Notes: Algebraic Number Theory - Neukirch

Henry Twiss
University of Minnesota

May 2020

1 Integrality

Page 7

- ... we see that $\det(bE - (a_{ij})) - \omega_i = 0$, $i = 1, \ldots, r$ ...

  To see this, note that by (2.3) we have $\det(bE - (a_{ij})) - \omega = 0$. Now take components.

- ... the integral closure $\overline{A}$ is itself integrally closed in B ...

  Notice that we have the tower $A \subseteq \overline{A} \subseteq \overline{\overline{A}}$. Now use Proposition (2.4).

- ... If A is an integral domain with field of fractions K ...

  At this point, identify A with its isomorphic copy in K and assume this for the remainder of the chapter.

Page 8

- ... Each element $\beta \in L$ is of the form

$$\beta = \frac{b}{a}, \quad b \in B,\ a \in A$$

  This implies L is the field of fractions of B because $A \subseteq B$. Indeed, let F be the field of fractions of B. Then $F = L$ or $F \subsetneq L$. We show $L \subseteq F$. F consists of elements of the form b/b' with $b, b' \in B$. But $A \subseteq B$ so F contains elements of the form b/a and so $L \subseteq F$. Hence $F = L$.

- ... hence the same holds for all the coefficients ...

  This is because these coefficients are just sums and products of the roots by Vieta's formulas. Notice here that this would not follow if $p(x)$ was not monic (see Vieta's formulas).

- $$Tr_{L|K}(x) = Tr(T_x), \quad N_{L|K}(x) = \det(T_x)$$

  Notice that the trace and norm are well-defined because the trace and norm of a matrix are basis independent.

Page 9

- $$f_x(t) = \det(t, \mathrm{id} - T_x) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in K[t]$$

  Indeed, this polynomial lies in $K[t]$ because the matrix corresponding to the endomorphism T_x (and id) has its entries in K.

- $$f_x(t) = p_x(t)^d, \quad f = [L : K(x)]$$

  This will be a commonly used fact later on, so we note it now for convenience. The equation above implies that $N_{L|K}(x) \in \mathbb{Z}$ if $x \in \mathcal{o}$ (this notation will be seen on page 14) because $x \in \mathcal{o}$ means x satisfies a polynomial over $\mathbb{Z}$, so $p_x(t) \in \mathbb{Z}[t]$. This fact generalizes to arbitrary separable extensions $L|K$ with rings of integers $\mathcal{O}$ and $\mathcal{o}$ respectively (see §8).

- $$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \cdots & -c_1 \end{pmatrix}$$

  This matrix is actually the transpose of the block matrices on the diagonal of the matrix for $T_x : y \mapsto xy$ if the columns and rows of the matrix are indexed by $\alpha_1, \alpha_1 x, \ldots, \alpha_1 x^{m-1}; \ldots; \alpha_d, \alpha_d, \ldots, \alpha_d x^{m-1}$ (which the text seems to suggest) in this order from left to right and up to down respectively. So we should be looking at the blocks

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -c_m \\ 1 & 0 & \cdots & 0 & -c_{m-1} \\ 0 & 1 & \cdots & 0 & -c_{m-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_1 \end{pmatrix}$$

Indeed, the first column then shows α_1 is sent to $\alpha_1 x$ which is how T_x acts on α_1. The reason why we are considering the first matrix is because it's easy to find the characteristic polynomial and the characteristic polynomial of a matrix and its transpose are the same. Also, look at $p_x(x)$ and notice what T_x does to $\alpha_i x^{m-1}$ to see why we need the $-c_i$'s in the matrix if this was not already clear.

Page 10

- > ... into m equivalence classes of d elements each ...

  If you don't see why this is immediately true, notice that there are m roots of the minimal polynomial $p_x(t)$ of x and each embedding permutes the roots of irreducible polynomials. Then recall that $d = [L : K(x)]$, so there are d ways to extend this embedding.

- > ... assume that $M|K$ is separable ...

  This implies $M|L$ and $L|K$ are separable extensions as well, so we are in the separable situation as before.

- > $$\cdots = \sum_{i=1}^{m} \sum_{\sigma \sim \sigma_i} \sigma x = \sum_{i=1}^{m} Tr_{\sigma_i M|\sigma_i L}(\sigma_i x) = \sum_{i=1}^{M} \sigma_i Tr_{M|L}(x) \cdots$$

  If these equalities are not obvious, see the Mathematics Stack Exchange post 2931966 for a more detailed explanation.

Page 11

- $$d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i \alpha_j))^2$$

  Note that the discriminant d is well-defined because the determinant is basis invariant and interchanging rows only changes the sign of the determinant (but we square on the right-hand side).

Page 12

- ... they [the a_j's] are given as the quotient of an element of A by the determinant $\det(Tr_{L|K}(\alpha_i \alpha_j)) = d^2$ ...

  To see this more concretely, set $\underline{a} = (a_1, \ldots, a_n)$, $x = (Tr_{L|K})(\alpha_i \alpha)$, and $D = (Tr_{L|K}(\alpha_i \alpha_j))$. Then $x = D\underline{a}^t$ which implies $D^* x = \det(D)\underline{a}^t = d\underline{a}^t$, and the left-hand side is a matrix with values in A.

- ... Since such an integral basis is automatically a basis of $L|K$ ...

  To see this, notice that a linearly independent set stays linearly independent over the field of fractions (use contradiction and clear denominators to see this). Spanning can be easily proved again using a contradiction argument.

Page 13

- ... Multiplying by an element of A, we may arrange for the α_i to lie in B ...

  More precisely, use the fact that the α_i are algebraic, clear denominators, and then multiply by the power of an element of A to get elements which form a new basis and lie in B.

- ... in particular, $\text{rank}(B) \leq [L : K]$, and since a system of generators of the A-module B is also a system of generators for the K-module L, we have $\text{rank}(B) = [L : K]$ ...

We first use the fact that since A is a PID, any submodule of a free module over A is also free. To see that a system of generators for B is also a system of generators for L, notice that a linearly independent set stays linearly independent over the field of fractions, and spanning can be proved easily. See the notes for page 12 for more information.

- > ... There exists an $a \in A$, $a \neq 0$, such that $a\mu_i \in B$ ...

  Recall $M \subseteq L$ so $\mu_i = \frac{b}{a}$ for some $b \in B$ and $a \in A$.

- > $$[L : K] = \text{rank}(B) \leq \text{rank}(M) \cdots$$

  The rank inequality follows because B can be embedded into M under the map $b \mapsto bm$ for any $m \neq 0$.

Page 14

- > ... namely $d'\beta_j = \sum_i d'a_{ij}\omega_i$. Thus $d'a_{i,j} \in A$ ...

  More generally, use induction to prove the b_i's are integral in $a = \sum_i b_i c_i$ if a and the c_i's are.

- > ... By changing indices the second matrix may be transformed to look like the first ...

  We mean that we can get the first matrix to look like the second just by using elementary row operations. It may be useful to take a moment and try this with a 3×3 matrix if the transformation process isn't immediately clear.

Page 15

- > ... then the base change matrix $T = (a_{ij})$, $\alpha'_i = \sum_j a_{ij}\alpha_j$, as well as its inverse, has integral entries

  This is a typo. It should read integer entries as the a_{ij} are integers.

2 Ideals

Page 16

- > ... every non-unit $\alpha \neq 0$ can be factored in $\mathcal{O}_K$ into a product of irreducible elements. For if α is not itself irreducible, then it can be written as a product of two non-units $\alpha = \beta\gamma$. Then by §2, one has
>
> $$1 \leq |N_{K|\mathbb{Q}}(\beta)| < |N_{K|\mathbb{Q}}(\alpha)|, \quad 1 < |N_{K|\mathbb{Q}}(\gamma)| < |N_{K|\mathbb{Q}}(\alpha)|$$

  This process terminates because the norm of an integral element in K is an integral element in K, that is an integer.

Page 17

- > ... every ideal $\mathfrak{a}$ is a finitely generated $\mathbb{Z}$-module by (2.10) and therefore *a fortiori* a finitely generated $\mathcal{O}_K$ module ...

