

THE ALGEBRAIC METHOD

0.1. **Integral Domains.** Emmy Noether and others quickly realized that the classical algebraic number theory of Dedekind could be abstracted completely. In particular, rings of integers can be seen as examples of a purely algebraic object called a Dedekind domain. Thus to study the algebraic method we need to meet a host of new algebraic objects and discover their properties; often in a setting that is much more abstract than the familiar subfields of complex numbers that we have been dealing with.

At the most general level, a ring of integers \mathcal{O}_K of a number field K is an example of an integral domain in its field of fractions.

Note: since all the rings we meet for the time being will have identity and be commutative and have identities mapped to each other by homomorphisms, we include these in our definition of a ring unless explicitly stated.

Definition 0.1.1. *An integral domain A is a ring which has no zero divisors (i.e.: no $a, b \in A$ with $ab = 0$, unless of course a or b is zero).*

Consider the set of all formal fractions of an integral domain A ,

$$(1) \quad A_{\text{frac}} = \left\{ \frac{a}{b} : a, b \in A, b \neq 0 \right\}.$$

We can define addition and multiplication of fractions as we normally would

$$(2) \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

However, we also want to identify fractions that ought to be the same, e.g:

$$(3) \quad \frac{am}{bm} = \frac{a}{b};$$

and we want to identify $a \in A$ with the fraction $\frac{a}{1}$. Once we have made these identifications, which we can denote by the equivalence relation \sim , then A_{frac}/\sim is a field, with A embedded in it.

Definition 0.1.2. *The field $K = A_{\text{frac}}/\sim$ is called the quotient field of A . The integral domain A is embedded in it by means of the identification $a \mapsto \frac{a}{1}$.*

As we did for rings of integers, we can define divisibility for an arbitrary integral domain A . This leads to a concept of associated elements and units, as before.

Units are best thought of as the elements of A which have a multiplicative inverse. The set of units U of an integral domain A is a group, since each unit by definition has an inverse. We write this group A^\times .

For each $\alpha \in K$ we can define a fractional principal ideal (α) of K , exactly as we did before. The ideal (α) is often written αA in this context, reminding one of the definition.

The set P of non-zero fractional principal ideals is a group under the operation $\alpha A \cdot \beta A = \alpha\beta A$. Two ideals αA and βA are identical iff α and β are associates, i.e: there is a unit ϵ such that $\alpha = \epsilon\beta$. Thus there is a 1-1 correspondence between principal fractional ideals, and elements of the quotient field modulo units. Thus we have

Theorem 0.1.3. *As groups*

$$(4) \quad P \cong K^\times / U.$$

Once again we are interested in unique factorization. One kind of integral domain with unique factorization is a principal ideal domain.

Definition 0.1.4. *An integral domain A is a principal ideal domain (PID) if all its ideals are principal, i.e: each ideal can be expressed in the form $I = \alpha A$ for some $\alpha \in K$.*

Definition 0.1.5. *A prime element $p \in A$ of an integral domain is one such that pA has only the factors pA and A , and p is not a unit in A .*

Clearly in a principal ideal domain, p is prime iff pA is maximal with respect to inclusion, amongst ideals not equal to A . For suppose pA is properly contained in an ideal mA not equal to A . Then since p belong to mA we must have $p = mn$ for some $n \in A$, not a unit. But then $pA = mA \cdot nA$ and p is not prime.

Theorem 0.1.6. *If pA is maximal in A , then A/pA is a field.*

Proof: Consider any $\alpha \in A$ not in pA . Since pA is maximal, the element 1 can be expressed as

$$(5) \quad 1 = a\alpha + b\rho \text{ with } a, b \in A, \rho \in pA.$$

Modding out by pA , the element ρ goes to zero. Thus the class of A is an inverse for the class of α in A/pA . But the class of α is an arbitrary non-zero class in A/pA . The result follows. \square

We have the well known result

Theorem 0.1.7. *Every principal ideal domain has unique factorization into prime elements.*

Proof: Each ideal is contained in a maximal ideal. For let $I_1 \subset I_2 \subset I_3 \subset \dots$ be an infinite sequence where the inclusions are strict. Now $I = \bigcup I_i$ is an ideal and hence principal, generated by α say. But α must be in one of the I_n and thus $I = I_n$, a contradiction. This also proves that any factorization of an ideal has only finitely many factors appearing in it.

