ABSTRACT ALGEBRAIC NUMBER THEORY

PETE L. CLARK

In these notes I wish to consider the possibility of generalizing classical algebraic number theory to the class of "abstract number rings." So far they are entirely expository, and none of the results are due to me.

Some basic conventions and notation:

Throughout these notes "ring" means commutative ring with unity.

For a ring R, by $\mathcal{I}(R)$ we will mean the set of nonzero ideals of R. Under multiplication of ideals, $\mathcal{I}(R)$ naturally has the structure of a commuative monoid.

For a ring R, we write $\Sigma(R)$ for the set of maximal ideals of R.

1. Introduction to abstract number rings

1.1. Definition.

Definition: An **abstract number ring** is a ring R which is infinite, is not a field, and satisfies:

(FN) For all nonzero ideals I of R, the quotient ring R/I has finite cardinality.

For any ring R satisfying (FN), we can define a **norm function** from the nonzero ideals to the positive integers:

$$||I|| = \#R/I.$$

The condition (FN) stands for "finite norms." The latter two conditions in the definition of an abstract number ring are nontriviality conditions in the sense that any finite ring, and any field, satisfies (FN).

1.2. Structure theorem for abstract number rings.

First an immediate but useful result:

Lemma 1. *Let $0 \neq I \subset J$ be ideals in an (FN)-ring. If $||I|| = ||J||$, then $I = J$.*

Theorem 2. *An abstract number ring is a Noetherian domain of dimension one.*

Proof: If $I \in \mathcal{I}(R)$, then Lemma 1 implies that any strictly increasing chain of ideals containing I must terminate after at most $||I||$ steps, so R is Noetherian. Moreover, if $\mathfrak{p}$ is any nonzero prime ideal of R, then $R/\mathfrak{p}$ is a finite integral domain, hence a field, hence $\mathfrak{p}$ is maximal. Thus the Krull dimension of R is at most one. It remains to be seen that R is a domain; if so, by hypothesis it is not a field, so

its Krull dimension is exactly one.

So assume that R is not a domain. Then the previous argument shows that all prime ideals in R are maximal; since R is Noetherian, it follows from the Akizuki-Hopkins theorem that R is Artinian and therefore admits a finite direct product decomposition

$$R \cong R_1 \times \ldots \times R_n,$$

with each R_i a local Artinian ring. If $n \geq 2$ then each R_i is of the form R/I_i for a nonzero ideal I_i of R, hence is finite, and therefore R itself is finite, contradiction. So we have reduced to the case in which R is an Artinian local ring which is not a field, say with maximal ideal $\mathfrak{m}$. We will show that such a ring satisfying (FN) is finite. Indeed, the maximal ideal $\mathfrak{m}$ in a local Artinian ring is nilpotent, so it suffices to show that each of the filtered quotients $\mathfrak{m}_i/\mathfrak{m}_{i+1}$ is finite. But each is a finitely generated module over the finite field $k = R/\mathfrak{m}$.

In particular, any abstract number ring has a field of fractions, which we shall invariably denote by K. We let $\tilde{R}$ be the normalization (a.k.a. integral closure) of R in K, which by the Krull-Akizuki thoerem is a Dedekind domain.

1.3. **Examples of abstract number rings.**

There are two basic examples of abstract number rings:

Example 1: The ring $\mathbb{Z}$ of integers. In this case the norm map can be viewed as the identity map on the positive integers.

Example 2: For any prime number p, the ring $\mathbb{F}_p[t]$ of polynomials over the finite field of order p. This is a PID so every nonzero ideal I has a unique monic generator $P(t)$, say of degree $d \geq 0$. Clearly then we have $||I|| = p^d$. An obvious difference is that in this case the norm function takes only p-power values.

We can build on these examples using the following results.