  What we mean here is the following. Let $B = \mathcal{O}_K$ and $A = \mathbb{Z}$, and note that the $\mathcal{O}_K$-submodule of L generated by $1 \in L$, namely $\mathcal{O}_K$, is a finitely generated $\mathcal{O}_K$-submodule of L. So by proposition 2.10 it's a free $\mathbb{Z}$-module of rank $[L : K]$, and in particular a finitely generated $\mathbb{Z}$-module. Since $\mathbb{Z}$ is noetherian and $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, any $\mathbb{Z}$-submodule of $\mathcal{O}_K$ so in particular any ideal $\mathfrak{a}$ of $\mathcal{O}_K$ will also be a finitely generated $\mathbb{Z}$-module. Since $\mathbb{Z} \subseteq \mathcal{O}_K$, $\mathfrak{a}$ is therefore a finitely generated $\mathcal{O}_K$-module.

- > ... $\mathfrak{p} \cap \mathbb{Z}$ is a nonzero prime ideal (p) in $\mathbb{Z}$: the primality is clear ...

  If the primality is not clear, consider the natural homomorphism $\varphi : \mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$. Then $\ker \varphi = \mathfrak{p} \cap \mathbb{Z}$ and so $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z})$ is an subring of an integral domain hence itself an integral domain. This happens if and only if $\mathfrak{p} \cap \mathbb{Z}$ is prime.

- > ... if $y \in \mathfrak{p}$, $y \neq 0$, and
  >
  > $$y^n + a_1 y^{n-1} + \cdots + a_n = 0$$
  >
  > is an equation for y with $a_i \in \mathbb{Z}$, $a_n \neq 0$, then $a_n \in \mathfrak{p} \cap \mathbb{Z}$ ...

  There are a few things to note here. Firstly, the condition $a_n \neq 0$ really just means that the polynomial $y^n + a_1 y^{n-1} + \cdots + a_n = 0$ is either the minimal polynomial for y or a multiple of it by another polynomial which is not a multiple of y. For if $a_n = 0$ we could factor out a y from $y^n + a_1 y^{n-1} + \cdots + a_n = 0$. Secondly, $a_n = -y^n - a_1 y^{n-1} - \cdots - a_{n-1} y$ which means a_n is a linear combination of elements in $\mathfrak{p}$ and hence an element of $\mathfrak{p}$.

- > ... The integral domain $\bar{o} = o_K/\mathfrak{p}$ arises from $\kappa = \mathbb{Z}/p\mathbb{Z}$ by adjoining algebraic elements and is therefore again a field ...

  Another way to see this is as follows. Taking $\mathfrak{a} = o_K$ in the first line of the proof, we see that o_K is a finitely generated $\mathbb{Z}$-module. Let the basis be $\alpha_1, \ldots, \alpha_n$. Then $o_K/\mathfrak{p} \cong \bigoplus_{i=1}^{n} \alpha_i(\mathbb{Z}/p\mathbb{Z})$ which implies $|o_K/\mathfrak{p}| \leq p^n$. This means $o_K/\mathfrak{p}$ is a finite integral domain, hence a field, which happens if and only if $\mathfrak{p}$ is a maximal ideal.

Page 19

- > **(3.5) Lemma.** Let $\mathfrak{p}$ be a prime ideal of o and define
  >
  > $$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq o\}.$$
  >
  > Then one has $\mathfrak{a}\mathfrak{p}^{-1} := \{\sum_i a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1}\} \neq \mathfrak{a}$, for every ideal $\mathfrak{a} \neq 0$.

  There are a few things to note about Lemma 3.5 and its proof. Firstly, $\mathfrak{p}^{-1}$ is not an ideal of o_K. Also, $1 \in \mathfrak{p}^{-1}$. Secondly, the first paragraph of the proof proves the lemma for the case $\mathfrak{a} = o$ and shows that $\mathfrak{p}^{-1} \subsetneq o$. On the other hand, notice $o \subseteq \mathfrak{p}^{-1}$.

- > ... Writing A for the matrix $(x\delta_{ij} - a_{ij})$ ...

  δ_{ij} is the Kronecker delta. That is

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

Page 20

- > $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$

  To get the first equality use the fact that $\mathfrak{a} = \mathfrak{a}\mathcal{O}$. Also, notice that $\mathfrak{p}\mathfrak{p}^{-1}$ is an ideal of $\mathcal{O}$. This can be checked directly by the definition.

- > ... we find that $\mathfrak{a}_i \mid a$, and therefore, the factors being relatively prime, we get $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n \mid a$, i.e., $a \operatorname{im} \mathfrak{a}$ ...

  Recall that the product of relatively prime ideals is equal to their intersection.

Page 21

- > ... If $n > 2m$ we may find as before an element $y_1 \in \mathcal{O}$ such that
>
> $$y_1 \equiv 1 \bmod \mathfrak{a}_1, \quad y_1 \equiv 0 \bmod \bigcap_{i=2}^{n} \mathfrak{a}_i,$$
>
> and, by the same token, elements $y_2, \ldots, y_n$ such that
>
> $$y_1 \equiv 1 \bmod \mathfrak{a}_i, \quad y_1 \equiv 0 \bmod \mathfrak{a}_j \quad \text{for } i \neq j.$$

  The proof of surjectivity in the Chinese Remainder Theorem is just an induction argument and this entire part of the proof is the induction hypothesis.

- > ... an $\mathcal{O}$-submodule $\mathfrak{a} \neq 0$ of K is a fractional ideal if and only if there exists a $c \in \mathcal{O}$, $c \neq 0$, such that $c\mathfrak{a} \subseteq \mathcal{O}$ is an ideal of the ring $\mathcal{O}$ ...

We really mean $(c)\mathfrak{a}$ instead of $c\mathfrak{a}$, but we can write the latter way because a quick check shows $(c)\mathfrak{a} = c\mathfrak{a}$. To see why the forward implication is true, notice that every generator for $\mathfrak{a}$ is of the form $\frac{y_i}{c}$ for some $y_i \in \mathcal{O}$ and some $c \in \mathbb{Z}$ by finding a common denominator. For the reverse implication, $c\mathfrak{a}$ is finitely generated, since $\mathcal{O}$ is noetherian, so $c^{-1}c\mathfrak{a} = \mathfrak{a}$ is as well.

- $$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}.$$

  Notice that $\mathfrak{a}^{-1}$ is a fractional ideal. In particular, it is nonempty because the common denominator for the generators of $\mathfrak{a}$ lie in it.

Page 22

- > ... then $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ is the inverse of $c\mathfrak{a}$ ...

  The equality $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$ is as expected, but requires a quick verification using containment and the definition of $\mathfrak{a}^{-1}$.

- > ... So the class group Cl_K measures the expansion that takes place when we pass from numbers to ideals, whereas the unit group $\mathcal{O}^*$ measures the contraction in the same process ...

  Indeed, if $h_K = |Cl_K|$ (h_K is called the class number, defined on page 36, and the fact it is finite is proved on the same page), then as number of fractional principle ideals in $\mathcal{O}$ increases h_K decreases. $h_K = 1$ exactly when $\mathcal{O}$ is a PID. So we can really think of Cl_K as measuring expansion by looking at h_K.

3 Lattices

Page 23

- In this chapter some familiarity with topological groups and Haar measures on locally compact topological groups is assumed. In particular, lattices are assumed to be topological spaces with the subspace topology induced from the standard Euclidean topology. A good reference for this material is Ramakrishnan and Valenza's *Fourier Analysis on Number Fields* sections 1.1 and 1.2.

Page 25

- > ... For let U be an arbitrary neighbourhood of 0. Then there exists a neighbourhood $U' \subseteq U$ of 0 such that every difference of elements of U' lies in U ...

  This is a reformulation of a basic property of topological groups which is that any neighbourhood U of the identity contains a symmetric neighbourhood V of the identity such that $VV \subseteq U$.

- > ... Putting now $q = (\Gamma : \Gamma_0)$, we have $q\Gamma \subseteq \Gamma_0$ ...

  We give a short proof of this fact, if it is not already clear. Since Γ/Γ_0 has order q, for every $\gamma + \Gamma_0 \in \Gamma/\Gamma_0$ we have $q(\gamma + \Gamma_0) = \Gamma_0$ and $q(\gamma + \Gamma_0) = q\gamma + \Gamma_0$. Hence $q\gamma \in \Gamma_0$. Therefore $q\Gamma \subseteq \Gamma_0$.

Page 26

- > ... since V_0 is closed ...

  V_0 is closed by the general fact that every finite dimensional subspace of a normed vector space over $\mathbb{R}$ (or $\mathbb{C}$) is closed.