Now suppose pA divides abA for a prime p , but not aA . Since pA is maximal, $1 = xp + ya$ for some $x, y \in A$. Thus $b = bxp + yab$. But $ab = zp$ for some $z \in A$ and thus pA divides bA . Unique factorization follows from this result as per the standard argument. \square

0.2. Ideals. We now proceed to the definition of ideals for general rings (not necessarily finitely generated or void of zero divisors). In the special case of rings of integers this definition will be equivalent to what we had before.

Definition 0.2.1. *An ideal J of a ring A is a subset of A such that*

- (i) *For any $a, b \in J$ we have $a + b \in J$;*
- (ii) *For $b \in J$ and any $a \in A$ we have $ab \in J$.*

We need to be careful in defining ideal multiplication for such rings, since they may not have finite sets of generators in general. Rather we let

$$(6) \quad JJ' = \left\{ \sum_{i=1}^n a_i a'_i : a_i \in J, a'_i \in J', n \in \mathbb{Z}_{>0} \right\}.$$

We also need to be careful about saying that an ideal is a factor of another. For rings of integers, we had that, for an ideal to divide another was equivalent to the first ideal containing the other. However, in general, whilst it is clear that if $J = J_1 J_2$ then $J_1 \supseteq J$, the converse is not at all clear.

We can define addition of ideals

$$(7) \quad J + J' = \{a + a' : a \in J, a' \in J'\}.$$

It is clear that ideal addition is associative.

Note that $J + J'$ contains J and J' , and if any ideal contains both of these then it contains $J + J'$. However for the reasons just outlined, we cannot call $J + J'$ a greatest common divisor as we did in the case of rings of integers.

For similar reasons we must distinguish the following two concepts.

Definition 0.2.2. *An ideal J of a ring A is irreducible if it has no factors other than A or J .*

Definition 0.2.3. *An ideal P is prime if it is necessarily the case given any $ab \in P$ with $a, b \in A$ that either $a \in P$ or $b \in P$.*

Theorem 0.2.4. *The ideal P is prime iff A/P is an integral domain.*

Proof: We have $(a + P)(b + P) \in P$ iff $ab \in P$. The result follows from the definitions of an integral domain and a prime ideal. \square

Definition 0.2.5. *An ideal M is maximal in the ring A if $M \neq A$ and if there is no ideal J with $M \subset J \subset A$.*

It was unnecessary in theorem (0.1.6) to assume that the maximal ideal was principal. Therefore the theorem applies for maximal ideals of rings in general.

Theorem 0.2.6. *Any maximal ideal M is prime.*

Proof: Suppose $ab \in M$. If $a \notin M$ then since M is maximal $1 = ax + my$ for $m \in M$ and $x, y \in A$. Thus $b = abx + bym \in M$. \square

0.3. Noetherian Rings. We can already see that having finitely generated rings was exceptionally useful in our development of the theory of algebraic integers. We investigate rings with this property.

Definition 0.3.1. *A ring A is Noetherian if all its ideals are finitely generated.*

We investigate what turns out to be equivalent.

Definition 0.3.2. *A ring is said to satisfy the ascending chain condition if each ascending chain of ideals*

$$(8) \quad A_1 \subseteq A_2 \subseteq \dots$$

eventually becomes stable, i.e. $A_i = A_n$ for all $i \geq n$ for some particular value of n .

Theorem 0.3.3. *A ring R is Noetherian iff it satisfies the ascending chain condition.*

Proof: If all ideals are finitely generated, let A_i be an ascending chain of ideals. Let $A = \bigcup A_i$. It is an ideal, hence finitely generated by $\alpha_1, \alpha_2, \dots, \alpha_n$ say. But one of the A_i will contain all the α_i and we are done.