Theorem 3. *(*[LM, Thm. 2.3]*) Let R be an abstract number ring with fraction field K, L/K a finite field extension, and S any ring with $R \subset S \subset L$. Then S is, if not a field, an abstract number ring. In particular, the normalization of an abstract number ring is a Dedekind abstract number ring.*

Proof: Suppose $R \subset S \subset L$, with S not a field. Certainly S is infinite; moreover, by the Krull-Akizuki theorem, S is Noetherian of dimension one, so it remains to see that S has property (FN). If $\mathfrak{q} \in \Sigma(S)$, then by [Multiplicative Ideal Theory, Lemma 9.1] $\mathfrak{p} := \mathfrak{q} \cap R \in \Sigma(R)$. Moreover, Krull-Akizuki also gives us that $S/\mathfrak{q}$ is a finite length module over $R/\mathfrak{p}$, hence is a finite-dimensional vector space over a finite field, so $||\mathfrak{q}|| < \infty$.

Corollary 4. *Let R be a domain which is infinite and finitely generated as a $\mathbb{Z}$-module. Then R is an abstract number ring, its quotient field K is an algebraic number field, and R is a finite index subring of $\mathcal{O}_K$, the normalization of $\mathbb{Z}$ in K.*

The rings in Corollary 4 are often referred to as **orders** in number fields.

Corollary 5. *Let X be an integral affine curve over a finite field k. Then the affine coordinate ring $R = k[X]$ is an abstract number ring.*

The two classes of examples treated by Corollaries 4 and 5 – i.e., orders in number fields, and coordinate rings of integral affine curves over finite fields – are the ones of most interest in number theory and arithmetic geometry. My main interest here is to what extent one can develop a theory at the level of generality of abstract number rings which specializes to recover (and perhaps, extend) the usual algebraic number theory applied to these orders in global fields.

On the other hand there are also "local examples". For instance, all of the rings $\mathbb{Z}[1/p]$, $\mathbb{Z}_{(p)}$ (i.e., $\mathbb{Z}$ localized at $\mathbb{Z} \setminus (p)$ and $\mathbb{Z}_p$ (the ring of p-adic integers) are abstract number rings. In general:

Proposition 6. *Let R be an abstract number ring.*
a) If S is a multiplicatively closed subset, then the localization $S^{-1}R$ is, if not a field, an abstract number ring.
b) If $\mathfrak{p}$ is a nonzero (hence maximal) prime ideal of R, then the completion $\hat{R}_{\mathfrak{p}}$ of R at $\mathfrak{p}$ is an abstract number ring.

Proof: a) Let $\iota : R \to S^{-1}R$ denote the canonical localization map. For any ideal I of $S^{-1}R$, we have $I = \iota_* \iota^* I$, hence ι induces an isomorphism $R/\iota^*(I) \to S^{-1}R/I$. Moreover, since I is nonzero, it contains some element $\frac{x}{s}$ with $0 \neq x \in R$, $s \in S$, and then $x \in I$ so $I \neq 0$.
b) ...

A result of Levitz and Mott gives a sort of converse.

Theorem 7. *Let R be a domain with integral closure $\tilde{R}$. TFAE:*
(i) R is an abstract number ring.
(ii) $\tilde{R}$ is a Dedekind domain and for all $\mathfrak{p} \in \Sigma(R)$, $R_{\mathfrak{p}}$ is an abstract number ring.

Proof: See [LM, Thm. 2.7].

Question 1. *Is there an abstract number ring which does not arise from our two basic examples – $\mathbb{Z}$ and $\mathbb{F}_p[t]$ – via any combination of the above constructions?*

I suspect this question has a negative answer. Indeed, we will see shortly that every abstract number ring built up from $\mathbb{Z}$ or $\mathbb{F}_p[t]$ using the above processes will have finite Picard group, whereas I do not see any reason why the Picard group of a general abstract number ring should be finite.

1.4. **Multiplicative properties of the norm.**

Lemma 8. *Let R be a DVR with maximal ideal $\mathfrak{m} = (\pi)$. For all $k \in \mathbb{N}$, the R-modules $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ are isomorphic.*

Proof: Multiplication by π^k is a surjective R-module homomorphism from R to $\mathfrak{m}^k$. Passing to the quotient, we get an isomorphism $R/\mathfrak{m} \to \mathfrak{m}^k/\mathfrak{m}^{k+1}$.