4 Minkowski Theory

Page 28

- $$j : K \to K_{\mathbb{C}} := \prod_{\tau} \mathbb{C}, \quad a \mapsto ja = (\tau a)$$

  What may be confusing here is why we use $K_{\mathbb{C}}$ instead of $\mathbb{C}^n$. The reason we do this is to emphasis that the setup of the theory involves a field K and the mapping $j : K \to K_{\mathbb{C}}$. Also, notice that in defining j we assume an implicit ordering of the complex embeddings $\tau : K \to \mathbb{C}$. This of course doesn't cause any issues because $\prod_{\tau} \mathbb{C}$ is independent of the ordering.

- ... Altogether, this defines an involution

  $$F : K_{\mathbb{C}} \to K_{\mathbb{C}}$$

  which, on the points $z = (z_\tau) \in K_{\mathbb{C}}$, given by

  $$F(z)_\tau = \bar{z}_{\bar{\tau}}$$

  There is a bit to unpack in this definition. F is defined on components, and acts by permuting and then conjugating them, so it maps $z_\tau \mapsto z_{\bar{\tau}} \mapsto \bar{z}_{\bar{\tau}}$. We verify F is an involution below:

  $$(FFz)_\tau = (F(Fz))_\tau = (F\bar{z})_{\bar{\tau}} = z_\tau$$

  An interesting thing to notice is that $F(ja) = ja$. Indeed, if $ja = (\tau a)$ then F acts on ja component-wise by $\tau a \mapsto \bar{\tau} a \mapsto \overline{\bar{\tau} a} = \tau a$.

Page 29

- ... It is also F-invariant ...

  By this we mean $Tr \circ F = F \circ Tr$.

- 1. This yields a mapping

  $$j : K \to K_{\mathbb{R}}$$

The mapping $j : K \to K_{\mathbb{R}}$ is literally the same map as $j : K \to K_{\mathbb{C}}$. The reason why we define $j : K \to K_{\mathbb{R}}$ is because we can view $j(K)$ as living in $K_{\mathbb{R}}$ instead of $K_{\mathbb{C}}$ because $F(ja) = ja$ for all $a \in K$ (that is, ja is F-invariant).

- > ... Since $Tr \circ F = F \circ Tr$ we have on $K_{\mathbb{R}}$ the $\mathbb{R}$-linear map
  >
  > $$Tr : K_{\mathbb{R}} \to \mathbb{R}$$

  The fact $Tr \circ F = F \circ Tr$ is telling us the following. Every point in $K_{\mathbb{R}}$ is by definition $\mathbb{R}$ invariant. In other words, if $z \in K_{\mathbb{R}}$ and we look at the component $z_{\bar{\tau}}$, then its conjugate is the component z_{τ}. This is just a superfluous way of saying $z_{\bar{\tau}} = \bar{z}_{\tau}$. Hence when we take the trace of z we are summing over pairs of conjugates which implies the trace is a real valued.

Page 31

- In the proof of Proposition 5.1 keep in mind that $\rho : K \to \mathbb{R}$ is a real embedding while $\sigma : K \to \mathbb{C}$ is a complex embedding, and instead of using function notation we identify components of images (that is x_{τ} for a fixed embedding τ real or complex) with the real or complex part of the domain component (this is how f is defined). Also, the part of the claim concerning scalar products is proved on components.

- > ... then $\Gamma = j\mathfrak{a}$ is a complete lattice in $K_{\mathbb{R}}$ ...

  The proof of Proposition 5.2 does not directly prove this statement because they assume it's immediate to the reader. Just notice that any integral basis for $\mathfrak{a}$ contains exactly n elements, and $n = r + 2s$.

Page 33

- > $$\ell : \mathbb{C}^* \to \mathbb{R}, \quad z \mapsto \log |z|$$

  Notice that this map is surjective since $(0, \infty) \subset \mathbb{C}^*$.

- > ... $F \in G(\mathbb{C}|\mathbb{R})$ acts on all groups in this diagram, trivially on K^* ...

By trivially we mean by conjugation.

5 The Class Number

Page 34

- $$\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$$

  This is finite. To see this first notice $\mathcal{O}_K \cong \mathbb{Z}^n$ as groups. If $a \in \mathfrak{a}$ such that $a \neq 0$ then $a | N_{K|\mathbb{Q}}(a)$ so $(N_{K|\mathbb{Q}}(a)) \subseteq (a) \subseteq \mathfrak{a}$. Clearly $\mathbb{Z}^n / N_{K|\mathbb{Q}}(a)\mathbb{Z}^n$ is finite, and there is an obvious surjection from this quotient to $\mathcal{O}_K/\mathfrak{a}$.

Page 35

- ... We are thus reduced to considering the case where $\mathfrak{a}$ is a prime power $\mathfrak{p}^\nu$ ...

  This is because
  $$\mathcal{O}_K/\mathfrak{a} = \mathcal{O}_K/\mathfrak{p}_1^{\nu_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{\nu_r}$$
  implies
  $$|\mathcal{O}_K/\mathfrak{a}| = |\mathcal{O}_K/\mathfrak{p}_1|^{\nu_1} \cdots |\mathcal{O}_K/\mathfrak{p}_r|^{\nu_r}.$$

- ... each quotient $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ is an $\mathcal{O}_K/\mathfrak{p}$-vector space ...

  The scalar multiplication is defined as $(a + \mathfrak{p}^{i+1})(r + \mathfrak{p}) = ra + \mathfrak{p}^{i+1}$ (we need to check $ra + \mathfrak{p}^{i+1}$ is a coset in $\mathfrak{p}^i/\mathfrak{p}^{i+1}$) and it's trivial to show this operation is well-defined.

Page 36

- ... This being true for all for all $\epsilon > 0$ and since $|N_{K|\mathbb{Q}}(a)|$ is always a positive integer there has to exist an $a \in \mathfrak{a}$, $a \neq 0$, such that
  $$|N_{K|\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a})$$

Notice that a depends on ϵ. We note $|N_{K|\mathbb{Q}}(a)|$ is a positive integer to stress the fact that we can choose an a such that $|N_{K|\mathbb{Q}}(a)|$ is minimal. Then we have a single a such that

$$|N_{K|\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}) + \epsilon$$

for all $\epsilon > 0$, and the claim follows.

- ... $\mathcal{O}_K/\mathfrak{p}$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$ ...

  To see this, $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z} + \mathfrak{p}/\mathfrak{p}$ by the second isomorphism theorem and $\mathbb{Z} + \mathfrak{p}/\mathfrak{p}$ is clearly a subfield of $\mathcal{O}_K/\mathfrak{p}$.

- ... The ideal $\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}]$ ...

  The first equality $\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1}$ shows that $\mathfrak{a}_1$ is indeed an ideal of $\mathcal{O}_K$ because $(\alpha) \subset \mathfrak{b}$. The second equality $\mathfrak{a}_1 = \alpha\gamma^{-1}\mathfrak{a}$ shows $\mathfrak{a}_1 \in [\mathfrak{a}]$ because $\alpha\gamma^{-1}\mathfrak{a} = (\alpha)(\gamma^{-1})\mathfrak{a} \in [\mathfrak{a}]$.

6 Dirichlet's Unit Theorem

Page 39

- > ... we now turn to the second main problem posed by the ring $\mathcal{O}_K$ of integers of an algebraic number field K, the group of units $\mathcal{O}_K^*$. It contains the finite group $\mu(K)$ of the roots of unity that lie in K ...

  Indeed, a root of unity satisfies the polynomial $x^n - 1$ for some n and so belongs to $\mathcal{O}_K$. Its inverse also satisfies $x^n - 1$ and so roots of unity are in $\mathcal{O}_K^*$. Also, it's a general fact of field theory that $\mu(K)$ is finite if $K|\mathbb{Q}$ is a finite field extension (which is assumed).

- > $$\mathcal{O}_K^* = \{\epsilon \in \mathcal{O}_K \mid N_{K|\mathbb{Q}}(\epsilon) = \pm 1\}, \quad \text{the group of units}$$

  This can be quickly proven using containment. For $\subseteq$ use the fact the norm is multiplicative, and for $\supseteq$ use Proposition 2.6 and notice there is a $\mathbb{Q}$-embedding $\sigma : K \to \overline{\mathbb{Q}}$ such that $\sigma(\epsilon) = \epsilon$.

- > ... For $\zeta \in \mu(K)$ and $\tau : K \to \mathbb{C}$ any embedding, we find $\log|\tau\zeta| = \log|1| = 0$ ...

