Extensions of Dedekind rings

Version 0.4 — 19. september 2013 klokken 16:13

The basic object we study in algebraic number theory are the rings of integers in algebraic number fields. The main focus is on the prime ideals rings. They are all by definition extensions of the integers, *i.e.,* there is an inclusion $\mathbb{Z} \subseteq A$.

Algebraic numbers theory is not primarily made to study the primes in $\mathbb{Z}$, but it is a more relative theory. The prime ideals in A are studied in relation to the rational primes. It is therefore of the foremost interest to understand what happens to a rational prime p in A, that is, describe in one way or another the decomposition of pA as a product of prime ideals in A.

This said, it is important for many reasons to treat the general case, on being the wider scope of action it gives. Hence our setting is a Dedekind ring A with field of fractions K and a finite, separable extension L of K. The object of study is the extension of Dedekind rings $A \subseteq B$, where B is the integral closure of A in K.

The quadratic case

The quadratic case is illustrative, and it is worthwhile doing separately. The student is encourage to fill in all missing details (even the tiniest!), and be sure she understands all statements and arguments thoroughly. Understanding this special case is to grasp principle of the general case.

Assume d is square free integer, and for simplicity assume that $d \not\equiv 1 \mod 4$. Then the ring of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is $A = \mathbb{Z}[\sqrt{d}]$, and this ring may be represented as then quotient $\mathbb{Z}[x]/(x^2 - d)$. The residue class of x corresponds to $\sqrt{d}$. Given a rational prime p. Then it holds that

$$A/pA = \mathbb{Z}[x]/(x^2 - d, p) = \mathbb{F}_p[x]/(x^2 - \bar{d}),$$

as is easily seen. This ring is a two-dimensional $\mathbb{F}_p$ algebra, whose structure depends on the behavior of the quadratic polynomial $x^2 - d \mod p$. There are three different scenarios that may occur:

- *The inert case:* $x^2 - d$ is *irreducible* mod p. Then $A/pA \simeq \mathbb{F}_p[x]/(x^2 - d)$ is a field. It is an extension of $\mathbb{F}_p$ of degree 2—which one might denote $\mathbb{F}_p(\sqrt{\bar{d}})$— hence a finite field with p^2 elements. The ideal pA is a *prime ideal.*

- *The split case*: $x^2 - d$ is a product of two *different* linear factors mod p. This happens if d is a square mod p. Then $x^2 - d \equiv (x - a)(x + a) \mod p$ where $a \in \mathbb{Z}$ is such that $a^2 \equiv d \mod p$. For the algebra A/pA we have the isomorphisms

  $$A/(p)A \simeq \mathbb{F}_p[x]/((x - \bar{a})(x + \bar{a})) = \mathbb{F}_p[x]/(x - \bar{a}) \times \mathbb{F}_p[x]/(x + \bar{a}).$$

  Hence $A/(p)A$ is isomorphic to the product of two copies of $\mathbb{F}_p$. In the first copy x corresponds to $\bar{a}$ and in the second to $-\bar{a}$. It holds that $(x^2 - d, p) = (x - a, p)(x + a, p)$, and hence $(p)A$ decomposes as $(p)A = (\sqrt{d} - a, p)(\sqrt{d} + a, p)$.

☐ *The ramified case*: $x^2 - d$ is a square mod p. This happens if the *discriminant* Δ is congruent zero mod p, but as $\Delta = 4d$, this is equivalent to $p|d$ or $p = 2$. In the first case $(x^2 - d, p) = (x^2, p) = (x, p)^2$ and $(p)A = (\sqrt{d}, p)^2$, in the second $(x^2 - d, 2) = (x - \sqrt{d}, 2)^2$. In both cases the algebra A/pA is *non-reduced*; it has nilpotent elements.

PROBLEM 1. Do the same in the case $d \equiv 1 \mod 4$. ✸

The general case

The setting in the general case is as follows. We are given an Dedekind domain A and its field of fractions K. Furthermore we are given is a finite, separable field extension $\mathbb{K} \subseteq L$ whose degree $[L : K]$ we denote by n, and the integral closure of A in L is denoted by B. To summarize, we have the diagram

$$\begin{array}{ccc} K & \longrightarrow & L \\ \uparrow & & \uparrow \\ A & \longrightarrow & B \end{array}$$

Our model case—which is the all-important case as well—is the case of the ring algebraic integers in an algebraic number field. We slightly change the role of the letters, and let K denote the number field, and A the ring of integers in K, *i.e.,* A is the integral closure of $\mathbb{Z}$ in K. The picture is like this

$$\begin{array}{ccc} \mathbb{Q} & \longrightarrow & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \longrightarrow & A \end{array}$$

A FEW SIMPLE POINTS There are a few simple, but important points to make about the structure of B as an A-module.

