Solutions 8

Units, Decomposition Of Prime Ideals

*1. (a) Let M be a bounded subset of a finite dimensional real vector space V. Construct another bounded subset $N \subset V$ such that for any complete lattice $\Gamma \subset V$ with $V = \Gamma + M$, the subset $\Gamma \cap N$ generates Γ.

(b) Deduce that, in principle, for every number field K one can effectively find generators of $\mathcal{O}_K^\times$.

Solution: See for example [Borewicz-Shafarevic: Zahlentheorie (1966) Kapitel II §5.3]. Alternatively, here is an ad hoc solution for (a):

After replacing M by the convex closure of $M + (-M)$ we may assume that M is convex and centrally symmetric. Let $n := \dim_{\mathbb{R}}(V)$. We claim that then $N := \max\{n, 2\}M$ has the desired property.

First let Γ' be the subgroup generated by $\Gamma \cap 2M$. By the assumption $V = \Gamma + M$, for any $\gamma \in \Gamma$ there exist $\delta \in \Gamma$ and $m \in M$ such that $\frac{\gamma}{2} = \delta + m$. Then $2m = \gamma - 2\delta \in \Gamma \cap 2M \subset \Gamma'$; hence $\gamma \in 2\Gamma + \Gamma'$. Since γ was arbitrary, it follows that the composite homomorphism $\Gamma' \hookrightarrow \Gamma \twoheadrightarrow \Gamma/2\Gamma$ is surjective. But Γ is a lattice of rank n, and so Γ' is a sublattice of some rank $n' \leqslant n$. We thus have a surjective homomorphism $\mathbb{Z}^{n'} \cong \Gamma' \twoheadrightarrow \Gamma/2\Gamma \cong (\mathbb{Z}/2\mathbb{Z})^n$, which implies that $n' = n$.

We can therefore choose $\mathbb{R}$-linearly independent elements $\gamma_1, \ldots, \gamma_n \in \Gamma \cap 2M$. With $\Gamma'' := \bigoplus_{i=1}^n \mathbb{Z}\gamma_i$ we then have $V = \bigoplus_{i=1}^n \mathbb{R}\gamma_i = \Gamma'' + \Phi$ for the subset $\Phi := \sum_{i=1}^n [-\frac{1}{2}, \frac{1}{2}]\gamma_i$. Here the fact that $\gamma_i \in 2M$ and the assumption that M is convex and centrally symmetric implies that $[-\frac{1}{2}, \frac{1}{2}]\gamma_i \subset M$. Again by the convexity of M we therefore have $\Phi \subset nM \subset N$, and so $V = \Gamma'' + N$. Finally this implies that $\Gamma = \Gamma'' + (\Gamma \cap N)$. Since Γ'' is already generated by a subset of $\Gamma \cap 2M \subset \Gamma \cap N$, it follows that Γ is generated by $\Gamma \cap N$, as desired.

2. Prove that for any odd prime number p the following are equivalent:

(a) $p \equiv 1 \bmod (4)$.

(b) p splits in $\mathbb{Z}[i]$.

(c) $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Solution: With $K := \mathbb{Q}(i)$ we already know that $\mathcal{O}_K = \mathbb{Z}[i]$. For any odd prime p, by the first supplement to Gauss's quadratic reciprocity law we also know that $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. By Example 6.2.5 of the lecture p is therefore split if $p \equiv 1 \bmod (4)$, and inert if $p \equiv 3 \bmod (4)$. In particular this proves (a)⇔(b).

Next suppose that p splits in $\mathbb{Z}[i]$, that is, that $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ for distinct prime ideals $\mathfrak{p}, \mathfrak{p}' \subset \mathcal{O}_K$. As $\mathcal{O}_K = \mathbb{Z}[i]$ is a principal ideal domain, we then have $\mathfrak{p} = (a + bi)$ for some $a, b \in \mathbb{Z}$. Also, since $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the primes above p, it follows that $\mathfrak{p}' = (a-bi)$. Together this implies that $(p) = (a+bi)(a-bi) = (a^2+b^2)$. Therefore p and a^2+b^2 differ by a factor on $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$. But as both numbers are positive rational, this factor must be 1; hence $p = a^2+b^2$. This shows (b)⇒(c).