  Notice that K-fixed embeddings are really maps $\tau : K \to \overline{\mathbb{Q}}$ but $\overline{\mathbb{Q}} \subset \mathbb{C}$ so we can regard τ as a map to $\mathbb{C}$. Also its a general (and easy to prove) fact that embeddings map roots of unity to roots of unity.

Page 40

- > ... $j\epsilon$ lines in a bounded domain of the $\mathbb{R}$-vector space $K_\mathbb{R}$. On the other hand, $j\epsilon$ is a point of the lattice $j\mathcal{O}_K$ of $K_\mathbb{R}$ (see (5.2)). Therefore the kernel of λ can contain only a finite number of elements, and thus being a finite group, contains only roots of unity in K^* ...

  We add a few details here. Taking the closure of this bounded domain we conclude the elements $j\epsilon$ form a discrete subset (because they lie in the lattice

$j\mathcal{O}_K$) of a compact set and are therefore finite. Now j is injective since each embedding $\tau : K \to \mathbb{C}$ is so that the kernel of λ is finite. It's a subgroup as well so $\epsilon^n = 1$ for every $\epsilon \in \ker \lambda$ and some n so that $\ker(\lambda) \subseteq \mu(K)$.

- > ... is a complete lattice in the $(r+s-1)$-dimensional vector space H ...

  The dimension of H is indeed $r+s-1$ because hyperplanes have one dimension lower than the ambient space.

- > ... the bounded domain
  >
  > $$\{(z_\tau) \in \prod_\tau \mathbb{C}^* \mid e^{-c} \leq |z_\tau| \leq e^c\}.$$
  >
  > It contains only finitely many elements of the set $j\mathcal{O}_K^*$ because this is a subset of the lattice $j\mathcal{O}_K$ ...

  Indeed, $\{(z_\tau) \in \prod_\tau \mathbb{C}^* \mid e^{-c} \leq |z_\tau| \leq e^c\}$ is compact and since $j\mathcal{O}_K^* \subset j\mathcal{O}_K$ is discrete (being a subset of a discrete set) their intersection is finite.

Page 41

- > ... Thus $M = \ell(T)$ will also be bounded ...

  The Γ-translates of M, $M + \gamma$ for $\gamma \in \Gamma$, will also cover H as desired for the following reason. $\ell : S \to H$ is surjective so $\ell(S) = H$. Also, $\ell(Tj_\epsilon) = \ell(T) + \ell(j_\epsilon) = M + \gamma$ and since $S = \bigcup_{\epsilon \in \mathcal{O}_K^*} Tj_\epsilon$ we conclude $H = \bigcup_{\gamma \in \Gamma} M + \gamma$.

- > ... where $c'_\tau = c_\tau |y_\tau|$, and one has $c'_\tau = c'_{\bar{\tau}}$ ...

  We choose the c_τ and define c'_τ ourselves, and so we are allowed to define $c'_{\bar{\tau}} = c_{\bar{\tau}} |y_{\bar{\tau}}|$. Implicitly, this is what we are doing.

Page 42

- > ... A is mapped isomorphically onto Γ by λ, i.e., on has $\mu(U) \cap A = \{1\}$ and therefore $\mathcal{O}_K^* = \mu(K) \times A$ ...

  Indeed, the map $\lambda|_A$ is a homomorphism because λ is and surjective since $\epsilon_i \mapsto v_i$ and the v_i's are a $\mathbb{Z}$-basis for Γ. So all we really need to show is $\lambda|_A$ is injective or equivalently $\mu(U) \cap A = \{1\}$. This is the case by considering the image of a general element of $\ker \lambda_A$ and using linear independence of the v_i's. To conclude $\mathcal{O}_K^* = \mu(K) \times A$, we need $\mu(K)$ and A to be normal in $\mathcal{O}_K^*$, $\mu(K)A = \mathcal{O}_K^*$, and $\mu(U) \cap A = \{1\}$. We already have the last of these three conditions. A is normal in $\mathcal{O}_K^*$ because normality is preserved under inverse images of homomorphisms and $A = \lambda^{-1}(\Gamma)$. $\mu(K)$ is normal because $\mu(K) = \ker \lambda$. By the first isomorphism theorem we have $\mathcal{O}_K^*/\mu(K) \cong \Gamma \cong A$. The isomorphism $\mathcal{O}_K^*/\mu(K) \xrightarrow{\sim} A$ sends $x\mu(K)$ to x which means x is an element of A. Since every element of $\mathcal{O}_K^*$ is in $x\mu(K)$ for some x it follows that $\mathcal{O}_K^* = A\mu(K)$.

Page 43

- > ... The t-dimensional volume of Φ therefore equals the $(t+1)$-dimensional volume of the parallelepiped spanned by the $\lambda_0, \lambda(\epsilon_1), \ldots, \lambda(\epsilon_t)$ in $\mathbb{R}^{t+1}$. But this has volume
  >
  > $$\pm \det \begin{pmatrix} \lambda_{01} & \lambda_1(\epsilon_1) & \cdots & \lambda_1(\epsilon_t) \\ \vdots & \vdots & & \vdots \\ \lambda_{0t+1} & \lambda_{t+1}(\epsilon_1) & \cdots & \lambda_{t+1}(\epsilon_t) \end{pmatrix}.$$
  >
  > Adding all rows to a fixed one, say the i-th row, this row has only zeroes, except for the first entry, which equals $\sqrt{r+s}$ ...

  The subscripts i on the $\lambda_i(e_j)$'s and $\lambda_{0i}(e_j)$'s for $1 \leq j \leq t$ are to indicate the components of $\lambda_0, \lambda(\epsilon_1), \ldots, \lambda(\epsilon_t)$. The reason why adding all rows to a fixed one gives zeroes in all entries except the first is because $\lambda(\mathcal{O}_K^*) \subseteq H$ and elements of the trace-zero hyperplane H have their entries sum to zero by definition. To find the determinant, add all rows to a fixed one, move the fixed row to the top of the matrix, and then partition it into a block matrix in the

obvious way. From here use formula for the determinant of a block matrix.

- > ... R is the absolute value of the determinant of an arbitrary minor of rank $t = r + s - 1$ of the following matrix:
  >
  > $$\begin{pmatrix} \lambda_1(\epsilon_1) & \cdots & \lambda_1(\epsilon_t) \\ \vdots & & \vdots \\ \lambda_{t+1}(\epsilon_1) & \cdots & \lambda_{t+1}(\epsilon_t) \end{pmatrix}.$$
  >
  > The absolute value R is called the regulator of the field K ...

  The phrase "R is the absolute value of the determinant of an arbitrary minor of rank $t = r + s - 1$" should not be taken in the usual sense. Notice that the matrix has t columns and $t+1$ rows, so by "arbitrary minor of rank $t = r+s-1$" we mean delete any row. Also, the regulator is well-defined because any choice of ϵ_is gives rise to a basis of Φ given by the $\lambda(\epsilon_i)$s and the determinant is independent of choice of basis. See the previous note for reason as to why we may take any minor (the minor is the bottom right block of the block matrix in the previous note).

7 Extensions of Dedekind Domains

Page 45

- > ... the integral domain $\mathcal{O}/\mathfrak{P}$ is an extension of the $\mathfrak{o}/\mathfrak{p}$, and therefore has itself to be a field, because if it were not, then it would admit a nonzero prime ideal whose intersection with $\mathfrak{o}/\mathfrak{p}$ would again be a nonzero prime ideal in $\mathfrak{o}/\mathfrak{p}$ ...

  We give a little more detail. To see that $\mathcal{O}/\mathfrak{P}$ is an extension of $\mathfrak{o}/\mathfrak{p}$, consider the natural homomorphism $\mathfrak{o} \to \mathcal{O}/\mathfrak{P}$. The kernel is $\mathfrak{o} \cap \mathfrak{P} = \mathfrak{p}$, so by the first isomorphism theorem $\mathfrak{o}/\mathfrak{p}$ is a a subfield of $\mathcal{O}/\mathfrak{P}$. If $\mathcal{O}/\mathfrak{P}$ is not a field let M a nonzero prime ideal of it and consider the homomorphism $\mathfrak{o}/\mathfrak{p} \to (\mathcal{O}/\mathfrak{P})/M$. The kernel is $\mathfrak{o}/\mathfrak{p} \cap M$ which is a prime ideal in $\mathfrak{o}/\mathfrak{p}$, a field, hence $M = \mathfrak{o}/\mathfrak{p}$. This is a contradiction.