☐ B is a finitely generated as A module.

This is the content of theorem xxx in nortes xxxx.

☐ $L = B \otimes_A K$, or stated a little differently $L = B_S$ where S is the multiplicative system $S = A \setminus \{0\}$.

One may phrase this by saying that every element in L is of the form b/a where $b \in B$ and $a \in A$. An element $\beta \in L$ satisfies a relation

$$a_r \beta^r + a_{r-1} \beta^{r-1} + \cdots + a_0 = 0$$

where the a_i's are in A, both a_r and a_0 being non-zero. Multiplying the equation by a_r^{r-1}, we see that $b = a_r \beta$ is integral over A, hence it lies in B. Therefore $\beta = b/a_r \in B_S$. In particular we have

☐ L is the field of fractions of B.

Finally,

☐ B is a torsion free A-module.

Recall B being torsion free means that if $ab = 0$ for $a \in A$ and $b \in B$, then either $a = 0$ or $b = 0$. This obviously holds since B is contained in the field L.

INTEGRAL BASISES The field L has of course many basises as a vector space over K. Some of them will have all their elements lying in B, and they are particuløarily interesting. We say that the basis $\beta_1, \ldots, \beta_n$ for L is *an integral basis* if $\beta_i \in B$ for $1 \leq i \leq n$.

Recall the *trace form* $\mathrm{tr}_{L/K}(xy)$ which is, L being separable over K, a non-degenerate quadratic form on L with values in K. We saw in prop xxx, that B is contained in the A-module spanned by the dual basis $\beta_1', \ldots, \beta_n'$. Clearly this module is a *free* A-module (well, it has a basis!!). Hence B enjoys the property

☐ B is contained in a free A-module of rank n.

THE CASE OF NUMBER RINGS We take a closer look at the all-important situation of a ring A of algebraic integers in an algebraic number field K. The theory of abelian groups, tells us that any finitely generated and torsion free abelian group is free. Thus B is free abelian group and has a basis as a $\mathbb{Z}$-module. Such a basis is of course also a basis for L over $\mathbb{Q}$ (use the second point above), so the rank of B is n, *i.e.,* we have $B \simeq \mathbb{Z}^n$. Be aware that there is a considerable distinction between a $\mathbb{Z}$-basis like we just described, and an *integral basis*, which is just a basis for K over $\mathbb{Q}$ contained in A.

☐ Let $b_1, \ldots, b_b$ be a $\mathbb{Z}$-basis for B, and assume that $b_1', \ldots, b_n'$ is an integral basis. Then for some matrix V with integral coefficients and non-zero determinant, $b_\bullet' = V b_\bullet$. The basis $b_\bullet'$ is a $\mathbb{Z}$-basis if and only if the determinant of V satisfies $\det V = \pm 1$.

PROBLEM 2. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square free integer satisfying $d \equiv 1 \mod 4$. Let A be the ring of algebraic integers in K. Show that the basis $1, \sqrt{d}$ is an integral basis for A, but not a $\mathbb{Z}$-basis. What is the determinant? ✸

BACK TO THE GENERAL CASE In the general case, when A is any Dedekind ring, it is no more true that finitely generated and torsion free modules necessarily free. For example, ideals in a Dedekind ring are of course torsion free, and they are free if and only if they are principle. and if the ring is not a UFD , there are ideals that are not free. However if A is a PID , every finitely generated and torsion free module is free. We shall not prove that. Since our ring B is contained in a free A-module, we get away with the weaker:

Proposition 1 *Assume that A is a* PID *and that M is a submodule of a free module. Then M is free.*

PROOF: The proof goes by induction on the rank of the containing free module, the rank one case being the hypothesis that A is a PID . Indeed, an ideal is free (of rank one) if and only if it generated by one element.

So assume $r > 1$, and suppose that $M \subseteq A^r$. At least one of the projection of A^r onto the factors, does not vanish on M, call it ϕ. The image $\phi(M)$ is a non-trivial ideal, which is a free module of rank one since A is PID . Therefore there is an exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow A \longrightarrow 0.$$

This sequence splits and $M = A \oplus N$. But $N \subseteq \operatorname{Ker}\phi$ and $\operatorname{Ker}\phi$ is isomorphic to A^{r-1}. Hence N is free by induction. ❑

In particular, this result applies to DVR 's, so every module M over the Dedekind ring A contained in a free A-module, is *locally free*, *i.e.,* the localized module $M_{\mathfrak{p}}$ is free over $A_{\mathfrak{p}}$ for all non-zero prime ideals $\mathfrak{p}$ in A.

