbb{Q}[\theta]$ given by

$$\begin{aligned} \iota_i : \mathbb{Q}[\theta] &\hookrightarrow \mathbb{C} \\ g(\theta) &\mapsto g(\theta_i). \end{aligned}$$

There are some easy things to check:

- This is well-defined: elements in K are polynomials in θ but they all differ by a multiple of the minimal polynomial of θ,
- This is an inject homomorphism and thus an embedding, and
- For distinct i you get distinct embeddings: just look at the image $\iota_i(\theta)$, these are distinct numbers in $\mathbb{C}$.

■

Definition 2.0.5 (Real and Nonreal embeddings)
Let $K_{/\mathbb{Q}}$ be a finite extension of degree $n = [K : \mathbb{Q}]$. We'll say an embedding $\sigma : K \to \mathbb{C}$ is **real** if $\sigma(K) \subseteq \mathbb{R}$, otherwise we'll say the embedding is **nonreal**.

Remark 2.0.6: If σ is a nonreal, then $\overline{\sigma}$ is a nonreal embedding, so this embeddings come in pairs. As a consequence, the total number of embeddings is given by $n = r_1 + 2r_2$, where r_1 is the number of real embeddings and r_2 is the number of nonreal embeddings.

Example 2.0.7 *(?):* Let $K = \mathbb{Q}(\sqrt[3]{2})$. Here $n = 3$ since this is the root of a degree 3 irreducible

polynomial. Using the proof we can find the embeddings: factor

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}).$$

where $\omega = e^{2\pi i/3}$ is a complex cube root of unity. We can form an embedding by sending $\sqrt[3]{2} \to \omega^j \sqrt[3]{2}$ for $j = 0, 1, 2$. The case $j = 0$ sends K to a subset of $\mathbb{R}$ and yields a real embedding, but the other two will be nonreal. So $r_1 = 1, r_2 = 1$, and we have $3 = 1 + 2(1)$ and this is consistent.

Remark 2.0.8: We've only been talking about fields, since unique factorization is trivial since there are no primes. There are thus "too many" units, compared to the rings we were considering before, so we'll restrict to subrings. The question is: where is the arithmetic? Given a number field K, we want a ring $\mathbb{Z}_K$ that fits this analogy:

$$\begin{array}{ccc} \mathbb{Q} & \rightsquigarrow & K \\ \downarrow & & \downarrow \\ \mathbb{Z} & \rightsquigarrow & \mathbb{Z}_K = ? \end{array}$$

Definition 2.0.9 (Algebraic Numbers)
Given $\alpha \in \mathbb{C}$ we say α is an **algebraic number** if and only if α is algebraic over $\mathbb{Q}$, i.e. the root of some polynomial in $\mathbb{Q}[x]$.

Remark 2.0.10: We know that if we define $\overline{\mathbb{Q}} \coloneqq \left\{\alpha \in \mathbb{C} \;\middle|\; \alpha \text{ is algebraic over } \mathbb{Q}\right\}$, we can alternatively describe this as $\overline{\mathbb{Q}} = \left\{\alpha \in \mathbb{C} \;\middle|\; [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty\right\}$. This is convenient because it's easy to see that algebraic numbers are closed under sums and products, just using the ways degrees behave in towers.

Corollary 2.0.11 ***(?).***
$\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ is a subfield and every number field is a subfield of $\overline{\mathbb{Q}}$.

These are still fields, so lets define some interesting subrings.

Definition 2.0.12 ($\overline{\mathbb{Z}}$)
Define $\overline{\mathbb{Z}} \coloneqq \left\{\alpha \in \mathbb{C} \;\middle|\; \alpha \text{ is the root of a monic polynomial } f \in \mathbb{Z}[x]\right\}$.

Theorem 2.0.13 ***($\overline{\mathbb{Z}}$ is a ring).***
$\overline{\mathbb{Z}}$ is a ring, and in fact a domain since it's a subring of $\mathbb{C}$.

We'll use an intermediate criterion to prove this:

Proposition 2.0.14 ***(Integrality Criterion).***
Let $\alpha \in \mathbb{C}$ and suppose there is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{C}$ with $\alpha M \subseteq M \neq 0$. Then $\alpha \in \overline{\mathbb{Z}}$, i.e. α is the root of a monic polynomial with integer coefficients.