Now suppose that $p = a^2+b^2$ for some $a, b \in \mathbb{Z}$. Then we have $p = (a+bi)(a-bi)$. Here $a, b \neq 0$, because p is not a square in $\mathbb{Z}$. In particular neither of $a \pm bi$ is a unit; thus p is not prime in $\mathcal{O}_K$. Being odd, it is also not ramified in $\mathcal{O}_K$. It only remains that p is split in $\mathcal{O}_K$, and then $p = (a+bi)(a-bi)$ is actually its prime factorization in $\mathcal{O}_K$. In particular this proves (c)⇒(b).

*3. Show that the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$ and compute its discriminant.

Solution: This solution is based partly on `https://math.stackexchange.com/a/183093`. Abbreviate $\omega := \sqrt[3]{2}$ and set $K := \mathbb{Q}(\omega)$. Then ω is integral over $\mathbb{Z}$ and therefore $\mathbb{Z}[\omega] \subset \mathcal{O}_K$. Conversely we can write any element $\alpha \in \mathcal{O}_K$ uniquely in the form $\alpha = a_1 + a_2\omega + a_3\omega^2$ with all $a_i \in \mathbb{Q}$ and must prove that all $a_i \in \mathbb{Z}$.

For this observe that α is a zero of the polynomial $f(X) := \prod_{i=1}^3 (X - \sigma_i(\alpha))$ for the three embeddings $\sigma_i \colon K \hookrightarrow \mathbb{C}$. Using the fact that these map ω to ω and $\zeta\omega$ and $\zeta^2\omega$ for $\zeta := e^{2\pi i/3}$, an explicit computation shows that

$$f(X) \;=\; X^3 - 3a_1X^2 + (3a_1^2 - 6a_2a_3)X + (6a_1a_2a_3 - a_1^3 - 2a_2^3 - 4a_3^3).$$

Here $\alpha \in \mathcal{O}_K$ implies that all coefficients lie in $\mathbb{Z}$. In particular we have $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 3a_1 \in \mathbb{Z}$. Similarly we obtain $\mathrm{Tr}_{K/\mathbb{Q}}(\omega\alpha) = 6a_3 \in \mathbb{Z}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\omega^2\alpha) = 6a_2 \in \mathbb{Z}$.

Next we have

$$\begin{aligned} -27 \cdot 4 \cdot \mathrm{Nm}_{K/\mathbb{Q}}(\alpha) \;&=\; 27 \cdot 4 \cdot (6a_1a_2a_3 - a_1^3 - 2a_2^3 - 4a_3^3) \\ &=\; 6 \cdot 3a_1 \cdot 6a_2 \cdot 6a_3 - 4 \cdot (3a_1)^3 - (6a_2)^3 - 2 \cdot (6a_3)^3. \end{aligned}$$

Here the left hand side is an even integer, and by what we have already seen the right hand side is an integer congruent to $(6a_2)^3$ modulo (2). Thus $6a_2$ is even and therefore $3a_2 \in \mathbb{Z}$. This in turn implies that the right hand side is an integer congruent to $2 \cdot (6a_3)^3$ modulo (4). As the left hand side is divisible by 4, it follows that $6a_3$ is even and therefore $3a_3 \in \mathbb{Z}$. Together we thus have $3a_i \in \mathbb{Z}$ for all i.

After adding to α an element of $\mathbb{Z}[\omega]$ we can now assume without loss of generality that $3a_i \in \{-1, 0, 1\}$ for all i. In other words we have $|a_i| \leqslant \frac{1}{3}$, which implies that

$$\big|\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)\big| \;=\; \big|6a_1a_2a_3 - a_1^3 - 2a_2^3 - 4a_3^3\big| \;\leqslant\; \frac{6+1+2+4}{27} \;<\; 1.$$

As the left hand side is an integer, it follows that $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = 0$. But this holds only for $\alpha = 0$. We have therefore shown that $\mathcal{O}_K = \mathbb{Z}[\omega]$.

Finally the discriminant of $\mathcal{O}_K = \mathbb{Z}[\omega]$ is the discriminant of the minimal polynomial X^3-2 of ω over $\mathbb{Q}$. It is therefore equal to

$$\begin{aligned}(\omega-\zeta\omega)^2(\omega-\zeta^2\omega)^2(\zeta\omega-\zeta^2\omega)^2 &= \omega^6(1-\zeta)^2(1-\zeta^2)^2(\zeta-\zeta^2)^2 \\ &= -\omega^6\big[(1-\zeta)(1-\zeta^2)\big]^3\zeta^3 \\ &= -4\cdot 3^3 \;=\; -108.\end{aligned}$$

Remark: In fact 108 is the smallest possible absolute value of the discriminant of a cubic number field.