Proposition 2 *In standard setup, B is a locally free A-module of rank $n = [L : K]$.*

PROOF: By the dual-basis-trick, B is contained in a free A-module, and hence is locally free by the above considerations. The statement about the rank follows since $L = B \otimes_A K$ implies that $L = B_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} K$. ❑

The fibre over a prime ideal

Now, fix a non-zero prime ideal $\mathfrak{p}$ in A. We are seriously interested in the set of primes in $\mathfrak{q}$ in B with $\mathfrak{p} \subseteq \mathfrak{q}$—or equivalently $\mathfrak{p} = \mathfrak{q} \cap A$— and we call that set for *the fibre over* $\mathfrak{p}$. The origin of this terminology comes from the map $\operatorname{Spec}B \to \operatorname{Spec}A$ whose fibre over $\mathfrak{p}$ is the set just described. As well, one says that $\mathfrak{q}$ *lies over* $\mathfrak{p}$. The map $\operatorname{Spec}A \to \operatorname{Spec}B$ is surjective. This is is true for any finite extension of rings, and goes under the name "The going up theorem".

THE RESIDUE FIELDS If $\mathfrak{q} \in \operatorname{Spec}B$ lies over $\mathfrak{p} \in \operatorname{Spec}A$, that is $\mathfrak{q} \cap A = \mathfrak{p}$, then the inclusion $A \subseteq B$ induces an extension $k(\mathfrak{p}) = A/\mathfrak{p} \subseteq B/\mathfrak{q} = K(\mathfrak{q})$ of the two residue fields. Since B is a finitely generated module over A, this extension is finite, and the degree $[k(\mathfrak{q}) : k(\mathfrak{p})]$ is a well defined integer. We denote it by $f_{\mathfrak{q}/\mathfrak{p}}$ or simply by $f_{\mathfrak{q}}$ or even f if there is no danger of confusion.

THE MULTIPLICITIES IN THE FIBRE Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ be the different prime ideals in the fibre over $\mathfrak{p}$. By the main theorem for Dedekind rings, the ideal $\mathfrak{p}B$ can be decomposed

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\ldots\mathfrak{q}_s^{e_s} \qquad (\spadesuit)$$

with the multiplicities e_i being natural numbers. They are called the *ramification indices of* $\mathfrak{p}$. If $\mathfrak{q}$ lies over $\mathfrak{p}$, one often writes $e_{\mathfrak{q}/\mathfrak{p}}$ for the corresponding ramification index. If $e_{\mathfrak{q}/\mathfrak{p}} = 1$, one says that $\mathfrak{q}$ is *unramified*, and if all the prime ideals $\mathfrak{q}$ in the fibre over $\mathfrak{p}$ are unramified, one says that $\mathfrak{p}$ itself is *unramified*. It might happen that $s = 1$, that is $\mathfrak{p}$ is the power of a prime ideal, then $\mathfrak{p}$ is *totally ramified*.

For each of the primes $\mathfrak{q}_i$ in the fibre the degree $[k(\mathfrak{q}_i), k(\mathfrak{p})]$ of the field extension $k(\mathfrak{p}) \subseteq k(\mathfrak{q}_i)$ is called the *relative degree* or the *local degree* of $\mathfrak{q}$ over $\mathfrak{p}$. We denote it by $f_{\mathfrak{q}/\mathfrak{p}}$ or simply by f or f_i.

There is a fundamental relation between the degree $[L : K]$, the local degrees f_i and the ramification indices e_i:

Theorem 1 *In standard set up, we have*

$$n = \sum_{i=1}^{s} e_i f_i.$$

To establish this formula, there are three points to make. The first one is that in combination with equation ✦ above the chinese residue theorem gives the following decomposition of the algebra $B/\mathfrak{p}B$ in a product of local algebras:

$$B/\mathfrak{p}B = B/\mathfrak{q}_1^{e_1} \oplus B/\mathfrak{q}_2^{e_2} \oplus \cdots \oplus B/\mathfrak{q}_s^{e_s}$$

The next one is that $B/\mathfrak{p}B$ is a module over $A/\mathfrak{p}$; that is, it is a vector space over the residue field $k(\mathfrak{p})$. The vector space is of finite dimension since B is finitely generated over A (the residue classes of a set of generators for B over A generates $B/\mathfrak{p}B$ over $A/\mathfrak{p}$), and in fact we have

Lemma 1 $\dim_{k(\mathfrak{p})} B/\mathfrak{p}B = [L : K] = n$.