Proof (of integrality criterion).
Chasing definitions, take M and choose a finite list of generators $\beta_1, \beta_2, \cdots, \beta_m$ for M. Then $\alpha M \subseteq M \implies \alpha\beta_i \in M$ for all M, and each $\alpha\beta_i$ is a $\mathbb{Z}$-linear combination of the β_i . I.e. we have

$$\alpha \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & a_{22} & \\ \vdots & & \ddots \end{bmatrix} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} \coloneqq A\vec{\beta},$$

where $A \in \mathrm{Mat}(n \times m, \mathbb{Z})$. We can rearrange this to say that

$$(\alpha \operatorname{id} - A) \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \mathbf{0}.$$

Not all of the β_i can be zero since $M \neq 0$, and thus $\alpha \operatorname{id} - A$ is singular and thus has determinant zero, so $\det(x \operatorname{id} - A)\Big|_{x=a} = 0$. We have

$$x \operatorname{id} - A = \begin{bmatrix} x - a_{1,} & & & \\ & x - a_{2,2} & & \\ & & \ddots & \\ & & & x - a_{m,m} \end{bmatrix},$$

where the off-diagonal components are constants in $\mathbb{Z}$ coming from A. Taking the determinant yields a monic polynomial: the term of leading degree comes from multiplying the diagonal components, and expanding over the remaining minors only yields terms of smaller degree. So $\det(x \operatorname{id} - A) \in \mathbb{Z}[x]$ is monic.

■

Proof (of theorem).
We want to show that $\overline{\mathbb{Z}}$ is a ring, and it's enough to show that

- $1 \in \overline{\mathbb{Z}}$, which is true since $x - 1$ is monic.
- It's closed under $+, \cdot$.

Note that the first property generalizes to $\mathbb{Z} \subseteq \overline{\mathbb{Z}}$, since $x - n$ is monic for any $n \in \mathbb{Z}$. For the second, let $\alpha, \beta \in \overline{\mathbb{Z}}$. Define $M \coloneqq \mathbb{Z}[\alpha, \beta]$, then it's clear that $(\alpha + \beta)M \subseteq M$ and $(\alpha\beta)M \subseteq M$ since $\mathbb{Z}[\alpha, \beta]$ are polynomials in α, β and multiplying by these expression still yields such polynomials. It only remains to check the following:

Claim: M is finitely-generated.

Proof (?).
Let α be a root of $f \in \mathbb{Z}[x]$ and β a root of g, both monic with $\deg f = n, \deg g = m$. We want to produce a finite generating set for $M \coloneqq \mathbb{Z}[\alpha, \beta]$, and the claim is that the following works: $\left\{\alpha^i \beta^j\right\}_{\substack{0 \le i < n \\ 0 \le j < m}}$, i.e. every element of M is some $\mathbb{Z}$-linear combination of these.
Note that this is clearly true if we were to include n, m in the indices by collecting terms of any polynomial in α, β, so the restrictions are nontrivial. It's enough to show that for any $0 \le I, J \in \mathbb{Z}$, the term $\alpha^I \beta^J$ is a $\mathbb{Z}$-linear combination of the restricted elements above. Divide by f and g to obtain $x^I = f(x)q(x) + r(x)$ and $x^J = g(x)\tilde{q}(x)\tilde{r}(x)$ where $r(x) = 0$ or $\deg r < n$ and similarly for $\tilde{r}$, where (importantly) all of these polynomials are in $\mathbb{Z}[x]$. We're not over a field: $\mathbb{Z}[x]$ doesn't necessarily have a division algorithm, so why is this okay? The division algorithm only requires inverting the leading coefficient, so in general $R[x]$ admits the usual division algorithm whenever the leading coefficient is in $R^\times$.
Now plug α into the first equation to obtain $\alpha^I = r(\alpha)$ where $\deg r < n$, which rewrite α^I as a sum of lower-degree terms. Similarly writing $\beta^J = r(\beta)$, we can express

$$\alpha^I \beta^J = r(\alpha) r(\beta),$$

which is what we wanted.

■

■

Remark 2.0.15: We've just filled in another part of the previous picture:

$$\begin{array}{ccc} \mathbb{Q} & K & \overline{\mathbb{Q}} \\ \downarrow & \downarrow & \downarrow \\ \mathbb{Z} & \mathbb{Z}_K & \overline{\mathbb{Z}} \end{array}$$

Definition 2.0.16 (Ring of Integers)
Define $\mathbb{Z}_K = \overline{\mathbb{Z}} \cap K$, the **ring of integers** of K. Note that this makes sense since the intersection of rings is again a ring.

Remark 2.0.17: Why not just work in $\overline{\mathbb{Z}}$? It doesn't have the factorization properties we want, e.g. there are no irreducible elements. Consider $\sqrt{2}$, we can factor is into two non-units (noting that $\sqrt{2}$ is not a unit) as $\sqrt{\sqrt{2}} \cdot \sqrt{\sqrt{2}}$, and it's easy to check that if a is not a unit then $\sqrt{a}$ is not a unit. So this would yield arbitrarily long factorizations, and is thus not Noetherian.

The following is a reality check, and certainly a property we would want:

Proposition 2.0.18 ***(The ring of integers of*** $\mathbb{Q}$ ***is*** $\mathbb{Z}$ ***).***
$\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$.