4. In the number field $K := \mathbb{Q}(\sqrt[3]{2})$, what are the possible decompositions of $p\mathcal{O}_K$ for rational primes p?

Solution: Let p be a rational prime and $p\mathcal{O}_K = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$ its prime factorization in $\mathcal{O}_K$. Then $\sum_{i=1}^r e_i f_i = [K/\mathbb{Q}] = 3$. Hence $1 \leqslant r \leqslant 3$ and the possibilities for $(r; e_1, f_1; e_2, f_2; \dots)$ are, up to permutation of the $\mathfrak{p}_i$:

$$\begin{aligned} r=1: &\quad (1;3,1) \\ &\quad (1;1,3) \\ r=2: &\quad (2;1,1;2,1) \\ &\quad (2;1,1;1,2) \\ r=3: &\quad (3;1,1;1,1;1,1)\end{aligned}$$

To compute the decomposition recall from exercise 3 above that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}] \cong \mathbb{Z}[X]/(X^3-2)$. For any prime p we therefore have $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[X]/(X^3-2)$, and the prime factorization of $p\mathcal{O}_K$ corresponds to the prime factorization of X^3-2 in $\mathbb{F}_p[X]$. For instance

$$\begin{aligned} &\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2[X]/(X^3) && \rightsquigarrow (1;3,1) \\ &\mathcal{O}_K/3\mathcal{O}_K \cong \mathbb{F}_3[X]/(X-2)^3 && \rightsquigarrow (1;3,1) \\ &\mathcal{O}_K/5\mathcal{O}_K \cong \mathbb{F}_5[X]/((X-3)(X^2+3X+4)) && \rightsquigarrow (2;1,1;1,2) \\ &\mathcal{O}_K/7\mathcal{O}_K \cong \mathbb{F}_7[X]/(X^3-2) && \rightsquigarrow (1;1,3) \\ &\mathcal{O}_K/31\mathcal{O}_K \cong \mathbb{F}_{31}[X]/((X-4)(X-7)(X-20)) && \rightsquigarrow (3;1,1;1,1;1,1)\end{aligned}$$

Hence we found all theoretically possible decompositions except $(2;1,1;2,1)$. We claim that this type does not occur:

If the decomposition $(2;1,1;2,1)$ occurs for some prime p, we must have $X^3-2 \equiv (X-a)^2(X-b) \mod p$ for some distinct $a, b \in \mathbb{Z}$. Hence the image of X^3-2 in $\mathbb{F}_p[X]$ is not separable. In this case, we have for the discriminant Δ of X^3-2:

$$0 \equiv \Delta = -\det\begin{pmatrix}1&0&0&-2&0\\0&1&0&0&-2\\3&0&0&0&0\\0&3&0&0&0\\0&0&3&0&0\end{pmatrix} = -108 = -2^2 3^3 \mod p,$$

where the matrix is the Sylvester matrix of X^3-2 and $\frac{d}{dX}(X^3-2)=3X^2$. Hence $p\in\{2,3\}$. But in these cases the decomposition type is $(1;3,1)$, as shown above. In conclusion, the decomposition cannot be of the form $(2;1,1;2,1)$.

5. Consider a Dedekind ring A with quotient field K, a finite separable extension L/K of degree n, and let B be the integral closure of A in L. Assume that $L=K(\alpha)$, where the minimal polynomial $f(X)=X^n+\sum_{i=0}^{n-1}a_iX^i$ of α over K lies in $A[X]$ and is *Eisenstein at* a prime ideal $\mathfrak{p}$ of A, that is, all $a_i\in\mathfrak{p}$ and $a_0\notin\mathfrak{p}^2$. Show that $\mathfrak{p}B=\mathfrak{q}^n$ with $\mathfrak{q}:=\mathfrak{p}B+\alpha B$ prime, so that $\mathfrak{p}$ is totally ramified in B.

   (*Hint:* Prove that $\mathfrak{p}B\subset\mathfrak{q}^j$ for all $1\leqslant j\leqslant n$ by induction on j.)