PROOF: This follows since by proposition 2 above B is a locally free of rank $[L : K]$ as an A-module, and $B/\mathfrak{p}B = B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ (Take $M = B$ in prop xxx). ❑

EXAMPLE 1. The case $A = \mathbb{Z}$ is again illustrative. Assume $\mathfrak{p} = (p)$ so that $A/(p) = \mathbb{F}_p$. Then $B \simeq \mathbb{Z}^n$ and $\mathfrak{p} = (p)$, then $B/pB \simeq \mathbb{Z}^n/p\mathbb{Z}^n = \mathbb{F}_p^n$. ❄

The third point concerns the different factors in the decomposition of $B/\mathfrak{p}B$ above. So let $\mathfrak{q}$ be one of the primes in the fibre, and let $f = [k(\mathfrak{q}) : k(\mathfrak{p})]$ be the degree of the residue field extension. Then we have the nice formula:

Lemma 2 $\dim_{k(\mathfrak{p})} B/\mathfrak{q}^e = ef$.

PROOF: Indeed, there is a canonical isomorphism $B/\mathfrak{q}^e = B_{\mathfrak{q}}/\mathfrak{q}^e B_{\mathfrak{q}}$. To understand such a ring, we observe that $R = B_{\mathfrak{q}}$ is a DVR with maximal ideal $\mathfrak{m} = \mathfrak{q}B_{\mathfrak{q}}$. We use induction on e, the case $e = 1$ being clear. There is an exact sequence

$$0 \longrightarrow \mathfrak{m}^{e-1}/\mathfrak{m}^e \longrightarrow R/\mathfrak{m}^e \longrightarrow R/\mathfrak{m}^{e-1} \longrightarrow 0$$

and $\mathfrak{m}^{e-1}/\mathfrak{m}^e \simeq k(\mathfrak{m})$ since it is non-zero (*e.g.,* Nakayama's lemma), generated by one element (namely the residue class of a uniformizing paramter to the $(e-1)$-th power) and killed by $\mathfrak{m}$. Hence by induction using that $f = \dim_{k(\mathfrak{p})} k(\mathfrak{q})$ we get:

$$\dim_{k(\mathfrak{p})} B/\mathfrak{q}^e = \dim_{k(\mathfrak{p})} B/\mathfrak{q}^{e-1} + \dim_{k(\mathfrak{p})} k(\mathfrak{q}) = (e-1)f + f = ef.$$

❑

Combining all this, we have eatblished the theorem.

PROBLEM 3. Assume that $K \subseteq E \subseteq L$ is a tower of finite, separable extensions. Let $A \subseteq B \subseteq C$ be the corresponding tower of integal closures. Assume that $\mathfrak{p}$ is a non-zero prime in Spec$A$, that $\mathfrak{q}$ is a non-zero prime in B lying over $\mathfrak{p}$ and that $\mathfrak{r}$ is one in C lying over $\mathfrak{q}$.

a) Show that the local degrees behave in a multiplicative way. That is

$$f_{\mathfrak{r}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}}$$

b) Show that the ramfication indices are multiplicative as well. That is

$$e_{\mathfrak{r}/\mathfrak{p}} = e_{\mathfrak{r}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}}$$

✸

The Galois case

If the field L is Galois over K, the situation simplifies considerably. Let $G = \mathrm{Gal}(L/K)$.

First of all, if β is integral over A, then $\sigma(\beta)$ is integral over A as well. In fact, the coefficients of any relation of integral dependence of β are invariant under G, hence $\sigma(\beta)$ satisfies the same relation as β does. This shows that the integral closure B of A is invariant under the Galois group.

Secondly, if $\mathfrak{q}$ is a prime ideal in B, then $\sigma(\mathfrak{p})$ is a årime ideal as well, indeed σ is a ring isomorphism. This shows that the Galois grou $\mathrm{Gal}(L/K)$ acts on Spec$B$. Since G acts trivially on A, one has $\mathfrak{q} \cap A = \sigma(\mathfrak{q}) \cap A$, and the fibres of Spec$B \to$ Spec$A$ are invariant under this action.