Conversely, let R satisfy the ascending chain condition. If A is an ideal of R which is not finitely generated, then there is a sequence of elements $\alpha_i \in A$ such that $(\alpha_1) \subset (\alpha_1, \alpha_2) \subset (\alpha_1, \alpha_2, \alpha_3) \subset \dots$ with all inclusions proper. But this contradicts the ascending chain condition. \square

Theorem 0.3.4. *For an integral domain A which is Noetherian, every non-zero element of A which is not a unit can be written (not necessarily uniquely) as the product of irreducible elements.*

Proof: Let $a \in A$ generate an ideal aA , which is maximal among principal ideals coming from elements that are not decomposable in the required manner. We can make the assumption that such an ideal exists since A is Noetherian. But $a = bc$, with $b, c \in A$ not units, since a is not irreducible. But $bA \supset aA$ and $cA \supset aA$, therefore by the maximality of aA amongst ideals of the given type, b and c are expressible in terms of irreducibles. But then so is their product, a . We have a contradiction. \square

Theorem 0.3.5. *Every principal ideal domain is Noetherian.*

Proof: Each ideal is generated by a single element. \square

Recall that we noted that a ring of integers \mathcal{O}_K has a \mathbb{Z} -basis of n elements where n is the degree of the number field K . Also note that our former definition of ideal included the condition that it be finitely generated. We wish to use our current definition of ideal, which does not make this assumption, and using only the result about the ring of integers itself, show that its ideals also have a finite \mathbb{Z} -basis and are thus finitely generated.

To prove this result we proceed completely algebraically and establish a general result which will be important later. To proceed we introduce the notion of Noetherian modules.

Before doing this however, let us recall a few elementary facts about modules.

0.4. R-Modules. Recall that an R -module M for a ring R is an Abelian group which has a multiplication by R defined on it, compatible with the group law in M .

We say M is finitely generated if there exist $x_1, x_2, \dots, x_n \in M$ such that every element x of M can be expressed in the form

$$(9) \quad x = a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

with the $a_i \in R$. Sometimes we write symbolically

$$(10) \quad M = Rx_1 + Rx_2 + \cdots + Rx_n.$$

An R -module can be thought of as a vector space over a ring R instead of a field.

Any Abelian group M can be made into a \mathbb{Z} -module by defining nx for $n \in \mathbb{Z}, x \in M$ to be $x + x + \cdots + x$. We tend to think of \mathbb{Z} -modules and Abelian groups as being the same thing. For example, it is true that a \mathbb{Z} -submodule of M is just an ordinary subgroup of M , made into a \mathbb{Z} -module.

Any ring R can be made into an R -module in the obvious way. Any R -submodule of R is the same thing as an ideal of R , made into an R -module.

One must be careful if one considers an R -module as an R' -module for some other ring R' . The R -submodules are not the same as the R' -submodules. In particular an R -submodule is a \mathbb{Z} -submodule (i.e: a subgroup), but the converse is not necessarily true.

0.5. Noetherian Modules.

Definition 0.5.1. *For a ring R , an R -module M is said to satisfy the ascending chain condition for modules if every ascending chain of R -submodules of M*

$$(11) \quad M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

eventually stabilizes.

Definition 0.5.2. An R -module M is said to be Noetherian if every R -submodule of M is finitely generated.

Theorem 0.5.3. Modules satisfy the ascending chain condition iff they are Noetherian.

Proof: Exactly as for rings and ideals. \square

Note: for a ring R considered as an R -module, the definitions of Noetherian for modules and rings coincide. For, an ideal of a ring R is essentially the same thing as a submodule of R when R is considered as an R -module. Also the ascending chain condition on the one implies it for the other.

Theorem 0.5.4. A submodule or quotient module of a Noetherian R -module M is Noetherian.

Proof: If N is a submodule of M , all its submodules are also submodules of M and we are done for the first part.

If M'_1 and M'_2 are submodules of M/N then consider the submodules M_1 and M_2 of M created by taking all elements of M whose classes are in the respective M' . Clearly if $M'_1 \subseteq M'_2$ then $M_1 \subseteq M_2$. Thus the ascending chain condition on M implies it on M/N . \square

A partial converse is

Theorem 0.5.5. If N is a submodule of an R -module M with N and M/N both Noetherian, then M is Noetherian.

Proof: If M' is a submodule of M , then $M' + N$ contains N and thus $(M' + N)/N$ is a submodule of M/N . But since the latter is Noetherian there exist elements x_1, x_2, \dots, x_n such that their classes modulo N generate $(M' + N)/N$. Thus for any $y \in M'$ there exist $a_1, a_2, \dots, a_r \in R$ such that $y - \sum_{i=1}^n a_i x_i \in N$. But this value is also in M' . Now N is Noetherian and $M' \cap N$ is a submodule, thus generated by y_1, y_2, \dots, y_m say. Thus there exist $b_1, b_2, \dots, b_m \in R$ such that $y - \sum_{i=1}^n a_i x_i = \sum_{j=1}^m b_j y_j$. But y was arbitrary in M' and hence $\{x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m\}$ generates M' . Also M' was an arbitrary submodule of M and thus M is Noetherian. \square

Corollary 0.5.6. If M_1, M_2, \dots, M_n are Noetherian R -modules, then $\prod M_i$ is Noetherian.