This immediately implies:

Corollary 9. *Let R be an abstract number ring which is a DVR. If $q = \#A/(\pi)$, then for all $n \in \mathbb{N}$,*

$$||(\pi^n)|| = q^n.$$

A function $f : \mathcal{I}(R) \to \mathbb{R}^+$ is **multiplicative** if for any comaximal ideals I and J – i.e., such that $I + J = R$ – we have $f(IJ) = f(I)f(J)$. A function $f : \mathcal{I}(R) \to \mathbb{R}^+$ is **completely multiplicative** if $f(IJ) = f(I)f(J)$ holds unrestrictedly, i.e., if it is a homomorphism of monoids.

Theorem 10. *Let R be an abstract number ring.*
a) The norm function is multiplicative.
b) The norm function is completely multiplicative iff R is normal.

Proof: Part a) follows immediately from the Chinese Remainder Theorem:

$$||IJ|| = \#(R/IJ) = \#(R/I) \cdot \#(R/J) = ||I||\ ||J||.$$

b) Suppose that R is normal, i.e., a Dedekind domain. Then every $I \in \mathcal{I}(R)$ is (uniquely) a product of prime ideals, so that it suffices to check that if $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of R, then $||\mathfrak{pq}|| = ||\mathfrak{p}||\ ||\mathfrak{q}||$. If $\mathfrak{p} \neq \mathfrak{q}$, then $\mathfrak{p}$ and $\mathfrak{q}$ are comaximal, so this is covered by part a). The other case to consider is $\mathfrak{p} = \mathfrak{q}$. Here we use the fact that since R is normal, so is its localization $R_{\mathfrak{p}}$, which is therefore a DVR. We then have

$$R/\mathfrak{p}^2 \cong R_{\mathfrak{p}}/(\mathfrak{p}R_{\mathfrak{p}})^2$$

and

$$R/\mathfrak{p} \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}},$$

so if $q = \#R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, then by Lemma 8 we have

$$||\mathfrak{p}^2|| = q^2 = ||\mathfrak{p}||^2,$$

and the result follows.

The converse is a result of Butts and Wade [BW].

2. The conductor

Let R be a one-dimensional Noetherian domain, with normalization $\tilde{R}$. We define the **conductor**

$$\mathfrak{f} = \{x \in R \mid x\tilde{R} \subset R\}.$$

The conductor is an ideal of $\tilde{R}$ which is, at the same time, an ideal of R. In fact, one characterization of $\mathfrak{f}$ is as the largest such "self-contracting" ideal of $\tilde{R}$.

Proposition 11. *(See handout 5 in Math8430) Let R be a one-dimensional Noetherian domain and let $\tilde{R}$ be its normalization. Then $\tilde{R}$ is finitely generated as an R-module iff the conductor ideal $\mathfrak{f}$ of $\tilde{R}/R$ is nonzero.*

3. Zeta function of an abstract number ring

Let R be an abstract number ring. We define its **zeta function** by

$$\zeta_R(s) = \sum_{I \in \mathcal{I}(R)} ||I||^{-s}.$$

In order for this to make even formal sense, we need the following result.

Lemma 12. *Let R be an abstract number ring and $N \in \mathbb{Z}^+$. Then the set*

$$\{I \in \mathcal{I}(R) \mid ||I|| = N\}$$

is finite.

Proof: Choose any $N+1$ distinct elements $x_1, \ldots, x_{N+1}$ of R, and let

$$S = \{x_i - x_j \mid i \neq j\}.$$

Note that S is a finite set consisting of nonzero elements of R, say $y_1, \ldots, y_M$. For each $1 \leq i \leq M$ it follows from Lemma 1 that there are only finitely many ideals I of R containing y_i, so overall the set of all ideals containing some element of S is finite. But if I is any ideal of norm N, then by the pigeonhole principle, $I \cap S$ is nonempty.

Thus, for each $n \in \mathbb{Z}^+$, $a_n = \{I \in \mathcal{I}(R) \mid ||I|| = n\}$ is a natural number, and we can rewrite $\zeta(s)$ as the formal Dirichlet series[1]

$$\zeta_R(s) = \sum_n \frac{a_n}{n^s}.$$

Things would certainly be more interesting however if $\zeta_R(s)$ defined a convergent Dirichlet series in some right half-plane $\Re(s) > \sigma$. Recall that for this to occur it is sufficient that the coefficients satisfy a polynomial growth condition: e.g. if $a_n = O(n^c)$ then the Dirichlet series converges absolutely for all $\Re(s) > c+1$.

