# 15. Cubic extensions

## 15.1 Binary cubic forms

Let $R$ be an int. dom. with field of fractions $K$.

$V(R) :=$ set of binary cubic forms

$$f(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3 \quad (a,b,c,d \in R)$$

Let $GL_2(R)$ act on $V(R)$ by

$$(Mf)(v) = \det(M)^{-1} \cdot f(M^T v) \text{ for } M \in GL_2(R),\ f \in V(R),\ v \in R^2.$$

**Lemma 15.1.1**

The discriminant

$$\mathrm{disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$
$$= \mathrm{disc}(f(X,1)) \quad \text{if } a \neq 0$$
$$= \mathrm{disc}(f(1,X)) \quad \text{if } d \neq 0.$$

**Rmk** $\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} f = \lambda \cdot f$

**Lemma 15.1.2**

a) $\mathrm{disc}(Mf) = \det(M)^2 \cdot \mathrm{disc}(f)$

b) The linear map $\varphi_M : V(K) \to V(K)$, $f \mapsto Mf$ has determinant $\det(\varphi_M) = \det(M)^2$.

c) Let $\eta_f : GL_2(K) \to V(K)$, $M \mapsto Mf$. $\rightsquigarrow$ $\mathrm{Jac}(\eta_f)(M) : T_M GL_2(K) \to V(K)$

$$T_M GL_2(K) = M_{2\times 2}(K) = K^4, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftrightarrow (a,b,c,d)$$

$$V(K) = K^4$$

$$|\mathrm{Jac}(\eta_f)(M)| = |\pm\mathrm{disc}(f)|.$$

## 15.2. Cubic extensions

Let R be [illegible] a principal ideal domain.

**Def** A ~~[illegible]~~ degree n ext. of R is an R-algebra S which is isomorphic to $R^n$ as an R-module.

**Ex** [illegible] $S = \underbrace{R\times\dots\times R}_{n}$

**Ex** $R=\mathbb{Z}$, $S =$ ring of integers of [illegible] number field of degree n.

**Lemma 15.2.1** For any [illegible] degree n ext. of R, ~~has an R-basis of the form $(1,\omega_1,\dots,\omega_{n-1})$.~~ we have $S/R \cong R^{n-1}$ as R-modules.

**Pf**

$$\begin{tikzcd}
R \arrow[r, hook] \arrow[d, hook] & S \arrow[d, hook] \\
K \arrow[r, hook] & S \otimes_R K
\end{tikzcd}$$

S is an integral [illegible] extension of R.

R is a UFD, hence integrally closed in K.

$\Rightarrow S \cap K = R$

$\Rightarrow$ The R-module $S/R$ is torsion-free.

$\Rightarrow S/R \cong R^{n-1}$

~~$\Rightarrow$ There is a basis of the form $(1,\omega_1,\dots,\omega_{n-1})$~~ □

We now consider the case $n=3$ (cubic extensions).

**Lemma 15.2.2**

Let $(\theta_1, \theta_2)$ be a basis of $S/R$.
There is a unique basis $(1, \omega_1, \omega_2)$ of $S$
with $\omega_i \equiv \theta_i \mod R$ for $i=1,2$.
and $\omega_1 \omega_2 \in R$.

**Pf** Take any $\omega_i' \in S$ with $\omega_i' \equiv \theta_i \mod R$. $\Rightarrow (1, \omega_1', \omega_2')$ is an $R$-basis of $S$.

Write $\omega_1' \omega_2' = n \cdot 1 + p \cdot \omega_1' + q \cdot \omega_2'$ with $n, p, q \in R$.

Write $\omega_i := \omega_i' + \delta_i$ with $\delta_1, \delta_2 \in R$.

Then, $\omega_1 \omega_2 = (n + \delta_1 \delta_2) \cdot 1 + (p + \delta_2) \cdot \omega_1' + (q + \delta_1) \cdot \omega_2'$
lies in $R$ if and only if $p + \delta_2 = 0$ and $q + \delta_1 = 0$. □

## Lemma 15.2.3

Define a commutative $R$-bilinear mult. operation on a free $R$-module $S := \langle 1, \omega_1, \omega_2 \rangle_R$ as follows, with $a, b, c, d, n,$ [redacted] $m, l \in R$:

$$\omega_1 \omega_2 = n$$

$$\omega_1^2 = m - b\omega_1 + a\omega_2$$

$$\omega_2^2 = l - d\omega_1 + c\omega_2$$

$$(1 \cdot 1 = 1, \quad 1 \cdot \omega_1 = \omega_1, \quad 1 \cdot \omega_2 = \omega_2)$$

This mult. op. is associative if and only if

$$n = -ad, \quad m = -ac, \quad l = -bd.$$

Pf associative

$$\Leftrightarrow \omega_1 \cdot (\omega_2^2) = (\omega_1 \omega_2) \cdot \omega_2 \quad \text{and} \quad (\omega_1^2) \cdot \omega_2 = \omega_1 \cdot (\omega_1 \omega_2)$$

$$\underbrace{\omega_1 \cdot (\omega_2^2)}_{\parallel} \qquad \underbrace{(\omega_1\omega_2)\cdot\omega_2}_{\parallel}$$

$$l\omega_1 - d(m - b\omega_1 + a\omega_2) + cn \qquad n\omega_2$$

$$\Updownarrow \qquad\qquad\qquad \Updownarrow$$

$$- - -$$

$$-dm + cn = 0 \text{ and } [\text{redacted}] \text{ and } [\text{redacted}]$$

$$l = -bd \qquad\qquad n = -ad$$

$\square$

Consider the set of pairs $(S,(\theta_1,\theta_2))$ as above, with equivalence rel.

