PSET8

Student: Ryan Baldwin, rbaldwi2@swarthmore.edu

Professor: Dr. Hsu

Collaborators:

Peer Reviewers: Adil Beken, Dr. Hsu

Due Date: April 4, 2025 (Extension granted up to April 5, 2025)

Artin Chapter Chapter 11: 1.3 (only statement with Q): Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing the rational numbers $\mathbb{Q}$ and the elements $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. Let $\gamma = \alpha + \beta$. Is $\mathbb{Q}[\alpha + \beta] = \mathbb{Q}[\gamma]$?

Proof. To determine if $\mathbb{Q}[\alpha + \beta] = \mathbb{Q}[\gamma]$ where $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$, and $\gamma = \alpha + \beta$, we must consider the smallest subrings of $\mathbb{C}$ containing the specified elements. We will show that each ring is contained within the other.

$\mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\alpha, \beta]$**:**

Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing $\mathbb{Q}$, $\alpha = \sqrt{2}$, and $\beta = \sqrt{3}$. By definition, $\mathbb{Q}[\alpha, \beta]$ contains all elements that can be obtained from $\mathbb{Q}$, $\sqrt{2}$, and $\sqrt{3}$ through a finite number of additions, subtractions, and multiplications.

Consider $\gamma = \alpha + \beta = \sqrt{2} + \sqrt{3}$. Since $\sqrt{2} \in \mathbb{Q}[\alpha, \beta]$ and $\sqrt{3} \in \mathbb{Q}[\alpha, \beta]$, and $\mathbb{Q}[\alpha, \beta]$ is closed under addition (as it is a subring), it follows that their sum $\gamma = \sqrt{2} + \sqrt{3}$ must also be an element of $\mathbb{Q}[\alpha, \beta]$.

Now, let $\mathbb{Q}[\gamma]$ denote the smallest subring of $\mathbb{C}$ containing $\mathbb{Q}$ and $\gamma = \sqrt{2} + \sqrt{3}$. By definition, $\mathbb{Q}[\gamma]$ contains all elements that can be obtained from $\mathbb{Q}$ and γ through a finite number of additions, subtractions, and multiplications. Since $\gamma \in \mathbb{Q}[\alpha, \beta]$ and $\mathbb{Q} \subseteq \mathbb{Q}[\alpha, \beta]$, and $\mathbb{Q}[\alpha, \beta]$ is closed under ring operations, any element formed from $\mathbb{Q}$ and γ using these operations must also be an element of $\mathbb{Q}[\alpha, \beta]$. Therefore, $\mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\alpha, \beta]$.

$\mathbb{Q}[\alpha, \beta] \subseteq \mathbb{Q}[\gamma]$**:**

To show the other containment, we want to show that both $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$ are elements of $\mathbb{Q}[\gamma]$. If we can show this, then since $\mathbb{Q} \subseteq \mathbb{Q}[\gamma]$ and $\mathbb{Q}[\gamma]$ is closed under ring operations, any element formed from $\mathbb{Q}$, $\sqrt{2}$, and $\sqrt{3}$ using these operations must also be an element of $\mathbb{Q}[\gamma]$, thus proving $\mathbb{Q}[\alpha, \beta] \subseteq \mathbb{Q}[\gamma]$.

We know $\gamma = \sqrt{2} + \sqrt{3} \in \mathbb{Q}[\gamma]$. Consider γ^2:

$$\gamma^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}.$$

Since $\gamma \in \mathbb{Q}[\gamma]$, and $\mathbb{Q}[\gamma]$ is a ring, γ^2 must also be in $\mathbb{Q}[\gamma]$. Also, $5 \in \mathbb{Q} \subseteq \mathbb{Q}[\gamma]$. Since $\mathbb{Q}[\gamma]$ is closed under subtraction, $\gamma^2 - 5 = (5 + 2\sqrt{6}) - 5 = 2\sqrt{6}$ is an element of $\mathbb{Q}[\gamma]$.

Now, consider γ^3:

$$\gamma^3 = (\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}.$$

Since $\gamma \in \mathbb{Q}[\gamma]$, γ^3 is also in $\mathbb{Q}[\gamma]$. We have the following system of equations where both $\gamma = \sqrt{2} + \sqrt{3}$ and $\gamma^3 = 11\sqrt{2} + 9\sqrt{3}$ are in $\mathbb{Q}[\gamma]$:

$$\sqrt{2} + \sqrt{3} = \gamma$$
$$11\sqrt{2} + 9\sqrt{3} = \gamma^3$$

Multiplying the first equation by 9 we see that $9\sqrt{2} + 9\sqrt{3} = 9\gamma$. Subtract this from the second equation yields $(11\sqrt{2} + 9\sqrt{3}) - (9\sqrt{2} + 9\sqrt{3}) = \gamma^3 - 9\gamma$, or equivalently, $2\sqrt{2} = \gamma^3 - 9\gamma$. Since $\gamma \in \mathbb{Q}[\gamma]$, $\gamma^3 - 9\gamma$ is also in $\mathbb{Q}[\gamma]$, and thus $2\sqrt{2} \in \mathbb{Q}[\gamma]$. Since $\frac{1}{2} \in \mathbb{Q} \subseteq \mathbb{Q}[\gamma]$, and $\mathbb{Q}[\gamma]$ is closed under multiplication, $\frac{1}{2}(2\sqrt{2}) = \sqrt{2} = \alpha$ is in $\mathbb{Q}[\gamma]$.