Example ($R = \mathbb{Z}$). Here we have $a_n = 1$, so $\zeta_R(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ is nothing else than the Riemann zeta function. From the above, it is absolutely convergent for $\Re(s) > 1$, and is well-known to have a pole at $s = 1$.

Example (zeta function of a DVR): Suppose that R is an abstract number ring and also a discrete valuation ring. Then R has a unique prime ideal, say $\mathfrak{p} = (\pi)$; put $q = ||\mathfrak{p}||$. By Lemma 8 all nonzero ideals in R are of the form (π^n) for $n \in \mathbb{N}$, and $||(\pi)^n|| = q^n$. Therefore

$$\zeta_R(s) = \sum_{n \in \mathbb{N}} q^{-ns} = \frac{1}{1 - q^{-s}}.$$

Example: ($R = \mathbb{Z}$, continued). Unique factorization gives the well-known identity

$$\zeta_{\mathbb{Z}}(s) = \sum_n \frac{1}{n^s} = \prod_p \sum_{n=0}^{\infty} p^{-ns} = \prod_p \frac{1}{1 - p^{-s}} = \prod_p \zeta_{\mathbb{Z}_p}(s).$$

Thus we have a factorization of the "global" zeta function $\zeta_{\mathbb{Z}}$ into the product of the local zeta functions, i.e., the products over the completions of $\mathbb{Z}$ at all nonzero prime ideals.

Example: ($R = \mathbb{F}_p[t]$). We have $a_n = 0$ unless n is a power of p, whereas a_{p^k} is equal to the number of monic polynomials of degree k, namely p^k. Thus

$$\zeta_R(s) = \sum_k \frac{p^k}{p^{ks}} = \sum_k (p^{1-s})^k = \frac{1}{1 - p^{1-s}}.$$

In view of the $R = \mathbb{Z}$ case, it is natural to try to express this as a product of local zeta functions. For any positive integer d, let N_d be the number of prime ideals of

[1]Unless otherwise specified, by $\sum_n \frac{a_n}{n^s}$, we understand the summation to be taken over all positive integers.

R of norm p^d. Then

$$\prod_{\mathfrak{p}} \zeta_{R_{\mathfrak{p}}}(s) = \prod_{d=1}^{\infty} \left(1 - p^{-ds}\right)^{-N(d)}.$$

Unlike the case of $R = \mathbb{Z}$, it is not visibly obvious whether this expression is equal to the global zeta function, in part because it is not clear what the numbers $N(d)$ are.

Nevertheless, we can easily derive the following result.

Theorem 13. *(Factorization of the zeta function, normal case) Let R be a normal abstract number ring. Write ζ for the zeta function $\zeta_R(s)$, and for $\mathfrak{p} \in \Sigma(R)$, write $\zeta_{\mathfrak{p}}$ for the zeta function of the DVR $R_{\mathfrak{p}}$. Then*

$$\zeta = \prod_{\mathfrak{p} \in \Sigma(R)} \zeta_p. \tag{1}$$

Proof: The right hand side of (1) is

$$\prod_{\mathfrak{p} \in \Sigma(R)} (1 - ||\mathfrak{p}||^{-s})^{-1} = \prod_{\mathfrak{p} \in \Sigma(R)} \sum_{n \in \mathbb{N}} ||\mathfrak{p}||^{-ns} \stackrel{*}{=} \prod_{\mathfrak{p} \in \Sigma(R)} \sum_{n \in \mathbb{N}} ||\mathfrak{p}^n||^{-s} \stackrel{**}{=} \zeta(s).$$

The first starred equality follows from the complete multiplicativity of the norm map in the normal case, whereas the second starred equality follows from this together with the unique factorization of a nonzero ideal in a Dedekind domain into primes.

What about the non-normal case?

References

[BW] H.S. Butts and L.I. Wade, *Two criteria for Dedekind domains*. Amer. Math. Monthly 73 1966 14–21.

[CL] K.L. Chew and S. Lawn, *Residually finite rings*. Canad. J. Math. 22 1970 92–101.

[LM] K.B. Levitz and J.L. Mott, *Rings with finite norm property*. Canad. J. Math. 24 (1972), 557–565.

[Nar] Narkiewicz.