   Solution: Since $f(\alpha)=0$, the element α is integral over A and hence lies in B. Next consider any prime ideal $\mathfrak{q}'\subset B$ over $\mathfrak{p}$. Then the equation $f(\alpha)=0$ shows that $\alpha^n\in\mathfrak{p}B\subset\mathfrak{q}'$. Thus the residue class of α is a nilpotent element of $B/\mathfrak{q}'$ and therefore zero. It follows that $\alpha\in\mathfrak{q}'$ and hence $\mathfrak{q}:=\mathfrak{p}B+\alpha B\subset\mathfrak{q}'$.

   Next we claim that $\mathfrak{p}B\subset\mathfrak{q}^j$ for all $1\leqslant j\leqslant n$. Since $\mathfrak{p}B\subset\mathfrak{q}$ this is clear for $j=1$. So assume that it holds for some $1\leqslant j<n$. Then we have $\alpha^n\in\mathfrak{q}^n\subset\mathfrak{q}^{j+1}$, and for all $0<i<n$ we have $a_i\alpha^i\in\mathfrak{p}\mathfrak{q}^i\subset\mathfrak{q}^{j+1}$. The equation $f(\alpha)=0$ thus implies that $a_0\in\mathfrak{q}^{j+1}$. But since $a_0\in\mathfrak{p}\smallsetminus\mathfrak{p}^2$, we have $\mathfrak{p}=a_0A+\mathfrak{p}^2$ and hence

$$\mathfrak{p}B=a_0B+\mathfrak{p}^2B\subset\mathfrak{q}^{j+1}+(\mathfrak{q}^j)^2=\mathfrak{q}^{j+1}.$$

   The claim thus follows by induction on j.

   In particular we have $\mathfrak{p}B\subset\mathfrak{q}^n\subset\mathfrak{q}'^n$ and hence $\mathfrak{p}B=\mathfrak{q}'^n\mathfrak{b}$ for some other non-zero ideal $\mathfrak{b}\subset B$. Now write $\mathfrak{p}B=\mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_r^{e_r}$ with distinct prime ideals $\mathfrak{q}_i$, exponents $e_i\geqslant 1$, and residue degrees $f_i\geqslant 1$. From the lecture we know that $\sum_{i=1}^r e_if_i=n$. Looking at the number of prime factors in the factorization $\mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_r^{e_r}=\mathfrak{p}B=\mathfrak{q}'^n\mathfrak{b}$ thus shows that $\sum_i e_i=n$ and that $\mathfrak{b}=(1)$. The factorization therefore reduces to $\mathfrak{p}B=\mathfrak{q}'^n$. The inclusions $\mathfrak{p}B\subset\mathfrak{q}^n\subset\mathfrak{q}'^n=\mathfrak{p}B$ then also imply that $\mathfrak{q}=\mathfrak{q}'$. Thus $\mathfrak{q}$ is the unique prime of B over $\mathfrak{p}$ and $\mathfrak{p}B=\mathfrak{q}^n$.

6. Consider the polynomial ring $A := k[x]$ over a field k of characteristic $p > 0$. Take an element $t \in k^\times$ and let y be a zero of the polynomial

$$f(Y) \ := \ Y^p - x^{p-1}Y - t \ \in \ A[Y]$$

in an algebraic closure of $K := \mathrm{Quot}(A)$.

(a) Show that f is invariant under the substitions $Y \mapsto Y + \alpha x$ for all $\alpha \in \mathbb{F}_p$.

(b) Show that f is separable and irreducible over K.

(c) Show that $L := K(y)/K$ is galois with Galois group isomorphic to $(\mathbb{F}_p, +)$.

*(d) Show that the integral closure B of A in L is equal to

$$\begin{cases} A[z] & \text{for } z := \frac{x}{y-s} \text{ if } t = s^p \text{ for some } s \in k, \\ A[y] & \text{if } t \text{ does not lie in the subfield } k' := \{a^p \mid a \in k\}. \end{cases}$$

(e) Determine the behavior of the prime $\mathfrak{p} := Ax \subset A$ in B.

(f) Discuss the action of $\mathrm{Gal}(L/K)$ on the residue field extension at $\mathfrak{p}$.

Solution:

(a) For any $\alpha \in \mathbb{F}_p$ we have $\alpha^p = \alpha$ and hence

$$f(Y+\alpha x) = (Y+\alpha x)^p - x^{p-1}(Y+\alpha x) - t = Y^p + \alpha x^p - x^{p-1}Y - \alpha x^p - t = f(Y).$$

(b) By (a) the polynomial f has the p distinct roots $y + \alpha x$ for all $\alpha \in \mathbb{F}_p$. Being a polynomial of degree p, it is therefore separable.