Now that we know $\sqrt{2} \in \mathbb{Q}[\gamma]$ and $\sqrt{2}+\sqrt{3} = \gamma \in \mathbb{Q}[\gamma]$, by closure under subtraction, $\gamma - \sqrt{2} = \sqrt{3} = \beta$ is also in $\mathbb{Q}[\gamma]$.

Since we have shown that $\sqrt{2} \in \mathbb{Q}[\gamma]$ and $\sqrt{3} \in \mathbb{Q}[\gamma]$, it follows that $\mathbb{Q}[\alpha, \beta] \subseteq \mathbb{Q}[\gamma]$.

Therefore, we have shown inclusion both ways. Namely that $\mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\alpha, \beta]$ and that $\mathbb{Q}[\alpha, \beta] \subseteq \mathbb{Q}[\gamma]$. Indeed, we can conclude that $\mathbb{Q}[\alpha + \beta] = \mathbb{Q}[\gamma]$.

□

Artin Chapter 11: 2.2: Let F be a field. The set of all formal power series $p(t) = a_0 + a_1t + a_2t^2 + \cdots$, with a_i in F, forms a ring that is often denoted by $F[[t]]$. By *formal* power series we mean that the coefficients form an abritrary sequence of elements of F. There is no requirement of convergence. Prove that $F[[t]]$ is a ring, and determine the units in this ring.

Proof. In order for the set of all formal power series

$$p(t) = \sum_{i=0}^{\infty} a_i t^i = a_0 + a_1 t + a_2 t^2 + \cdots$$

with a_i in F to form a ring, the set must satisfy a number of strict properties. The set must be an abelian group under addition; closed, associative and contain a multiplicative identity of 1 under multiplication; and must satisfy the distributive property.

Indeed, because any formal power series can be represented as a sequence of polynomials, we introduce the additive and multiplicative law of compositions defined for the i-th entries as follows:

For any $p(t)$ with coefficients a_i and $q(t)$ with coefficients b_i in $F[[t]]$,

$$(p+q)_i = a_i + b_i$$

$$(p \cdot q)_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

.

The i-th coefficient of the product $p(t)q(t)$ is determined by a finite sum involving the first $i+1$ coefficients of both $p(t)$ and $q(t)$. Even though the product itself is a formal power series, each individual coefficient can be computed directly.

Therefore, we can note that the addition and multiplication of formal power series are defined in a way that extends the familiar addition and multiplication of polynomials. When we consider polynomials as formal power series with a finite number of nonzero coefficients, the rules for addition and multiplication coincide.

$F[[t]]$ is an abelian group under addition:

Since the sume of any two elements in F remain in F, the sum of any two formal power series must remain in $F[[t]]$, and the set is closed under addition as one would expect when working with polynomial addition. Noting that addition in F is associative, addition in $F[[t]]$ must also be associative given the addition of polynomials is also associative. Next, we let all coefficients in a series equal to 0, and we obtain the constructed series $z(t) = 0 + 0t + 0t^2 + \cdots = 0$. This series, $z(t) = 0$, serves as our additive identity element in the set. Furthermore, since F is a field, for every a_i there exists an $-a_i$ such that

$a_i + (-a_i) = 0$. From this it then follows that for every formal power series $p(t)$ in the set, there exists an inverse $-p(t)$ such that $p(t) + (-p(t)) = 0$. Lastly, since all elements in F commute additively, then it must follow that all elements in $F[[t]]$ commute additively. Therefore, the set $F[[t]]$ is an abelian group under addition.

$F[[t]]$ is closed, associative and contains multiplicative identity 1 under multiplication:

Since the product of any two elements in F remain in F, the product of any two formal power series must also be in $F[[t]]$ given the multiplication of two polynomials is another polynomial, and so the set is closed under multiplication. And because multiplication in F is associative, it follows that multiplication in $F[[t]]$ is associative as polynomial multiplication behaves as such. Likewise, since all elements in F commute multiplicatively, then it follows that all elements in $F[[t]]$ commute multiplicatively, again, because polynomials behave as such and the coefficients are elements in the field F. Lastly, we let the first coefficient in a series equal to 1 and all proceeding coefficients equal to 0, and we obtain the constructed series

$$e(t) = 1 + 0t + 0t^2 + \cdots = 1.$$

This series, $e(t) = 1$, serves as our multiplicative identity element in the set. Therefore, the set $F[[t]]$ is closed under a multiplicative law of composition that is both commutative and associative with identity 1.

