1. Find the necessary and sufficient condition on a prime p such that $\mathbb{Z}[\sqrt{5}] \otimes_{\mathbb{Z}} \mathbb{F}_p$ has a

ⓐ (non-zero) nilpotent element.

ⓑ zero-divisor.

2. Assume A is a commutative finite-dimensional F-algebra. For $a \in A$, let $l_a : A \to A$, $l_a(x) := ax$. Clearly l_a is an F-linear map. The trace of $\underline{\underline{a}}$ over F is defined to be $\mathrm{Tr}_{A/F}(a) := \mathrm{tr}(l_a)$. For an F-basis $\{a_1, \ldots, a_d\}$ of A, let

$$\Delta_{A/F}(a_1, \ldots, a_d) := \det(\mathrm{Tr}_{A/F}(a_i a_j)).$$

ⓐ Prove that if $\Delta(\mathcal{B}) \neq 0$ for a basis $\mathcal{B}$, then $\Delta(\mathcal{B}') \neq 0$ for any other basis $\mathcal{B}'$.

ⓑ Prove that $\mathrm{Nil}(A) := \{a \in A \mid a \text{ is nilpotent}\}$ is an ideal of A, and if $a \in \mathrm{Nil}(A)$, then $a^{\dim_F A + 1} = 0$.

ⓒ Prove that if $\mathrm{Nil}(A) \neq 0$, then $\Delta(\mathcal{B}) = 0$ for any basis $\mathcal{B}$.

(d) Let E be a field extension of F. Prove that, $\Delta_{A/F}(\mathcal{B}) \neq 0$ for some F-basis $\mathcal{B}$ if and only if $\Delta_{A\otimes_F E/E}(\mathcal{B}') \neq 0$ for some E-basis $\mathcal{B}'$ of $A\otimes_F E$.

($p(x)$: monic & $\deg p \geq 1$)

(e) Let $p(x) \in F[x]$, E a splitting field of $p(x)$, and $A = F[x]/\langle p(x) \rangle$. Prove that the following statements are equivalent:

(i) The (symmetric) bilinear form $f: A\times A \to F$

$$f(a_1, a_2) := Tr_{A/F}(a_1 a_2)$$

is non-degenerate, i.e.

$$(\forall x,\ f(a,x) = 0) \Rightarrow a = 0.$$

(ii) $\Delta_{A/F}(\mathcal{B}) \neq 0$ for some F-basis $\mathcal{B}$.

(iii) $A\otimes_F E$ is reduced, i.e. $Nil(A\otimes_F E) = 0$.

(iv) $p(x)$ does not have multiple roots, i.e.

$$\exists\ \alpha_i \neq \alpha_j \in E \text{ if } i \neq j : \quad p(x) = \prod_{i=1}^{n} (x - \alpha_i).$$

(v) $\gcd(p(x), p'(x)) = 1$, where $p'(x)$ is the "derivative" of $p(x)$, i.e. if $p(x) = \sum_{i=0}^{n} a_i x^i$, then $p'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.

[From the proof of part (a), you can see that if $\Delta_{A/F}(\mathcal{B}) \neq 0$ for some F-basis $\mathcal{B}$, then

$$\Delta_{A/F} := \Delta_{A/F}(\mathcal{B})\, F^{\times 2} \in F^{\times}/F^{\times 2}$$

is independent of the choice of $\mathcal{B}$. This is called the discriminant of A over F.]

[If the statements of part (e) hold, we say A is separable over F.]

3. Let $p(x) \in F[x]$ be a monic irreducible polynomial and let $A = F[x]/\langle p(x)\rangle$ $(= F[\alpha]$, where $\alpha = x + \langle p(x)\rangle)$

(a) Prove that A is separable over F iff $p'(x) \neq 0$

(Hint: this is a corollary of 2.e(v).)

(b) Assume A is separable over F and E is a splitting field of $p(x)$ over F. Prove that

$$A \otimes_F E \simeq E \oplus \cdots \oplus E \quad (\deg(p) \text{ copies.})$$

Use this to prove $Tr_{A/F}(\alpha^i) = \alpha_1^i + \cdots + \alpha_d^i$. for any i,

where $p(x) = \prod_{i=1}^{d} (x - \alpha_i)$.