Also, the substitutions $Y \mapsto Y + \alpha x$ induce an action of the group $(\mathbb{F}_p, +)$ on the ring $A[Y]$. By (a) this action fixes f, so it permutes the different monic irreducible factors of f. As the action on the roots is already transitive, it is also transitive on the irreducible factors. Since $(\mathbb{F}_p, +)$ is cyclic of prime order, the number of irreducible factors is therefore either 1 or p. In the first case f is irreducible, as desired.

In the second case we must have $y \in K$. Since $y^p - x^{p-1}y - t = 0$, the element y is also integral over $A = k[x]$, and since $k[x]$ is a normal integral domain, we then have $y \in k[x]$. Now the equation $y^p = x^{p-1}y + t$ implies that $p \cdot \deg_x(y) = p - 1 + \deg_x(y)$ and therefore $\deg_x(y) = 1$. Thus we must have $y = ax + b$ for some $a, b \in k$. But

$$f(ax + b) = (ax + b)^p - x^{p-1}(ax + b) - t = (a^p - a)x^p - bx^{p-1} + (b^p - t)$$

can only vanish if b and $b^p - t$ vanish, which is impossible because $t \neq 0$. Thus the second case does not occur.

(c) We have already seen that all roots of f lie in $L := K(y)$ and are transitively permuted by $(\mathbb{F}_p, +)$. Thus L/K is a splitting field of f and hence Galois with Galois group $(\mathbb{F}_p, +)$.

*(d) Suppose first that $t = s^p$ for some $s \in k$. Then $z := \frac{x}{y-s}$ satisfies $y = \frac{x}{z} + s$ and hence

$$0 \;=\; f(\tfrac{x}{z} + s) \;=\; (\tfrac{x}{z} + s)^p - x^{p-1}(\tfrac{x}{z} + s) - s^p \;=\; \tfrac{x^p}{z^p} - \tfrac{x^p}{z} - x^{p-1}s$$

and therefore

$$x - xz^{p-1} - sz^p \;=\; 0. \tag{$*$}$$

As $s \in k^\times$ this shows that z is integral over A and therefore lies in B. Also $s \neq 0$ implies that $1 - z^{p-1} \neq 0$ and hence $x = sz^p/(1 - z^{p-1})$. Since x is transcendental over k, this shows that z is also transcendental over k. We can therefore treat it like a variable over k, so that the subring $A[z] = k[x, z] \subset B$ becomes the subring

$$k\Big[z, \frac{sz^p}{1 - z^{p-1}}\Big] \;\subset\; k(z).$$

This subring contains the element

$$s^{-1} \cdot \frac{sz^p}{1 - z^{p-1}} + z \;=\; \frac{z^p}{1 - z^{p-1}} + z \;=\; \frac{z}{1 - z^{p-1}}$$

and thus also the element

$$z^{p-2} \cdot \frac{z}{1 - z^{p-1}} + 1 \;=\; \frac{z^{p-1}}{1 - z^{p-1}} + 1 \;=\; \frac{1}{1 - z^{p-1}}$$

and is therefore equal to

$$k\Big[z, \frac{1}{1 - z^{p-1}}\Big] \;\subset\; k(z).$$

But this is the localization of the principal ideal domain $k[z]$ obtained by inverting $1 - z^{p-1}$, which is again normal by Proposition 1.4.4. Thus $A[z] = B$, as desired.

Now suppose that t does not lie in the subfield $k' := \{a^p \mid a \in k\}$. Computing the formal derivative $\frac{\mathrm{d}f}{\mathrm{d}Y} = -x^{p-1}$ we find that the discriminant of f is

$$\pm \prod_{\alpha \in \mathbb{F}_p} \tfrac{\mathrm{d}f}{\mathrm{d}Y}(y + \alpha x) \;=\; \pm \prod_{\alpha \in \mathbb{F}_p} x^{p-1} \;=\; \pm x^{p(p-1)}.$$

By Propositions 1.7.4–5 we therefore have $B \subset x^{-p(p-1)}A[y]$. If $B \neq A[y]$, there is therefore an element in $B \cap x^{-1}A[y] \smallsetminus A[y]$. After subtracting an element of $A[y]$ we can write this in the form $x^{-1}g(y)$ for some non-zero polynomial $g(Y) \in k[Y]$ of degree $< p$. As this element is integral over A, its norm must satisfy

$$\mathrm{Nm}_{L/K}(x^{-1}g(y)) \;=\; \prod_{\alpha\in\mathbb{F}_p} x^{-1}g(y+\alpha x) \;\in\; A.$$