Proof: It suffices to show it for $n = 2$ and proceed by induction. Now M_1 is a Noetherian submodule of $M_1 \times M_2$. The quotient $M_1 \times M_2 / M_1 \cong M_2$ is also Noetherian. Hence by the theorem, so is $M_1 \times M_2$. \square

Theorem 0.5.7. If R is a Noetherian ring and M a finitely generated R -module, then it is Noetherian.

Proof: M is a quotient of a free R -module on n generators say. I.e: $M \cong R^n/N$ with N some submodule of R^n . Since R^n is Noetherian by the corollary, then the result follows from theorem (0.5.4). \square

Theorem 0.5.8. *The ring of integers \mathcal{O}_K of an algebraic number field is Noetherian as a \mathbb{Z} -module.*

Proof: Note \mathbb{Z} is a Noetherian ring. Therefore since \mathcal{O}_K is a finitely generated Abelian group, i.e: a finitely generated \mathbb{Z} -module, \mathcal{O}_K is a Noetherian \mathbb{Z} -module. \square

Note that we can say more. For, every \mathcal{O}_K -submodule of \mathcal{O}_K is certainly a subgroup, i.e: a \mathbb{Z} -submodule, i.e: each \mathcal{O}_K -ideal is a \mathbb{Z} -submodule. But since \mathcal{O}_K is a Noetherian \mathbb{Z} -module, each ideal must be a finitely generated \mathbb{Z} -submodule, and therefore certainly finitely generated as an \mathcal{O}_K -submodule. Thus \mathcal{O}_K is Noetherian as an \mathcal{O}_K -module. That is

Corollary 0.5.9. *Every ring of integers \mathcal{O}_K is a Noetherian ring.*

0.6. Fractional Ideals. We can define fractional ideals for an integral domain A in its field of quotients.

Definition 0.6.1. *An A -module M contained in K is a fractional ideal if there is a non-zero $a \in A$ such that $a \cdot M \subseteq A$. If we can take $a = 1$ we call it an integral ideal, the definition agreeing with what we had previously.*

We define ideal multiplication as we did for integral ideals. There is no need for fractional ideals to be invertible in general. Eventually we will investigate systems where this is the case. For now we merely note that ideal multiplication is commutative, associative and that A acts as an identity.

We say that a fractional ideal M divides another N when there is an integral ideal J such that $N = MJ$.

0.7. Integrality. There is a second property of rings of integers that is essential to their usefulness. It is the property that each element $\alpha \in \mathcal{O}_K$ is integral over \mathbb{Z} . We investigate this property for general rings.

Definition 0.7.1. *Let A and R be rings with $A \subseteq R$. An element $x \in R$ is said to be integral over A if it satisfies some*

$$(12) \quad x^n + a_1x^{n-1} + \cdots + a_n = 0,$$

for $a_i \in A$.

Theorem 0.7.2. *The following are equivalent*

- (i) $x \in R$ is integral over A ;
- (ii) $A[x]$ is a finitely generated A -module;
- (iii) $A[x] \subseteq B$ a subring of R which is also a finitely generated A -module.

Proof: (i) \rightarrow (ii) From $x^n + a_1x^{n-1} + \dots + a_n = 0$, any power of x higher than $n - 1$ can be expressed in terms of $\{1, x, x^2, \dots, x^{n-1}\}$.

(ii) \rightarrow (iii) Take $B = A[x]$.

(iii) \rightarrow (i) Let y_1, y_2, \dots, y_n generate B . Then $xy_i \in B$, thus there exist $a_{ij} \in A$ such that $xy_i = \sum_{j=1}^n a_{ij}y_j$. Considering these as n equations in n unknowns y_i , the resulting coefficients have determinant zero, the expression of which is a monic polynomial in x . Thus x is integral over A . \square

Definition 0.7.3. A ring A is integral over a subring A if every element of R is integral over A .