- > ... let $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ ($\mathfrak{p} \neq 0$), so that $\pi\mathfrak{o} = \mathfrak{p}\mathfrak{a}$ with $\mathfrak{p} \nmid \mathfrak{a}$, hence $\mathfrak{p} + \mathfrak{a} = \mathfrak{o}$ ...

  We get $\pi\mathfrak{o} = \mathfrak{p}\mathfrak{a}$ by taking the prime decomposition of $\pi\mathfrak{o}$ and then letting $\mathfrak{a}$ be the product of all the factors except $\mathfrak{p}$. $\mathfrak{p} \nmid \mathfrak{a}$ because otherwise $\pi \in \mathfrak{p}^2$. Since $\mathfrak{p}$ is maximal, $\mathfrak{p} + \mathfrak{a} = \mathfrak{o}$.

- > ... Let $\alpha_1, \ldots, \alpha_n$ be a basis of $L|K$ contained in $\mathcal{O}$ ...

  To get the basis in $\mathcal{O}$, choose a basis and then clear denominators.

- > ... we find $s \notin \mathfrak{p}$ ...

  Otherwise, s and b lie in $\mathfrak{p}$ hence $+b = 1$ lies in $\mathfrak{p}$ as well which is impossible since $\mathfrak{p}$ is prime.

- > ... $s = \pi x$ for some $x \in \mathcal{O} \cap K = \mathfrak{o}$ ...

  Clearly $x \in \mathcal{O}$. $\pi \in \mathfrak{o}$, and so has an inverse in K. Since $s \in \mathfrak{o}$ we can view it as an element in K, and therefore $x = \pi^{-1}s \in K$.

- > ... The prime ideals occurring in the decomposition are precisely those prime ideals $\mathfrak{P}$ of $\mathcal{O}$ which lie over $\mathfrak{p}$ in the sense that one has the relation
  >
  > $$\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}$$

  We give justification to this statement. If $\mathfrak{P}$ is an arbitrary prime occurring in the prime decomposition of $\mathfrak{p}\mathcal{O}$, then $\mathfrak{p} \subset \mathfrak{p}\mathcal{O} \subset \mathfrak{P}$, so $\mathfrak{p} \subseteq \mathfrak{P} \cap o$. By maximality of $\mathfrak{p}$, $\mathfrak{p} = \mathfrak{P} \cap o$. Conversely, if $\mathfrak{p} = \mathfrak{P} \cap o$ then $\mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}$. If no prime ideal $\mathfrak{P}'$ occurring in the prime decomposition of $\mathfrak{p}\mathcal{O}$ was $\mathfrak{P}$ we could find $a_i \in \mathfrak{P}'$ such that $\prod_i a_i \in \mathfrak{p}\mathcal{O} \subset \mathfrak{P}$ with no $a_i \in \mathfrak{P}$. This is absurd.

Page 46

- > ... we have seen in the proof of (8.1) that $\mathcal{O}$ is a finitely generated o-module, so certainly $\dim_K(\mathcal{O}/\mathfrak{p}\mathcal{O}) < \infty$ ...

  Indeed, since $\mathcal{O}$ is a finitely generated o-module so is $\mathcal{O}/\mathfrak{p}\mathcal{O}$. Now the generators of $\mathcal{O}/\mathfrak{p}\mathcal{O}$ as a o-module are representatives for the generators of $\mathcal{O}/\mathfrak{p}\mathcal{O}$ as a $o/\mathfrak{p}$-vector space. Hence $\dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) = \operatorname{rank}_o(\mathcal{O}/\mathfrak{p}\mathcal{O}) < \infty$.

- > ... find $a \in \mathfrak{a}^{-1}$ such that $a \notin \mathfrak{a}^{-1}\mathfrak{p}$, hence $a\mathfrak{a} \not\subseteq \mathfrak{p}$. Then the elements $aa_1, \ldots, aa_m$ lie in $\mathcal{O}$, but not all belong to $\mathfrak{p}$ ...

  Clearly $\mathfrak{a}^{-1}\mathfrak{p} \subseteq \mathfrak{a}^{-1}$. If we couldn't find such an a, then $\mathfrak{a}^{-1}\mathfrak{p} = \mathfrak{a}^{-1}$ which contradicts the prime decomposition of $\mathfrak{a}^{-1}$. So, such an a exists. The elements $aa_1, \ldots, aa_m$ lie in $\mathcal{O}$ by definition of $a \in \mathfrak{a}^{-1}$, and not all lie in $\mathfrak{p}$ because otherwise $a\mathfrak{a} \subseteq \mathfrak{p}$ since the a_is generate $\mathfrak{a}$.

- > ... Since $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$, we have $\mathfrak{p}N = N$ ...

  By $\mathfrak{p}N$ we really mean $\mathfrak{p}\mathcal{O}N$. To see why $\mathfrak{p}N = N$, notice $N = \mathcal{O}/M$ is a $\mathcal{O}$-module and recall that $\mathfrak{p}\mathcal{O}$ is an ideal (hence subset) of $\mathcal{O}$. This implies $\mathfrak{p}N \subseteq N$. For the reverse inclusion, let $\alpha + M$ be a class in N. Since $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$, we may write $\alpha = m + \sum_{i=1}^{k} p_i\alpha_i$ for some $p_i \in \mathfrak{p}$ and $\alpha_i \in \mathcal{O}$. Then $\alpha + M = \sum_{i=1}^{k} p_i\alpha_i + M$. The right-hand side is a class in $\mathfrak{p}N$, so $\alpha + M$ is a class in $\mathfrak{p}N$. This implies $N \subseteq \mathfrak{p}N$.

Page 47

- > ... we find $d \equiv (-1)^s \bmod \mathfrak{p}$ because $a_{ij} \in \mathfrak{p}$ ...

  Since the determinant of a matrix is a polynomial in the entries, and modular arithmetic respects addition and multiplication, we may calculate d modulo $\mathfrak{p}$ by taking the entries of $(a_{ij}) - I$ modulo $\mathfrak{p}$ and then calculating the determinant.

- > ... It follows that $L = dL = K\omega_1 + \cdots + K\omega_m$ ...

  Recall L is $\frac{\mathcal{O}}{\mathcal{O}^\times}$ as fractions and not as a quotient, K is the field of fractions of $\mathcal{O}$, and $d \in \mathfrak{p} \subseteq L$. With this is mind,

  $$L = dL = \frac{d\mathcal{O}}{\mathcal{O}^\times} \subseteq \frac{\mathcal{O}\omega_1 + \cdots + \mathcal{O}\omega_m}{\mathcal{O}^\times} = K\omega_1 + \cdots + K\omega_m.$$

  The reverse inclusion is clear since the $\omega_i s$ are in $\mathcal{O} \subset L$ and $K \subseteq L$.

- > ... for if $\alpha \in \mathfrak{P}_i^\nu \smallsetminus \mathfrak{P}_i^{\nu+1}$ ...

  Such an α exists by the unique prime decomposition of ideals.

- > ... $\mathfrak{P}_i^\nu$ is the gcd of $\mathfrak{P}_i^{\nu+1}$ and $(\alpha) = \alpha\mathcal{O}$ so that $\mathfrak{P}_i^\nu = \alpha\mathcal{O} + \mathfrak{P}_i^{\nu+1}$ ...

  Indeed, $\mathfrak{P}_i^{\nu+1}$ does not divide (α), hence cannot be the gcd, because α is not an element of $\mathfrak{P}_i^{\nu+1}$. By prime decomposition, the next ideal to consider is $\mathfrak{P}_i^\nu$. It divides (α) because α is an element of $\mathfrak{P}_i^\nu$. Both ideals considered also obviously divide $\mathfrak{P}_i^{\nu+1}$.

- > ... the separable extension $L|K$ is given by a primitive element $\theta \in \mathcal{O}$ with minimal polynomial
  >
  > $$p(X) \in o[X]$$

  We may assume $\theta \in \mathcal{O}$ because if $\theta' \in L \smallsetminus \mathcal{O}$ was our primitive element, then $\theta' = \frac{\theta}{a}$ with $\theta \in \mathcal{O}$ and $a \in o \in K$. So if we clear denominators, we may use θ

as our primitive element and it satisfies a polynomial which (we may assume is minimal) in $o[X]$.

- > ... Since $\mathcal{O}$ is a finitely generated o-module (see proof of (8.1)), one has $\mathfrak{F} \neq 0$ ...