Multiplying by x^p then implies that

$$\prod_{\alpha\in\mathbb{F}_p} g(y+\alpha x) \;\in\; x^pA.$$

Since $g(y+\alpha x) \equiv g(y)$ modulo xB, this in turn implies that $g(y)^p \in xB$. Writing out $g(y) = \sum_{i=0}^{p-1} a_iy^i$ with $a_i \in k$ we can now deduce that

$$\sum_{i=0}^{p-1} a_i^py^{pi} \;=\; \Big(\sum_{i=0}^{p-1} a_iy^i\Big)^p \;\in\; xB.$$

But $f(y) = 0$ implies that $y^p \equiv t \bmod xB$; so we obtain that

$$\sum_{i=0}^{p-1} a_i^pt^i \;\in\; xB.$$

Here the left hand side is contained in k, and the right hand side is a proper ideal of B; so we must have $\sum_{i=0}^{p-1} a_i^pt^i = 0$. This means that t is a root of the non-zero polynomial $g'(Y) := \sum_{i=0}^{p-1} a_i^pY^i \in k'[Y]$. As this polynomial has degree $< p$, it follows that t is separable over k'. But $t^p \in k'$ already implies that the minimal polynomial of t over k' is a divisor of $Y^p - t^p \in k'[Y]$ and therefore has only the single root t. Together this shows that the minimal polynomial must be equal to $Y - t$ and therefore $t \in k'$. As this contradicts our assumption, we conclude that $B = A[y]$ in this case.

(e) In the case $t = s^p$ for some $s \in k$ we have

$$B \;=\; A[z] \;\cong\; k[x,Z]/(x - xZ^{p-1} - sZ^p)$$

by (d) and $(*)$. Modulo $\mathfrak{p} = (x)$ we therefore have

$$B/\mathfrak{p}B \;\cong\; k[x,Z]/(x - xZ^{p-1} - sZ^p, x) \;\cong\; k[Z]/(sZ^p).$$

By Proposition 6.2.5 of the lecture it follows that $\mathfrak{p}B = \mathfrak{q}^p$ with the maximal ideal $\mathfrak{q} := (x,z) \subset B$. Thus $\mathfrak{p}$ is totally ramified in B.

Aliter: The polynomial $x - xZ^{p-1} - sZ^p \in A[Z]$ satisfies the Eisenstein criterion for the prime $\mathfrak{p} = (x) \subset A$. Thus $\mathfrak{p}B = \mathfrak{q}^p$ follows from the above exercise 5, without having to determine the precise form of B in (d).

In the case $t \notin k'$ we have $B = A[y] \cong k[x,Y]/(f)$ by (d). Modulo $\mathfrak{p} = xA$ we therefore have

$$B/\mathfrak{p}B \;\cong\; k[x,Y]/(f,x) \;\cong\; k[Y]/(Y^p - t).$$

Here by assumption $Y^p - t$ has no zero in k. Any irreducible factor in $k[Y]$ therefore has degree > 1. As any irreducible polynomial of degree $< p$ over k is separable, it then follows that $Y^p - t$ is already irreducible over k. Thus the factor ring $k[Y]/(Y^p - t)$ is already a field, and so $\mathfrak{q} := B\mathfrak{p}$ is the unique prime ideal of B above $\mathfrak{p}$.

(f) In the first case of (e) the residue field extension is trivial, and in the second case it is purely inseparable of degree p, because the polynomial $Y^p - t$ is inseparable. In both cases we have $\mathrm{Aut}(k(\mathfrak{q})/k(\mathfrak{p})) = 1$, and $\mathrm{Gal}(L/K)$ acts trivially on $k(\mathfrak{q})$.

Remark: In the second case it is still best to define the inertia group $I_\mathfrak{q}$ as the kernel of the homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Aut}(k(\mathfrak{q})/k(\mathfrak{p}))$, although we then have $|I_\mathfrak{q}| = p \neq 1 = e$. In the case of imperfect residue fields the correct definition of an unramified prime $\mathfrak{q}|\mathfrak{p}$ requires that $e_{\mathfrak{q}/\mathfrak{p}} = 1$ *and* that the residue field extension is separable. In that way an unramified extension always remains unramified when one enlarges the base field k to an inseparable extension $k(s)$.