Theorem 0.7.4. If $A \subset B \subset C$ are rings and B is a finitely generated A -module, C a finitely generated B -module, then C is a finitely generated A -module.

Proof: If $\{\beta_1, \beta_2, \dots, \beta_m\}$ generate B over A and $\{\gamma_1, \gamma_2, \dots, \gamma_n\}$ generate C over B , then $\{\beta_1\gamma_1, \beta_1\gamma_2, \dots, \beta_m\gamma_n\}$ generate C over A . \square

Theorem 0.7.5. If A is a subring of B , the set of elements of B integral over A is a ring.

Proof: If $\alpha, \beta \in B$ are integral over A , then $A[\alpha]$ is a finitely generated A -module. Now $A[\alpha\beta] \subseteq A[\alpha, \beta] = A[\alpha][\beta]$. Now β is integral over A , so certainly integral over $A[\alpha]$ and thus this final ring is finitely generated as an $A[\alpha]$ -module. Upon application of the previous theorem $A[\alpha\beta]$ is contained in a ring which is a finitely generated A -module. Thus $\alpha\beta$ is integral over A . The same argument applies for $\alpha \pm \beta$ and thus the result follows. \square

We often apply this result to a number field $B = K$. Then setting $A = \mathbb{Z}$ tells us that the elements of K integral over \mathbb{Z} , i.e: \mathcal{O}_K , is a ring.

Definition 0.7.6. The set of elements of B integral over A is called the integral closure of A in B .

Recall that a number field K was the field of quotients of its ring of integers \mathcal{O}_K . In fact we can prove the following in ways already described in the algebraic number theory notes.

Theorem 0.7.7. Let A be an integral domain with field of fractions K , and L some extension field of K . If $\alpha \in L$ is algebraic over K then there exists $d \in A$ such that $d\alpha$ is integral over A .

Corollary 0.7.8. In the theorem, if B is the integral closure of A in L , the B has field of quotients L .

Proof: Since $d\alpha \in B$ for any algebraic α and suitable $d \in A$, then $\alpha = \frac{\beta}{d}$ for some $\beta \in B$. I.e: the arbitrary algebraic $\alpha \in L$ is in the field of quotients of B . \square

Definition 0.7.9. An integral domain A is integrally closed if it is the integral closure of itself in its field of quotients K , i.e.: $\alpha \in K$, α integral over A implies $\alpha \in A$.

Theorem 0.7.10. Any PID is integrally closed.

Proof: We prove more. Let A be any unique factorization domain. Consider the fraction $\frac{a}{b}$. If b is a unit, then $\frac{a}{b} \in A$ already. If not, assume $p \mid b$, but $p \nmid a$ and p is irreducible. Suppose $\frac{a}{b}$ is integral over A , i.e:

$$(13) \quad \left(\frac{a}{b}\right)^n + a_1 \left(\frac{a}{b}\right)^{n-1} + \cdots + a_n = 0$$

for $a_i \in A$. Multiply by a^n throughout. Now p divides all the terms except possibly a^n . But it must then also divide a^n , a contradiction. \square

We wish to show that rings of integers \mathcal{O}_K are integrally closed. We will prove

Theorem 0.7.11. The integral closure B of an integral domain A in an algebraic extension L of its field of fractions K , is integrally closed.

Proof: We need to show that any $\gamma \in L$ integral over B is actually in B . We do this by showing that γ is actually integral over A and hence in B . We need the lemma

Lemma 0.7.12. If $A \subset B \subset C$ are integral domains and B is integral over A , C integral over B , then C is integral over A .

Proof: If $\gamma \in C$, then since it is integral over B

$$(14) \quad \gamma^n + b_1 \gamma^{n-1} + \cdots + b_n = 0 \text{ for } b_i \in B.$$

Let $B' = A[b_1, b_2, \dots, b_n]$, then B' is finitely generated as an A -module (as we have seen before), so $B'[\gamma]$ is finitely generated as an A -module, since γ is integral over B' . Thus γ is integral over A by theorem (0.7.2). $\square\square$

0.8. Dedekind Domains. It turns out that there is one other property of rings of integers which is indispensable. It is the condition that every non-zero prime ideal is maximal. The proof of this fact is not trivial for rings of integers. In fact it is better to develop Dedekind domains first, then prove this property later.