$(S,(\theta_1,\theta_2)) \sim (S',(\theta_1',\theta_2'))$ if there is an R-alg. isom. $S\to S'$

sending $\theta_i$ to $\theta_i'$.

## Cor 15.2.4

We [redacted] have a bijection

$$\{(S,(\theta_1,\theta_2))\}/\sim \;\longleftrightarrow\; V(R)$$

$$(S,(\theta_1,\theta_2)) \longmapsto aX^3+bX^2Y+cXY^2+dY^3 = f(X,Y)$$

with, $a,b,c,d\in R$ [redacted] as in Lemma 15.2.3, $\omega_i\equiv\theta_i \bmod R$.

## Lemma 15.2.5

Let [redacted] $(S,(\theta_1,\theta_2))$, f as above.

We have a map

$$S/R \longrightarrow \Lambda^2(S/R)$$

$$[\alpha] \longmapsto \underbrace{[\alpha]\wedge[\alpha^2]}$$

indep. of repr. $\alpha$ mod R:

$$\begin{aligned}&[\alpha+r]\wedge[(\alpha+r)^2]\\ &=[\alpha+r]\wedge[\alpha^2+2\alpha r+r^2]\\ &=[\alpha]\wedge[\alpha^2+2\alpha r]\\ &=[\alpha]\wedge[\alpha^2]\end{aligned}$$

and an isomorphism $\overset{\cong\,\Lambda^2R^2}{\Lambda^2(S/R)} \longrightarrow R$.

$$\theta_1\wedge\theta_2 \longmapsto 1$$

Let [redacted] $\varphi: S/R \to R$ be the composition.

Then, $f(X,Y)=\varphi([X\theta_1+Y\theta_2])$.

**Pf** $\alpha := X\omega_1 + Y\omega_2$

$\alpha^2 \equiv -(bX^2+dY^2)\omega_1 + (aX^2+cY^2)\omega_2$ mod R by the formula in Lemma 15.2.3.

$\Rightarrow [\alpha] \wedge [\alpha^2] \underset{\cdot}{=} f(X,Y)\cdot(\theta_1 \wedge \theta_2).$ □

### Cor 15.2.6

The bijection is $GL_2(R)$-equivariant.

**Pf** $(Mf)(v) = \dfrac{f(M^T v)}{\det(M)}$ $\leftarrow$ "from the map $S/R \to \Lambda^2(S/R)$" $\leftarrow$ "from the map $\Lambda^2(S/R) \to R$" □

### Thm 15.2.7

a) We have a bijection

$$\{\text{cubic ext.}^s \text{ of } R\}/\cong \;\longleftrightarrow\; GL_2(R)\backslash V(R)$$

b) If S corr. to f, then

$$\mathrm{Aut}(S) \cong \mathrm{Stab}_{GL_2(R)}(f).$$

c) $\mathrm{disc}(S) = \mathrm{disc}(f)$

**Pf** This follows because $GL_2(R)$ acts transitively on the set of bases $(\theta_1, \theta_2)$ of $S/R$.

c) is a computation. □

## Lemma 15.2.8

Let $\underset{ax^3+\dots}{\underset{\shortparallel}{f}} \in V(R)$. If $a \in R^\times$, then the corr. $(S,(\theta_1,\theta_2))$ is

given by $S = R[X]/(f(X,1))$

$$\omega_1 = aX$$
$$\omega_2 = aX^2+bX+c$$
$$(\theta_i \equiv \omega_i \bmod R).$$

Pf computation $\square$

Another example:

$-X^2Y+XY^2$ corr. to $S = R\times R\times R$
$\omega_1=(1,0,0)$
$\omega_2=(0,1,0)$

## Rmk 15.2.9

For any $f \in V(R)$, the corr. $S$ is the ring of global sections of the scheme $V_{\mathbb{P}^1_R}(f)$ (= the vanishing locus of the hom. pol. $f$ on $\mathbb{P}^1_R$).

## Lemma 15.2.10

$S$ is an integral domain if and only if $f \in \mathbf{K}[X,Y]$ is irreducible.

Pf $S$ int. dom.

$\Longleftrightarrow L := S \otimes_R K$ int. dom.

~~Hence, we can assume $R = K$.~~

If $a \neq 0$, then $L \cong K[X]/(f(X,1))$ ~~then int. dom~~ int. dom.

$\Longleftrightarrow f(X,1) \in K[X]$ irred.

$\Longleftrightarrow f(X,Y) \in K[X,Y]$ irred.

If $a = 0$, then $\omega_1 \omega_2 = 0$, so $L$ is not an int. dom.

and $f(X,Y) = (bX^2 + cXY + dY^2) \cdot Y$ is not irred.

$\square$

## 15.3. Three points in $\mathbb{P}^1$

We have a bijection

$$\bar{K}^\times \backslash \{f \in V(\bar{K}) \mid \operatorname{disc}(f) \neq 0\} \longleftrightarrow \{ A \subseteq \mathbb{P}^1(\bar{K}) \mid \# A = 3 \}$$

$$[f] \longmapsto \text{roots of } f \text{ in } \mathbb{P}^1(\bar{K})$$

$$\left[ \prod_{i=1}^{3} (b_i X - a_i Y) \right] \longmapsfrom \{[a_1 : b_1], \dots, [a_3, b_3]\}$$