Distributive property:

Let $p(t) = \sum_{i=0}^{\infty} a_i t^i$, $q(t) = \sum_{i=0}^{\infty} b_i t^i$, and $r(t) = \sum_{i=0}^{\infty} c_i t^i$ be elements of $F[[t]]$.

Consider the i-th coefficient of $(p(t)+q(t))r(t)$. We have $(p(t)+q(t)) = \sum_{i=0}^{\infty}(a_i+b_i)t^i$, so the i-th coefficient of the product is $\sum_{j=0}^{i}(a_j + b_j)c_{i-j}$.

By the distributive property of the field F, this is equal to $\sum_{j=0}^{i}(a_j c_{i-j}+b_j c_{i-j})$, which can be rewritten as $\sum_{j=0}^{i} a_j c_{i-j} + \sum_{j=0}^{i} b_j c_{i-j}$. These are precisely the i-th coefficients of $p(t)r(t)$ and $q(t)r(t)$ respectively.

Thus, $(p(t) + q(t))r(t) = p(t)r(t) + q(t)r(t)$. This distributive behavior mirrors how polynomial multiplication distributes over addition while also relying on the field's properties.

Thus, the addition and multiplication defined on the set $F[[t]]$ satisfies the distributive property.

Indeed, we have show that the set $F[[t]]$ is a commutative ring with identity.

The Units of $F[[t]]$:

Let $p(t) = \sum_{i=0}^{\infty} a_i t^i$ and $q(t) = \sum_{i=0}^{\infty} b_i t^i$ be two elements in $F[[t]]$. Then, we call $p(t)$ a unit if there exists a $q(t)$ such that $p(t)q(t) = 1 = 1 + 0t + 0t^2 + \cdots$. We shall construct the criteria for $p(t)$ to be a unit directly.

Consider the first three coefficients of the product $p(t)q(t)$:

$$a_0b_0 = 1,$$
$$a_0b_1 + a_1b_0 = 0,$$
$$a_0b_2 + a_1b_1 + a_2b_0 = 0.$$

Through some algebraic manipulation, we see that the general form of the coefficients of the product $p(t)q(t)$ can be expressed as follows:

$$a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \cdots + a_ib_0 = 0.$$

We will now show through induction that this equation can always be solved to obtain all b_i so long as $a_0 \neq 0$. Let us assume that we have already solved for $b_0, b_1, \ldots, b_k$, by our recurrisve hypothesis, we see that the $k+1$-th coefficient must satisfie the formula

$$a_0b_{k+1} + a_1b_k + a_2b_{k-1} + \cdots + a_kb_0 = 0.$$

Since we have already solved for $b_0, b_1, \ldots, b_k$ and all a_i are elements of the field F, let the sum of the known coefficients be $c_k = a_1b_k + a_2b_{k-1} + \cdots + a_kb_0$. We then see that

$$\begin{gathered} a_0b_{k+1} + c_k = 0 \\ a_0b_{k+1} = -c_k \\ b_{k+1} = -a_0^{-1}c_k \end{gathered}$$

Thus, we have shown that b_{k+1} can be uniquely determined by the previous coefficients $b_0, b_1, \ldots, b_k$ and with all a_i in F so long as $a_0 \neq 0$, as 0 is the only element in the field without a multiplicative inverse.

Furthermore, we can conclude that $p(t)$ is a unit if and only if $a_0 \neq 0$. That is to say, the units of $F[[t]]$ are precisely elements of the form $p(t) = a_0 + a_1t + a_2t^2 + \cdots$ where $a_0 \neq 0$. □

Artin Chapter 11: 3.2 Prove that every nonzero ideal in the ring of Gauss integers contains a nonzero integer.

Proof. Consider a nonzero ideal I in the ring of Gaussian integers $\mathbb{Z}[i]$. Because I is a nonzero ideal, we know that the set is nonempty and any element in the ideal multiplied by any element in the ring is another element in the ideal.

Let $a+bi$ be a nonzero element in the ideal. Furthermore, let $a+(-b)i$ be an element in the ring $\mathbb{Z}[i]$, where $-b$ is the additive inverse of the integer b. If we multiply $a+bi$ by $a-bi$, then we see that a^2+b^2 is an element in the ideal.

Since a and b are integers and at least one is nonzero, we have shown that the nonzero integer a^2+b^2 will be in every nonzero ideal in the ring of Gaussian integers. Thus, we can conclude that every nonzero ideal in the ring of Gaussian integers contains a nonzero integer. □