One ring which does obviously have this property however, is the ring \mathbb{Z} . In fact \mathbb{Z} is the first clear example of a Dedekind domain.

Definition 0.8.1. An integral domain A is a Dedekind domain if

- (i) A is Noetherian, i.e.: all its ideals are finitely generated,
- (ii) A is integrally closed, i.e.: it is its own integral closure in its field of fractions; and
- (iii) Every non-zero prime ideal is maximal.

Later we use the fact that \mathbb{Z} is a Dedekind domain and that a ring of integers \mathcal{O}_K is the integral closure of \mathbb{Z} in an algebraic number field K , to prove that \mathcal{O}_K is a Dedekind domain.

Dedekind, Noether, Krull and Matusita are responsible for the following theorem which shows why Dedekind domains are so useful, and which allows us to characterize them fully.

Theorem 0.8.2. *The following are equivalent*

- (i) *A is a Dedekind domain.*
- (ii) *The set of integral ideals of A has unique factorization into prime ideals.*
- (iii) *Every integral ideal of A can be expressed as a product of prime ideals.*
- (iv) *The set of non-zero fractional ideals in A is a multiplicative Abelian group.*

Note that a Dedekind domain isn't necessarily a ring of integers of an algebraic number field; it is a more general abstract algebraic object, of which the latter turns out to be an example.

We now prove

Theorem 0.8.3. *In a Dedekind domain, an ideal being prime is equivalent to it being irreducible.*

Proof: Suppose P is reducible, $P = JJ'$. Then $P \subset J$ and $P \subset J'$ with strict inclusions. Thus there exist $a \in J, a' \in J'$ with $a \notin P, a' \notin P$ but $aa' \in JJ' = P$ and so P is not prime.

Conversely if J is irreducible in a Dedekind domain, then when it is expressed as the product of primes, it can only have a single prime in its decomposition, i.e: J must be prime. \square

Theorem 0.8.4. *For fractional ideals in a Dedekind domain A , "to divide is to contain".*

Proof: We already know that if $M \mid M'$ then $M \supseteq M'$. Conversely if $M \supseteq M'$ then $A = MM' \supseteq M'M^{-1}$. Thus $(M'M^{-1})M = M'$ with $M'M^{-1}$ integral, i.e: $M \mid M'$. \square

As noted before, this theorem allows us to call $M + M'$ the greatest common divisor of M and M' . In like manner, $M \cap M'$ acts as the least common multiple of M and M' .

We already know that a PID is a unique factorization domain and hence a Dedekind domain. However, the converse is also true.

Theorem 0.8.5. *A Dedekind domain with unique factorization on its elements is a PID.*

Proof: Let $0 \neq a \in P$, with P a prime ideal, be given. Let $a = \prod_{i=1}^r p_i^{e_i}$ be its unique factorization into primes. Since P is prime and $a \in P$, then $p_i \in P$ for some i . Thus $Ap_i \subseteq P$. But Ap_i is prime, for if $a, b \in A$

with $ab \in Ap_i$ then $p_i \mid ab$, and since A has unique factorization, $p_i \mid a$ or $p_i \mid b$. But all prime ideals are maximal and since $Ap_i \subseteq P$ we must have equality. Thus the arbitrary prime ideal P is principal and so all ideals are principal. That is, we have a PID. \square

Just as we had for rings of integers, we have

Theorem 0.8.6. *Let M be a non-zero fractional ideal in a Dedekind domain A . Then there exists a fractional ideal M' such that MM' is a given principal ideal.*

Proof: If $aA \neq 0$ is given, then $M' = aM^{-1}$ will do. \square

Theorem 0.8.7. *If A is a Dedekind domain, then every fractional ideal of A can be generated by at most two elements.*

Proof: We prove it for integral ideals J , but it then clearly follows for fractional ideals. We will show that for any other ideal J' , there is a $b \in A$ such that $A = J' + J^{-1} \cdot Ab$. Then we can select $J' = J^{-1} \cdot Aa$ with $a \in J$ so that J' is integral. Then clearly multiplying by J we have, $J = Aa + Ab$ (read greatest common divisor for addition here).