  $\mathfrak{F} \neq 0$ for the following reason. Let $\omega_1, \ldots, \omega_n$ be a generating set for $\mathcal{O}$ as an o-module. Since $L = K(\theta)$ and $[L : K] = n$ is finite, we can say $L = K[\theta]$. So, we may write $\omega_i = \sum_{j=1}^{n} k_{ij}\theta^i$ for each i and some $k_{ij} \in K$. Setting $\alpha_i = \prod_{j=1}^{n} k_{ij}$ and recalling that K is the field of fractions of o we conclude $\alpha_i\omega_i \in o[\theta]$. Setting $\alpha = \prod_{i=1}^{n} \alpha_i$ we find $\alpha\omega_i \in o[\theta]$ for all i. Since the ω_is generate $\mathcal{O}$, $\alpha\mathcal{O} \subseteq o[\theta]$ so that $\alpha \in \mathfrak{F}$.

- > ... Let $\mathfrak{p}$ be a prime ideal of o which is relatively prime to the conductor $\mathfrak{F}$ ...

  When we say $\mathfrak{p}$ is relatively prime to $\mathfrak{F}$ we mean $\mathfrak{p}\mathcal{O}$ is relatively prime to $\mathfrak{F}$.

Page 48

- > ... As $\mathfrak{F} \subseteq \mathcal{O}'$ ...

  It is indeed the case that $\mathfrak{F} \subseteq \mathcal{O}'$ because if $\alpha \in \mathfrak{F}$, then $\alpha\mathcal{O} \subseteq \mathcal{O}'$. So in particular $\alpha \in \mathcal{O}'$ because $\mathcal{O}$ has an identity.

- > ... the homomorphism $\mathcal{O}' \to \mathcal{O}/\mathfrak{p}\mathcal{O}$ is surjective. It has kernel $\mathfrak{p}\mathcal{O} \cap \mathcal{O}'$, which equals $\mathfrak{p}\mathcal{O}'$. Since $(\mathfrak{p}, \mathfrak{F} \cap o) = 1$, it follows that $\mathfrak{p}\mathcal{O} \cap \mathcal{O}' = (\mathfrak{p} + \mathfrak{F})(\mathfrak{p}\mathcal{O} \cap \mathcal{O}') \subseteq \mathfrak{p}\mathcal{O}'$. ...

  This is a typo, we mean to write $(\mathfrak{p} + (\mathfrak{F} \cap o))(\mathfrak{p}\mathcal{O} \cap \mathcal{O}')$. Now the inclusion $\mathfrak{p}\mathcal{O}' \subseteq \mathfrak{p}\mathcal{O} \cap \mathcal{O}'$ is clear. To prove the reverse inclusion we first show that if $\mathfrak{p}\mathcal{O}$ and $\mathfrak{F}$ are relatively prime, then so are $\mathfrak{p}$ and $\mathfrak{F} \cap o$ (this is another way of saying $(\mathfrak{p}, \mathfrak{F} \cap o) = 1$). Let $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ (not necessarily all unique) be the decomposition of $\mathfrak{F}$ into prime ideals. Then $\mathfrak{P}_i \cap o \subsetneq \mathfrak{p}$. Otherwise, $\mathfrak{P}_i \cap o \subseteq \mathfrak{p}$, and by maximality of $\mathfrak{P}_i \cap o$, $\mathfrak{P}_i \cap o = \mathfrak{p}$. But this means $\mathfrak{P}_i$ is a prime of $\mathfrak{F}$

lying above $\mathfrak{p}$, hence a prime idea of $\mathfrak{p}\mathcal{O}$, contradicting relative primality. Now let $\alpha_i \in \mathfrak{P}_i \cap \mathcal{o} \setminus \mathfrak{p}$, and define $\alpha = \prod_{i=1}^{r} \alpha_i$. Then $\alpha \in \mathfrak{F} \cap \mathcal{o} \setminus \mathfrak{p}$ so $\mathfrak{F} \cap \mathcal{o} \subsetneq \mathfrak{p}$. By maximality of $\mathfrak{p}$, $\mathfrak{p} + (\mathfrak{F} \cap \mathcal{o}) = \mathcal{o}$ which means $\mathfrak{p}$ and $\mathfrak{F} \cap \mathcal{o}$ are relatively prime. Then

$$\mathfrak{p}\mathcal{O} \cap \mathcal{O}' = (\mathfrak{p} + (\mathfrak{F} \cap \mathcal{o}))(\mathfrak{p}\mathcal{O} \cap \mathcal{O}') \subseteq \mathfrak{p}\mathcal{O}',$$

where the containment is true for the following reason. By the definition of $\mathfrak{F}$, $\mathfrak{F}\mathcal{O} \subseteq \mathcal{O}'$, hence $(\mathfrak{F} \cap \mathcal{o})\mathfrak{p}\mathcal{O} \subseteq \mathfrak{p}\mathcal{O}'$. So $(\mathfrak{p} + (\mathfrak{F} \cap \mathcal{o}))(\mathfrak{p}\mathcal{O} \cap \mathcal{O}') = \mathfrak{p}(\mathfrak{p}\mathcal{O} \cap \mathcal{O}') + (\mathfrak{F} \cap \mathcal{o})(\mathfrak{p}\mathcal{O} \cap \mathcal{O}') \subseteq \mathfrak{p}\mathcal{O}' + \mathfrak{p}\mathcal{O}' = \mathfrak{p}\mathcal{O}'$.

- > ... The second isomorphism is deduced from the surjective homomorphism
  >
  > $$\mathcal{o}[X] \to \bar{\mathcal{o}}[X]/(\bar{p}(X)).$$
  >
  > Its kernel is the ideal generated by $\mathfrak{p}$ and $p(X)$, and in view of $\mathcal{O}' = \mathcal{o}[\theta] = \mathcal{o}[X]/(p(X))$, we have $\mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \bar{\mathcal{o}}[X]/(\bar{p}(X))$ ...

The surjective isomorphism sends a polynomial $f(X)$ with coefficients in $\mathcal{o}$ to the polynomial $\overline{f}(X)$ where the bar indicates $f(X)$ has coefficients reduced modulo $\mathfrak{p}$. Then $\overline{f}(X)$ is taken modulo $(\bar{p}(X))$. The ideal generated by $\mathfrak{p}$ and $p(X)$ is by definition $\mathfrak{p}\mathcal{o}[X] + (p(X))$. Since the kernel of the map is $\mathfrak{p}\mathcal{o}[X] + (p(X))$, $\mathcal{o}[X]/\mathfrak{p}\mathcal{o}[X] + (p(X)) \cong \bar{\mathcal{o}}[X]/(\bar{p}(X))$. Now the surjective homomorphism

$$\mathcal{o}[\theta] \to \mathcal{o}[X]/\mathfrak{p}\mathcal{o}[X] + (p(X)),$$

which sends $f(\theta)$ to $f(x)$ and then reduces modulo $\mathfrak{p}\mathcal{o}[X] + (p(X))$ clearly has kernel $\mathfrak{p}\mathcal{o}[\theta] + (p(\theta)) = \mathfrak{p}\mathcal{o}[\theta]$ because $p(X)$ is the minimal polynomial for θ (this is essentially using the fact $\mathcal{o}[\theta] = \mathcal{o}[X]/(p(X))$). Therefore

$$\mathcal{O}'/\mathfrak{p}\mathcal{O}' = \mathcal{o}[\theta]/\mathfrak{p}\mathcal{o}[\theta] \cong \mathcal{o}[X]/\mathfrak{p}\mathcal{o}[X] + (p(X)) \cong \bar{\mathcal{o}}[X]/(\bar{p}(X)).$$

- ... Since $\bar{p}(X) = \prod_{i=1}^{r} \bar{p}_i(X)^{e_i}$, the Chinese remainder theorem finally gives the isomorphism

$$\bar{\mathcal{O}}[X]/(\bar{p}(X)) \cong \bigoplus_{i=1}^{r} \bar{\mathcal{O}}[X]/(\bar{p}_i(X))^{e_i}.$$

