

**Dedekind's Theorem (one of them, anyway)**  
Math 581, Spring 2006

**Background information:** For our purposes here, “ring” will mean commutative ring with identity. You should remind yourself of the definition for a ring homomorphism. Recall that the kernel of a ring homomorphism is an ideal, and that given an ideal, there is a homomorphism (the canonical map) with kernel equal to that ideal. The ideal is maximal if and only if the image of the canonical map is a field.

If  $R$  is a ring and  $\phi$  is a ring homomorphism on  $R$ , then we get an induced homomorphism  $\bar{\phi}$  on the polynomial ring  $R[X]$  by letting  $\phi$  act on the coefficients:

$$\bar{\phi}(r_n X^n + r_{n-1} X^{n-1} + \cdots + r_0) := \phi(r_n) X^n + \phi(r_{n-1}) X^{n-1} + \cdots + \phi(r_0).$$

If  $R$  is a subring of  $S$ , then for every element  $s \in S$  we also get a homomorphism from the polynomial ring  $R[X]$  into  $S$  by evaluating at  $s$ :

$$r_n X^n + r_{n-1} X^{n-1} + \cdots + r_0 \mapsto r_n s^n + r_{n-1} s^{n-1} + \cdots + r_0.$$

Recall that the polynomial ring  $F[X]$  is a Euclidean domain via the usual division algorithm for polynomials whenever  $F$  is a field. It is thus a principal ideal domain and a unique factorization domain. In particular, if  $P(X) \in F[X]$  is an irreducible polynomial and we let  $(P(X))$  denote the principal ideal generated by  $P(X)$ , then the quotient ring  $F[X]/(P(X))$  is an extension field of  $F$  of degree equal to the degree of  $P(X)$ .

As usual,  $K$  will denote a number field with ring of integers  $\mathfrak{O}_K$ . The upper case script German (“fraktur”) font will be used to denote fractional ideals and the lower case Greek font will be used to denote elements of  $K$ .

We'll denote the finite field with  $q$  elements by  $\mathbb{F}_q$ .

**Theorem:** Suppose  $\mathfrak{O}_K = \mathbb{Z}[\alpha]$  and  $p$  is a prime number. Let  $P(X) \in \mathbb{Z}[X]$  be the minimal polynomial for  $\alpha$  and let  $\bar{P}(X)$  denote the image of  $P(X)$  under the homomorphism  $\bar{\phi}$  from  $\mathbb{Z}[X]$  to  $\mathbb{F}_p[X]$  induced by the canonical map  $\phi: \mathbb{Z} \rightarrow \mathbb{F}_p$ . If

$$\bar{P}(X) = \bar{P}_1^{e_1}(X) \cdots \bar{P}_r^{e_r}(X)$$

is the factorization of  $\bar{P}$  into a product of monic irreducible polynomials, then the principal ideal generated by  $p$  in  $\mathfrak{O}_K$  factors as

$$(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where the residue class degree of each  $\mathfrak{P}_i$  is  $f_i := \deg \bar{P}_i(X)$ . Further,

$$\mathfrak{P}_i = \text{gcd}(p, P_i(\alpha))$$

for each  $i$ , where  $\bar{\phi}(P_i(X)) = \bar{P}_i(X)$ .

**Proof:** Fix an  $i$  for the moment and let  $\alpha_i$  be a root of  $\bar{P}_i(X)$  in some extension field. We then have the commutative diagram

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\theta_1} & \mathbb{Z}[\alpha] = \mathfrak{O}_K \\ \bar{\phi} \downarrow & & \theta_3 \downarrow \\ \mathbb{F}_p[X] & \xrightarrow{\theta_2} & \mathbb{F}_p[\alpha_i] \cong \mathbb{F}_q \end{array}$$

where  $\theta_1$  and  $\theta_2$  are evaluation maps and

$$\theta_3(z_n\alpha^n + z_{n-1}\alpha^{n-1} + \cdots + z_0) = \phi(z_n)\alpha_i^n + \phi(z_{n-1})\alpha_i^{n-1} + \cdots + \phi(z_0).$$

Note that the kernel of  $\theta_1$  is the principal ideal generated by  $P(X)$  and the kernel of  $\theta_2$  is the principal ideal generated by  $\overline{P}_i(X)$ , so that

$$\mathbb{F}_p[\alpha_i] \cong \mathbb{F}_p[X]/(\overline{P}_i(X)) \cong \mathbb{F}_q,$$

where  $q = p^{f_i}$ . This implies that the kernel of  $\theta_3$  is a maximal ideal of  $\mathfrak{O}_K$ ; call it  $\mathfrak{P}_i$ . The residue class degree of  $\mathfrak{P}_i$  is  $f_i$  since  $\mathfrak{O}_K/\mathfrak{P}_i \cong \mathbb{F}_q$ .

Consider the kernel of the composition  $\theta := \theta_3 \circ \theta_1 = \theta_2 \circ \overline{\phi}$ . Since the kernel of  $\overline{\phi}$  is the principal ideal in  $\mathbb{Z}[X]$  generated by  $p$  and the kernel of  $\theta_2$  is the principal ideal generated by  $\overline{P}_i(X)$ , the kernel of  $\theta$  is the ideal of  $\mathbb{Z}[X]$  generated by  $p$  and  $P_i(X)$ . Thus, the kernel of  $\theta_3$  is generated by  $\theta_1(p) = p$  and  $\theta_1(P_i(X)) = P_i(\alpha)$ . In other words,  $\mathfrak{P}_i = \gcd(p, P_i(\alpha))$ .

Now  $\overline{P}(X) = \overline{P}_1^{e_1}(X) \cdots \overline{P}_r^{e_r}(X)$  if and only if  $P(X) - P_1(X)^{e_1} \cdots P_r(X)^{e_r} \in \ker \overline{\phi}$ , and this in turn implies that  $P_1(\alpha)^{e_1} \cdots P_r(\alpha)^{e_r} \in (p)$ . Since  $\mathfrak{P}_i^{e_i} \subseteq \gcd(p, P_i(\alpha)^{e_i})$  for each  $i$ , we see that  $(p) \supseteq \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ . Taking norms and noting that  $e_1 f_1 + \cdots + e_r f_r = \deg P(X) = [K : \mathbb{Q}]$ , we see that  $N((p)) = N(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r})$ . Hence  $(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$  and  $e_i$  must be the ramification index of  $\mathfrak{P}_i$  for each  $i$ .