Thus let $J' = \prod_{i=1}^r P_i$. Also let $J_i = JP_1P_2 \dots P_rP_i^{-1}$. If $b_i \in J_i, b_i \notin J_iP_i$ then clearly $P_i \nmid Ab_i$ but $J_i \mid Ab_i$, thus $A = P_i^{e_i} + Ab_iJ_i^{-1}$.

Let $b = b_1 + b_2 + \dots + b_r$. Now $b \notin JP_i$ for every $i = 1, 2, \dots, r$. For $b_j \in J_j \subseteq JP_i$ for every $i \neq j$, since $JP_i \mid J_j$ for $i \neq j$. But $b_j \notin J_jP_j$, i.e: $J^{-1}Ab_j \not\subseteq P_1P_2 \dots P_r$, so $J^{-1}Ab_j \not\subseteq P_j$ so $b_j \notin JP_j$.

But this means that $AbJ^{-1} \not\subseteq P_i$ for any i and then $J' = \prod P_i$ and AbJ^{-1} have no common factors. \square

Theorem 0.8.8. *If L is a finite separable extension of a field of fractions K of a Dedekind domain A , then the integral closure B of A in L is a Dedekind domain.*

Proof: We prove B is integrally closed, Noetherian and that every prime ideal is maximal. To prove the second fact, we need a lemma; the first fact having been proven already in theorem (0.7.11).

Lemma 0.8.9. *If A is an integral domain with field of quotients K , and M a free A -module over a basis of n elements, then there exists a K -vector space V containing M . Any two bases of M have the same cardinality n .*

Proof: Let $V = K\zeta_1 + K\zeta_2 + \dots + K\zeta_n$ be a K -vector space with formal basis $\zeta_1, \zeta_2, \dots, \zeta_n$. Let x_1, x_2, \dots, x_n be a basis of M as an A -module. Define $\theta(\sum_{i=1}^n a_i x_i) = \sum_{i=1}^n a_i \zeta_i$. Thus θ is an isomorphism of M to its image in V .

If $y_1, y_2, \dots, y_r \in M \subseteq V$ are linearly independent over A , then since any relation over K in V can be made into one over A in M by multiplying by a common denominator, we have $r \leq n$. Thus any basis of M has $m \leq n$ elements. But applying the argument in reverse, we

have for the original basis $n \leq m$. Thus any basis has $m = n$ elements. \square

Apply the lemma to A and K of the theorem. We first require the following lemma, which we will not prove; the proof being almost equivalent to Hilbert's theorem 5.

Lemma 0.8.10. *The integral domain B of the theorem is contained in a free A -module M of finite rank n .*

Thus by the previous lemma, B is a submodule of M of rank n . Therefore since A is a Noetherian ring, then B is therefore a Noetherian A -module, hence certainly a Noetherian B -module, i.e: a Noetherian ring, as required. \square

We now show that every non-zero prime ideal Q of B is maximal. Let $0 \neq \beta \in Q$. since B is integral over A ,

$$(15) \quad \beta^n + a_1\beta_{n-1} + \cdots + a_n = 0$$

for some $a_i \in A$. Let this polynomial be minimal so that $a_n \neq 0$. Then $\beta \mid a_n$ and so $a_n \in \beta B \cap A$. But $\beta B \subseteq Q$ thus $P = Q \cap A \neq (0)$, which is clearly prime. Thus A/P is a field, and since Q is prime, B/Q is at least an integral domain.

But now $a + P \mapsto a + Q$ makes A/P a subfield of B/Q . Since B is integral over A , reducing minimum polynomials, we see that B/Q is algebraic over A/P .

Lemma 0.8.11. *Any integral domain B containing a field k and algebraic over k is itself a field.*

Proof: Let $0 \neq \beta \in B$. Consider the map $x \rightarrow \beta x$ from the finite dimensional k -vector space $k[\beta]$ to itself. This map is injective since $\beta x = 0 \implies x = 0$, as $\beta, x \in B$ with B an integral domain. Thus the map is non-degenerate and must map linearly the vector space $k[\beta]$ surjectively onto itself. Thus there exists $\beta' \in k[\beta]$ such that $\beta\beta' = 1$. \square

Now B/Q is a field and so Q is maximal as required. \square

This theorem can now be used directly with $A = \mathbb{Z}, K = \mathbb{Q}$ to show

Theorem 0.8.12. *The ring of integers \mathcal{O}_L of an algebraic number field L is a Dedekind domain.*