This shows that the prime ideals of the ring $R = \bar{\mathcal{O}}[X]/(\bar{p}(X))$ are the principle ideals $(\bar{p}_i)$ generated by the $\bar{p}_i(X)$ mod $\bar{p}(X)$, for $i = 1, \ldots, r$, that the degree $[R/(\bar{p}_i) : \bar{\mathcal{O}}]$ equals the degree of the polynomial $\bar{p}_i(X)$, and that

$$(0) = (\bar{p}) = \bigcap_{i=1}^{r} (\bar{p}_i)^{e_i}$$

There are a couple of things we want to mention here. Firstly, recall that powers of coprime ideals are coprime and so $\bar{p}_i(X)^{e_i}$ and $\bar{p}_j(X)^{e_j}$ are coprime for all $1 \leq i, j \leq r$ with $i \neq j$. This lets us use the Chinese remainder theorem. Secondly, a prime ideal in $\bar{\mathcal{O}}[X]/(\bar{p}_i(X))^{e_i}$ is precisely a prime ideal of $\bar{\mathcal{O}}[X]$ containing $(\bar{p}_i(X))^{e_i}$. Since $\bar{\mathcal{O}}$ is a field, $\bar{\mathcal{O}}[X]$ is a PID, in particular a UFD, and hence the irreducible $\bar{p}_i(X)$ is prime from which is follows that $(\bar{p}_i(X))$ is the only prime ideal of $\bar{\mathcal{O}}[X]$ containing $(\bar{p}_i(X))^{e_i}$. If there were another, it would have to be of the form $(\bar{q}(X))$ for some irreducible $\bar{q}(X)$. But then $\bar{f}(X)\bar{q}(X)^{e_i} = \bar{p}_i(X)^{e_i}$ for some $\bar{f}(X)$. Since $\bar{q}(X) \neq 1$ and both $\bar{q}(X)$ and $\bar{p}_i(X)$ are irreducible we deduce $\bar{f}(X) = 1$ and therefore $\bar{q}(X) = \bar{p}_i(X)$. So, the prime ideal of $\bar{\mathcal{O}}[X]/(\bar{p}_i(X))^{e_i}$ is $(\bar{p}_i(X))/(\bar{p}_i(X))^{e_i}$. Now a prime ideal in a direct sum ring is a prime ideal of one of the terms and the full ring everywhere else, in other words it takes the form:

$$\bigoplus_{\substack{i=1 \\ i \neq j}}^{r} \bar{\mathcal{O}}[X]/(\bar{p}_i(X))^{e_i} \oplus (\bar{p}_j(X))/(\bar{p}_j(X))^{e_j}.$$

The image of $(\bar{p}_j)$ under the isomorphism is exactly this prime ideal. Indeed, $(\bar{p}_j(X))$ is relatively prime to $(\bar{p}_i(X))^{e_i}$ for all $i \neq j$, so $(\bar{p}_j(X)) + (\bar{p}_i(X))^{e_i} = \bar{\mathcal{O}}[X]$; this implies the image of $(\bar{p}_j)$, which is $(\bar{p}_j(X))$, is $\bar{\mathcal{O}}[X]/(\bar{p}_i(X))^{e_i}$ for all terms j with $j \neq i$, and for $j = i$, obviously the image of $(\bar{p}_j)$ is $(\bar{p}_j(X))/(\bar{p}_j(X))^{e_j}$. This proves the claim concerning the prime ideals of R. Using the above, $R/(\bar{p}_i)$ under the isomorphism is isomorphic to $\bar{\mathcal{O}}[X]/(\bar{p}_i(X))$ by the second isomorphism theorem. Clearly $[\bar{\mathcal{O}}[X]/(\bar{p}_i(X)) : \bar{\mathcal{O}}]$ is the degree of the polynomial

$\bar{p}_i(X)$. Hence so is $[R/(\bar{p}_i) : \bar{o}]$. The first equality in

$$(0) = (\bar{p}) = \bigcap_{i=1}^{r} (\bar{p}_i)^{e_i}$$

is clear. To see the second, notice $(\bar{p}) \subseteq \bigcap_{i=1}^{r} (\bar{p}_i)^{e_i}$. To get the reverse equality, the image of $\bigcap_{i=1}^{r} (\bar{p}_i)^{e_i}$ under the isomorphism is trivial and so $\bigcap_{i=1}^{r} (\bar{p}_i)^{e_i}$ is contained in the kernel which is $(\bar{p})$.

- > ... let $\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}$ be the preimage of $\overline{\mathfrak{P}_i}$ with respect to the canonical homomorphism
  >
  > $$\mathcal{O} \to \mathcal{O}/\mathfrak{p}\mathcal{O}$$

  Indeed, $\overline{\mathfrak{P}_i}$ is the principle ideal generated by $p_i(\theta)$ mod $\mathfrak{p}\mathcal{O}$ so as a set it is exactly $\mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}$ which is precisely the preimage. Note the preimage of a prime ideal is prime under a homomorphism so $\mathfrak{P}_i$ is also prime.

- > ... $\mathfrak{P}_i$, for $i = 1, \ldots, r$, varies over the prime ideals of $\mathcal{O}$ above $\mathfrak{p}$. $f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}]$ is the degree of the polynomial $\bar{p}_i(X)$. Furthermore $\mathfrak{P}_i^{e_i}$ is the preimage of $\overline{\mathfrak{P}_i}^{e_i}$ (because $e_i = \#\{\overline{\mathfrak{P}}^{\nu} | \nu \in \mathbb{N}\}$), and $\mathfrak{p}\mathcal{O} \supseteq \bigcap_{i=1}^{r} \mathfrak{P}_i^{e_i}$, so that $\mathfrak{p}\mathcal{O} \mid \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ and therefore $\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ because $\sum e_i f_i = n$ ...

  There are several details to go over here. The $\mathfrak{P}_i$s vary over the prime ideals of $\mathcal{O}$ above $\mathfrak{p}$ because $\mathfrak{p} \subseteq (\mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}) \cap o$ since $\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}$ and $\mathfrak{p} \subseteq o$. By the fourth isomorphism theorem $\overline{\mathfrak{P}_i} = \mathfrak{P}_i/\mathfrak{p}\mathcal{O}$, and hence by the second isomorphism theorem $\overline{\mathcal{O}}/\overline{\mathfrak{P}_i} \cong \mathcal{O}/\mathfrak{P}_i$. Since $[\overline{\mathcal{O}}/\overline{\mathfrak{P}_i} : \bar{o}]$ is the degree of $\bar{p}_i(X)$ so is $f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}]$. Obviously $\mathfrak{P}_i^{e_i} \subseteq \pi^{-1}(\overline{\mathfrak{P}_i}^{e_i})$, which implies $\overline{\mathfrak{P}_i}^{e_i} \subseteq \overline{\mathfrak{P}_i}^{e_i}$ where the inclusion is really equality. Therefore, the prime decomposition of $\pi^{-1}(\overline{\mathfrak{P}_i}^{e_i})$ is $\mathfrak{P}_i^{e_i}$ (use contradiction and the natural surjection) and we have equality. $\mathfrak{p}\mathcal{O} \supseteq \bigcap_{i=1}^{r} \mathfrak{P}_i^{e_i}$ because $(0) = \bigcap_{i=1}^{r} \overline{\mathfrak{P}_i}^{e_i}$. Since powers of coprime ideals are coprime, $\mathfrak{P}_i^{e_i}$ and $\mathfrak{P}_j^{e_j}$ for $i \neq j$ and so $\bigcap_{i=1}^{r} \mathfrak{P}_i^{e_i} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$. The last statement is true for the following reason. Since $\mathfrak{p}\mathcal{O} \mid \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ and the $\mathfrak{P}_i$s are the only prime ideas in the decomposition of $\mathfrak{p}\mathcal{O}$, it must be the case that $\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i'}$ where $e_i' \geq e_i$ for all i. But then $\sum e_i' f_i = \sum e_i f_i = n$ and so $e_i' = e_i$ for all i (use induction on r).

Page 49

- > ... Let $\theta \in \mathcal{O}$ be a primitive element for L, i.e., $L = K(\theta)$, and let $p(X) \in o[X]$ be its minimal polynomial. Let
  >
  > $$d = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \in o$$
  >
  > be the discriminant of $p(X)$ ...

  By saying d is the discriminant of $p(X)$, we really mean d is the discriminant of the basis $1, \theta, \ldots, \theta^{n-1}$ for $L|K$. $1, \theta, \ldots, \theta^{n-1}$ is in fact a basis for $L|K$ since $K[x]/(p(X)) \cong K(\theta) = L$ and the image of the basis for $K[x]/(p(X))|K$ under the isomorphism is precisely $1, \theta, \ldots, \theta^{n-1}$.

- > ... every prime idea $\mathfrak{p}$ of K which is relatively prime to d and to the conductor $\mathfrak{F}$ of $o[\theta]$ is unramified ...