ⓒ Prove that $\Delta_{A/F}(1, \alpha, \ldots, \alpha^{d-1}) = \prod_{i<j} (\alpha_i - \alpha_j)^2$.

(Hint: Use part ⓑ; let

$$X = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_d \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{d-1} & \alpha_2^{d-1} & \cdots & \alpha_d^{d-1} \end{bmatrix},$$

and consider $X \cdot X^T$; Use Vondermond determinant

which says $\det(X) = \prod_{i<j} (\alpha_i - \alpha_j)$.)

ⓓ We know that any $\sigma \in Aut(E/F)$ is uniquely determined by its values at $\alpha_1, \ldots, \alpha_d$ and σ permutes $\alpha_1, \ldots, \alpha_d$. This gives us an embedding of $Aut(E/F)$ into S_d (group of permutations of $\alpha_1, \ldots, \alpha_d$). Prove that the following statements are equivalent if $char(F) \neq 2$:

ⓘ The discriminant $\Delta_{A/F}$ of A over F

is trivial (in $F^\times / F^{\times 2}$).

(ii) $\prod_{i<j} (\alpha_i - \alpha_j) \in F$.

(iii) $\mathrm{Aut}(E/F) \hookrightarrow A_d$ via the above embedding where A_d is the subgroup of the even permutations.

[In parts (c) and (d), the assumptions of part (b) hold.]

Remark. Let $p_1(x), p_2(x) \in F[x]$ be two irreducible polynomials of degree d. Let E be a splitting field of $p_1(x) \cdot p_2(x)$ and let $\alpha_1, \alpha_2 \in E$ such that $p_1(\alpha_1) = p_2(\alpha_2) = 0$. Then if $\alpha_2 \in F[\alpha_1]$, then $A := F[\alpha_1] = F[\alpha_2]$ and

$$\Delta_{A/F}(1, \alpha_1, \ldots, \alpha_1^{d-1})\, F^{\times 2} = \Delta_{A/F}(1, \alpha_2, \ldots, \alpha_2^{d-1})\, F^{\times 2}.$$

This is a useful trick to show $p_2(x)$ has no solution in $F[\alpha_1]$.

4. (a) Assume $ax^2 + bx + c \in F[x]$ has no root in F, $a \neq 0$ & $\mathrm{char}(F) \neq 2$. Let E be its splitting field.

Prove that $\Delta_{E/F} = (b^2-4ac)\,F^{\times 2}$.

[Hint: 3 part ⓒ.]

ⓑ Assume $\mathrm{char}(F) \neq 2$, $D_1, D_2 \in F^\times$. Prove that

$$\{F^{\times 2}, D_1F^{\times 2}, D_2F^{\times 2}, D_1D_2F^{\times 2}\} \subseteq F^\times/F^{\times 2}$$

is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ iff

$[F[\sqrt{D_1}, \sqrt{D_2}] : F] = 4$ iff

$[F[\sqrt{D_1} + \sqrt{D_2}] : F] = 4$.

5. Let $a \in \mathbb{F}_p^\times$. Then by Fermat's (little) theorem, it is clear that $x^p - x + a$ has no root in $\mathbb{F}_p$. Let E be its splitting field over $\mathbb{F}_p$.

ⓐ Prove that if $\alpha \in E$ is a root of $x^p - x + a$, then $E = \mathbb{F}_p[\alpha]$. (Hint: Show that if β is a root, so is $\beta + 1$.)

ⓑ Prove that $x^p - x + a$ is irreducible over $\mathbb{F}_p$. (In particular, $[E : \mathbb{F}_p] = p$.)

6. Let L be an extension of K_1 and K_2. Assume L is generated by K_1 and K_2, i.e. L is the composite of K_1 and K_2. Let $F = K_1 \cap K_2$. Prove that $K_1 \otimes_F K_2$ is a field iff $[L:F] = [K_1:F][K_2:F]$.

7. Prove that if $[F[\alpha]:F]$ is odd, then $F[\alpha] = F[\alpha^2]$.