Proof (of proposition).
$\subseteq$: easy, since $\mathbb{Z} \subseteq \overline{\mathbb{Z}}$ and $\mathbb{Z} \subseteq \mathbb{Q}$, and is thus in their intersection $\mathbb{Z}_{\mathbb{Q}}$.
$\supseteq$: Let $\alpha \in \mathbb{Z}_{\mathbb{Q}} = \mathbb{Q} \cap \overline{\mathbb{Z}}$, so α is a root of $x^n - a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. We know $\alpha = a/b$ with $a, b \in \mathbb{Z}$, and we can use the rational root test which tells us that $a \mid a_0, b \mid 1$, so $b = \pm 1, \alpha = a/\pm 1 = \pm a \in \mathbb{Z}$ and thus $\alpha \in \mathbb{Z}$.

■

We'll want to study $\mathbb{Z}_K$ for various number fields K, but we'll need more groundwork.

Proposition 2.0.19 ***(Easy criterion to check if an integer is algebraic).***
Let $\alpha \in \overline{\mathbb{Q}}$, then

$$\alpha \in \overline{\mathbb{Z}} \iff \min_{\alpha} \in \mathbb{Z}[x],$$

where $\min_{\alpha}(x)$ is the unique monic irreducible polynomial in $\mathbb{Q}[x]$ which vanishes at α.

Proof (?).
$\Longleftarrow$: Trivial, if the minimal polynomial already has integer coefficients, just note that it's already monic and thus $\alpha \in \overline{\mathbb{Z}}$ by definition.
$\Longrightarrow$: Why should the minimal polynomial have *integer* coefficients? Choose a monic $f(x) \in \mathbb{Z}[x]$ with $f(\alpha) = 0$, using the fact that $\alpha \in \overline{\mathbb{Z}}$, and factor $f(x) = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{C}[x]$. Note that each $\alpha_i \in \overline{\mathbb{Z}}$ since they are all roots of f (a monic polynomial in $\mathbb{Z}[x]$). Use the fact that $\min_{\alpha}(x)$ divides every polynomial which vanishes on α over $\mathbb{Q}$, and thus divides f (noting that this still divides over $\mathbb{C}$). Moreover, every root of $\min_{\alpha}(x)$ is a root of f, and so every such root is some α_i.
Now factor $\min_{\alpha}(x)$ over $\mathbb{C}$ to obtain $\min_{\alpha}(x) = \prod_{i=1}^{m}(x - \beta_i)$ with all of the $\beta_i \in \overline{\mathbb{Z}}$. What coefficients appear after multiplying things out? Just sums and products of the β_i, so all of the coefficients are in $\overline{\mathbb{Z}}$. Thus $\min_{\alpha}(x) \in \overline{\mathbb{Z}}[x]$. But the coefficients are also in $\mathbb{Q}$ by definition, so the coefficients are in $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ and thus $\min_{\alpha}(x) \in \mathbb{Z}[x]$.

■

Example 2.0.20 ***(Showing an integer is not algebraic using minimal polynomials):*** $\sqrt{5}/3 \notin \overline{\mathbb{Z}}$ since $\min_{\alpha}(x) = x^2 - 5/9 \notin \mathbb{Z}[x]$, so this is not an algebraic integer.

Proposition 2.0.21 *(*$\mathrm{ff}(\mathbb{Z}_K) = K$ *).*

a. $\overline{\mathbb{Z}}$ has $\overline{\mathbb{Q}}$ as its fraction field, and
b. For any number field K, $\mathbb{Z}_K$ has K as its fraction field.

Moreover, both of these statements follow from:

c. If $\alpha \in \overline{\mathbb{Q}}$ then $d\alpha \in \overline{\mathbb{Z}}$ for some $d \in \mathbb{Z}^{\geq 0}$

Remark 2.0.22: Thus the subring is "big" in the sense that if you allow taking quotients, you

recover the entire field. That $c \implies a, b$: suppose you want to write $\alpha \in \overline{\mathbb{Q}}$ as $\alpha = p/q$ with $p, q \in \overline{\mathbb{Z}}$. Use c to produce $d\alpha \in \overline{\mathbb{Z}}$, then just take $d\alpha/d$. The same argument works for b.

Exercise 2.0.23 (?)
Prove the proposition!

Proposition 2.0.24 *(?).*
Suppose $\alpha \in \overline{\mathbb{C}}$ and α is a root of a monic polynomial in $\overline{\mathbb{Z}}[x]$. Then $\alpha \in \overline{\mathbb{Z}}$.

Remark 2.0.25: This says that if a number α is the root of a monic polynomial whose coefficients are *algebraic* integers, then α itself is an algebraic integer coefficients. This corresponds to the fact that integral over integral implies integral in commutative algebra.

Exercise 2.0.26 (Prove the proposition.)
Prove this! Can use the integrality criterion (slightly challenging), can also use Galois theory.

ToDos

List of Todos

2

Definitions

2

Theorems

2

Exercises

Figures

List of Figures