Thirdly, we have the imporant:

Lemma 3 *The action of* $\mathrm{Gal}(L/K)$ *is transitive on the fibres. That is, if* $\mathfrak{q}$ *and* $\mathfrak{q}'$ *are two prime ideals such that* $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$*, then for at least one* $\sigma \in \mathrm{Gal}(L/K)$*, we have* $\sigma(\mathfrak{q}) = \mathfrak{q}'$.

PROOF: Assume not. Then $\mathfrak{q}'$ is not among the prime ideals $\sigma(\mathfrak{q})$ as σ runs through $\mathrm{Gal}(L/K)$. By prime avoidance, $\mathfrak{q}'$ is not contained in the union $\bigcup_{\sigma \in \mathrm{Gal}(l/K)} \sigma(\mathfrak{q})$. There is therefore an element $x \in \mathfrak{q}'$, but $x \notin \sigma(\mathfrak{q})$ for any σ.

We let $y = \prod \sigma(x)$. Then y is invariant under $\mathrm{Gal}(L/K)$ and therefore lies in A. It lies in $\mathfrak{q}'$, and hence in $\mathfrak{q}' \cap A$. On the other hand, y can not lie in $\mathfrak{q}$. Indeed, if it did, $\mathfrak{q}$ being a prime ideal, one of the $\sigma(x)$'s would lie in $\mathfrak{q}$, and therefore $x \in \sigma^{-1}(qfr)$ which is not the case. Hence $y \notin \mathfrak{q} \cap A$. But $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$, contradiction. ❑

This has the nice implication that all the ramification indices and all the residue degrees in a fibre must be equal! Indeed:

Theorem 2 *Assume that L is Galois over K and that $\mathfrak{p} \in \mathrm{Spec}A$. Let $\mathfrak{q}$ be in the fibre over $\mathfrak{p}$. Then $\mathfrak{p}B$ decomposes as*

$$\mathfrak{p}B = \bigcap_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{q})^e$$

Furthermore, if $f = [k(\mathfrak{q}) : k(\mathfrak{p})]$, then

$$n = sef.$$

where s denoted the number of prime ideals lying over $\mathfrak{p}$.

To get a simple formulation as possible, we used the intersection in this theorem. The reason being that there might be non-trivial elements in G with $\sigma(\mathfrak{q}) = \mathfrak{q}$. To avoid unwanted repetitions in the product (in the intersection they do no harm) one must write

$$\mathfrak{p}B = \prod_{\sigma \in S} \sigma(\mathfrak{q})^e$$

where S is a full set of representatives of the cosets of the so called isotropy group $G_{\mathfrak{q}} = \{\, \sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q} \,\}$.

PROOF: The ideal $\mathfrak{p}B$ is invariant under the Galois group so for any $\sigma \in \mathrm{Gal}(L/K)$, we have

$$\mathfrak{p}B = \sigma(\mathfrak{q}_1)^{e_1} \cdot \cdots \cdot \sigma(\mathfrak{q}_s)^{e_s} = \mathfrak{q}_1^{e_1} \cdot \cdots \cdot \mathfrak{q}_s^{e_s}$$

If i and j are two of the indices, there is by lemma 3 a σ with $\mathfrak{q}_i = \sigma(\mathfrak{q}_j)$. By uniqueness of the decomposition $e_i = e_j$, and all the ramification indices are equal. The automorphism $\sigma\colon B \to B$ induces an isomorphism between $k(\mathfrak{q}_i) = B/\mathfrak{q}_i$ and $k(\mathfrak{q}_j) = B/\mathfrak{q}_j$ as algebras over $A/\mathfrak{p}$. Hence $f_i = f_j$. ❑

PROBLEM 4. Let L be a cubic extension of the field K, *i.e.,* an extension with $[L : K] = 3$ and let $\alpha \in L$ be an element. Then the characteristic polynomial of α is

$$x^3 - \mathrm{tr}_{L/K}(\alpha)x^2 + N_{L/K}(\alpha)\,\mathrm{tr}_{L/K}(\alpha^{-1})x - N_{L/K}(\alpha)$$

✸

PROBLEM 5. Let $K = \mathbb{Q}(\sqrt{5})$ and let $\rho = (\sqrt{5}+1)/2$ be the "golden number".

a) Show that $A = \mathbb{Z}[\rho]$ is the ring of algebraic integers in K.

b) Show that 5 ramifies in A and find the ideal $\mathfrak{q}$ such that $(5)A = \mathfrak{q}^2$. Show that no other prime ramifies in A.

c) Show that if $p < 11$ and $p \neq 5$, then pA is a prime ideal.

d) Show that $(11)A = \mathfrak{p}_1\mathfrak{p}_2$ where the $\mathfrak{p}_i$'s are different prime ideal, and both are principal ideals.