  In the latter part of the proof it is shown why $\mathfrak{p}$ is unramified if it meets these conditions. What we show here is that finitely many prime ideals $\mathfrak{p}$ don't meet these conditions. First notice $d \notin \mathfrak{p}$ is equivalent to $\mathfrak{p} + do = o$. Now let $do = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_s^{e_s'}$ be the decomposition into prime ideals. Then $d \in \mathfrak{p}$ if and only if $\mathfrak{p}$ is in the decomposition of do. Indeed, if $\mathfrak{p}$ is in the decomposition of do then $d \in do = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_s^{e_s'} \subseteq \mathfrak{p}$. Otherwise, if $d \in \mathfrak{p}$ then $do = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_s^{e_s'} \subseteq \mathfrak{p}$. If $\mathfrak{p}$ is not in the decomposition, then we may choose $\alpha_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ (because $\mathfrak{p}_i$ and $\mathfrak{p}$ are different prime ideals) and define $\alpha = \prod_{i=1}^{s} \alpha_i^{e_i'}$. Then $\alpha \in \mathfrak{p}$ and by primality $\alpha_i \in \mathfrak{p}$ for some i, a contradiction. There are finitely many prime ideals in the decomposition of do so we are done in this case. Now let $\mathfrak{F} = \mathfrak{P}_1^{e_1''} \cdots \mathfrak{P}_t^{e_t''}$ be the decomposition into prime ideals, and suppose $\mathfrak{p}$ is a prime ideal which is not relatively prime to the conductor, so $\mathfrak{p}\mathcal{O} + \mathfrak{F}$ is a nonzero proper ideal of $\mathcal{O}$. Then there is a prime ideal $\mathfrak{P}$ such that $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}$ and $\mathfrak{P} \mid \mathfrak{F}$. For an analogous reason as to why $\mathfrak{p}$ is one of the prime ideals in the decomposition of $d\mathcal{O}$ above, $\mathfrak{P}$ is one of the prime ideals of $\mathfrak{F}$. The converse is easy since if $\mathfrak{p}\mathcal{O}$ and $\mathfrak{F}$ share a prime ideal $\mathfrak{P}$, then $\mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}$ and $\mathfrak{F} \subseteq \mathfrak{P}$ so $\mathfrak{p}\mathcal{O} + \mathfrak{F} \subseteq \mathfrak{P} \neq \mathcal{O}$. Since there are finitely many prime ideal in the decomposition of $\mathfrak{F}$ we are done in this case as well. So, there are finitely many primes $\mathfrak{p}$ which are not both relative prime to d and $\mathfrak{F}$.

- > ...so certainly if $\bar{p}(X)$ has no multiple roots. But this is the case since the discriminant $\bar{d} = d \bmod \mathfrak{p}$ of $\bar{p}(X)$ is nonzero. The residue class field extensions $\mathcal{O}/\mathfrak{P}_i|o/\mathfrak{p}$ are generated by $\bar{\theta} = \theta \bmod \mathfrak{P}_i$ and therefore separable ...

  Since the $\bar{p}_i(X)$s are monic irreducibles, they are the minimal polynomial of some element. Its then easy to see $\bar{p}(X) = \bar{p}_1(X)^{e_1} \cdots \bar{p}_r(X)^{e_r}$ has no multiple roots if and only if $e_i = 1$ for all i, just recall the minimal polynomial of an element divides any polynomial that has that element as a root. Now $d \bmod \mathfrak{p}$ is zero if and only if $(\theta_i - \theta_j)^2 \bmod \mathfrak{p} \equiv ((\theta_i - \theta_j) \bmod \mathfrak{p})^2 \bmod \mathfrak{p}$ is zero for some $i < j$ and this happens if and only if $\bar{p}(X)$ has a multiple root. Since $o/\mathfrak{p}$ is a finite field and every extension of a finite field is separable, we conclude $\mathcal{O}/\mathfrak{P}_i|o/\mathfrak{p}$ is separable. This is independent of looking at the generator.

Page 50

- > ...the **Legendre symbol** $\left(\frac{a}{p}\right)$, which, for every rational number a relatively prime to p, is defined to be $\left(\frac{a}{p}\right) = 1$ or -1, according as $x^2 \equiv a \bmod p$ has or does not have a solution. This symbol is multiplicative,
  >
  > $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$
  >
  > This is because the group $\mathbb{F}_p^*$ is cyclic of order $p-1$ and the subgroup $\mathbb{F}_p^{*2}$ of squares has index 2, i.e., $\mathbb{F}_p^*/\mathbb{F}_p^{*2} \cong \mathbb{Z}/2\mathbb{Z}$. Since $\left(\frac{a}{p}\right) = 1 \iff \bar{a} \in \mathbb{F}_p^{*2}$, one also has
  >
  > $$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

  There are a couple of things to note here. Firstly, we mean integer instead of rational number. Often, we allow a to be any integer and extend the definition by defining $\left(\frac{a}{p}\right) = 0$ if p divides a. We do not do this at the present. If the argument for why the Legendre symbol is multiplicative is not clear, notice

that if

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p,$$

(this equivalence is called Euler's criterion) then

$$\left(\frac{ab}{p}\right) \equiv ab^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p.$$

Since the Legendre symbol takes values in $\{\pm 1\}$, $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0, \pm 2$, but the odd prime p divides $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ by the congruence above so the ± 2 case is impossible. We now give a full proof of Euler's criterion. By Lagrange's theorem, $x^2 \equiv a \bmod p$ has at most two solutions, and actually has none or exactly two because if x is a solution then so is $-x$. This implies there are at least $\frac{p-1}{2}$ quadratic residues because if there were less, one of the congruences $x^2 \equiv a \bmod p$ has more than two solutions. Now $(a, p) = 1$ implies, by Fermat's little theorem, that $a^{p-1} \equiv 1 \bmod p$. This is equivalent to

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \bmod p.$$

Since $\mathbb{F}_p$ is a field, one of these terms must be zero. Now $\left(\frac{a}{p}\right) = 1 \iff \bar{a} \in \mathbb{F}_p^{*2}$, so $\left(\frac{a}{p}\right) = 1$ implies $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem again. This means every quadratic residue makes the first factor zero, and if we apply Lagrange's theorem again there can be no more than $\frac{p-1}{2}$ quadratic residues. Hence by the previous count, there are exactly $\frac{p-1}{2}$ quadratic residues each of which make the first factor zero implying

$$\left(\frac{a}{p}\right) \equiv 1 \equiv a^{\frac{p-1}{2}} \bmod p,$$

if a is a quadratic residue. It follows that the other $\frac{p-1}{2}$ nonresidues a must make the second factor zero, implying

$$\left(\frac{a}{p}\right) \equiv -1 \equiv a^{\frac{p-1}{2}} \bmod p.$$

Page 52

- $\dots \sum_{a,b} \left(\frac{-ab}{\ell}\right) \zeta^{a+b} = \sum_{a,b} \left(\frac{ab^{-1}}{\ell}\right) \zeta^{a-b} \dots$

  This follows by substituting $-b$ for b, and then using the fact $\left(\frac{b}{\ell}\right) = \left(\frac{b^{-1}}{\ell}\right)$ and multiplicativity to write $\left(\frac{ab^{-1}}{\ell}\right)$ for $\left(\frac{ab}{\ell}\right)$.

- $\dots \sum_c \left(\frac{c}{\ell}\right) = 0$, as one sees by multiplying the sum with a symbol $\left(\frac{x}{\ell}\right) = -1 \dots$

  To see this note
  $$-\sum_c \left(\frac{c}{\ell}\right) = \sum_c \left(\frac{xc}{\ell}\right) = \sum_c \left(\frac{c}{\ell}\right),$$
  since both c and xc run over $(\mathbb{Z}/\ell\mathbb{Z})^*$ as c does, and this equality happens if and only if $\sum_c \left(\frac{c}{\ell}\right) = 0$.

- $\dots \tau^p \equiv \sum_a \left(\frac{a}{\ell}\right) \zeta^{ap} \dots$

  From the definition of τ and the binomial theorem we have $\tau \equiv \sum_a \left(\frac{a}{\ell}\right)^p \zeta^{ap} \bmod p$. Since p is an odd prime $\left(\frac{a}{p}\right)^p = \left(\frac{a}{p}\right)$, and so we deduce $\tau \equiv \sum_a \left(\frac{a}{\ell}\right) \zeta^{ap} \bmod p$.