✸

PROBLEM 6. Let $f(x) = x^2 - x - 5$ and let ξ be a root of $f(x)$. Let $K = \mathbb{Q}(\xi)$.

a) Show that $A = \mathbb{Z}[\xi]$ is the ring of algebraic integers in K.

b) Show that $\xi + 2$ is invertibel in A.

c) Show that 3 and 7 are the only primes that ramify in A.

d) Show that $3A = (\rho + 1)^2$ and $7A = (\rho + 3)^2$.

e) Decompose $2A$ and $5A$ as products of prime ideals in A.

✸

PROBLEM 7. Let $\eta = \sqrt[3]{2}$ and let $K = \mathbb{Q}(\eta)$ and let A be the ring of integers in K.

a) Show that 2 is totally ramified in A.

b) Let $\alpha = 1 + \xi$. Show that α satisfies the equation

$$x^3 - 3x^2 - 3x - 3 = 0$$

Conclude that $N_{K/\mathbb{Q}}(\alpha) = 3$ and that $\alpha^2 - \alpha + 1$ is a unit in A.

c) Show that 3 is totally ramified in A.

✸

PROBLEM 8. Let p be a prime and let $f(x) \in \mathbb{F}_p[x]$ be a polynomial. Show that the number of different homomorphisms from $\mathbb{F}_p[x]/(f(x))$ is bounded above by p. ✸

PROBLEM 9. Assume that K is a number field of degree n with ring of integers A. Assume that there is a prime p less than n such that p splits completely in A. Show that A has no primitive element, *i.e.,* no element $t \in A$ is such that $A = \mathbb{Z}[t]$. ✸

PROBLEM 10. In this example we exhibit a cubic extension K of in which the ring of integers is not generated by one element. Let $f(x) = x^3 - 3X + 9$, and let t be one of its roots. Further let $K = \mathbb{Q}(t)$.

a) If $u = 3/t$. Use the equation $t^3 - 3t + 9 = 0$ to show that $u^3 - u^2 + 3 = 0$. Hence u is integral over $\mathbb{Z}$. Show that $u \notin \mathbb{Z}[t]$.

b) Show that the subgroup B spanned by 1, u and t actually is a subring, that is $B = \{\, a + bu + ct \mid a, b, c \in \mathbb{Z} \,\}$ is a subring. HINT: Prove that $t^2 = 3 - 3u$, that $u^2 = u - t$ and that $ut = 3$.

c) Show that $\mathrm{tr}_{K/\mathbb{Q}}(t) = -3$ and that $\mathrm{tr}_{K/\mathbb{Q}}(u) = 0$. HINT: Use minimal polynomials.

d) Show that $1, u, t$ is a basis for $\mathbb{Q}(t)$ over $\mathbb{Q}$ and show that the discriminant of this basis equals $-3 \cdot 7 \cdot 11$.

e) Conclude that B is the ring of integers.

f) Show that $B/3B \simeq \mathbb{F}_3[u,t]/(t^2, ut, u^2 - u - t) \simeq \mathbb{F}_3[u]/(u^2(u-1))$ and use this to decompose 3 in B.

✸

PROBLEM 11. This example is due to Dedekind. It exhibit a cubic number field whose ring of integers does not have a primitive element; *i.e.,* is not of the form $\mathbb{Z}[\xi]$. Let $f(x) = x^3 + x^2 - 2x + 8$, and let t be a root of f. Put $K = \mathbb{Q}(t)$, and denote by A the ring of algebraic integers A in K.

a) Put $u = 4/t$. Show that u satisfies the equation $u^3 - u^2 + 2u + 8 = 0$ and hence belongs to A.

b) Show that the subgroup of K generated by 1, u and t, that is $B = 1\cdot\mathbb{Z} + u\cdot\mathbb{Z} + t\cdot\mathbb{Z}$, is a subring by showing that $t^2 = 2 - t - 2u$, $u^2 = -2 - 2t + u$ and $tu = 4$.

c) Compute the discriminant of the basis $1, u, t$ and conclude that $A = B$.

d) Show that $A/2A = \mathbb{F}_2[U,T]/(UT, U(U-1), T(T-1)$ and conclude that 2 splits completely in A, that is $(2)A$ is the product of three different prime ideals.

e) Show that A does not have a primitive element.

✸