5. Let P be the field of complex numbers, Φ the subfield of rationals. Show that tr. d. $P/\Phi = c = |P|$. Show that, if B is a transcendency basis of P/Φ, then any 1–1 surjective mapping of B can be extended to an automorphism of P/Φ. Hence show that P has as many automorphisms as 1–1 surjective mappings.

6. Prove that, if P is finitely generated over Φ, then this holds for any subfield E/Φ.

4. Lüroth's theorem. The purely transcendental extensions $P = \Phi(\xi_1, \xi_2, \cdots, \xi_r)$ appear to be the simplest types of extension fields. Nevertheless, it is easy to ask difficult questions about such extensions, particularly about subfields of P/Φ if $r > 1$. If $r = 1$ the situation is comparatively simple and we shall look at this in this section.

Let $P = \Phi(\xi)$, ξ transcendental, and let η be an element of P which is not contained in Φ. We can write $\eta = f(\xi)g(\xi)^{-1}$ where $f(\xi)$ and $g(\xi)$ are polynomials in ξ which we may assume have no common factor of positive degree in ξ. We may write $f(\xi) = \alpha_0 + \alpha_1\xi + \cdots + \alpha_n\xi^n$, $g(\xi) = \beta_0 + \beta_1\xi + \cdots + \beta_n\xi^n$ where either $\alpha_n \neq 0$ or $\beta_n \neq 0$, so n is the larger of the degrees of f and g. The relation $\eta = f(\xi)g(\xi)^{-1}$ gives $f(\xi) - \eta g(\xi) = 0$ and

$$0 = (\alpha_n - \eta\beta_n)\xi^n + (\alpha_{n-1} - \eta\beta_{n-1})\xi^{n-1} + \cdots + (\alpha_0 - \eta\beta_0).$$

Moreover, $\alpha_n - \eta\beta_n \neq 0$ since α_n or $\beta_n \neq 0$ and $\eta \notin \Phi$. Thus we see that ξ is a root of the equation of degree n: $\sum_0^n (\alpha_i - \eta\beta_i)x^i = 0$ with coefficients in $\Phi(\eta)$. We proceed to show that $\sum_0^n (\alpha_i - \eta\beta_i)x^i$ is irreducible in $\Phi(\eta)[x]$. First, it is clear that η is transcendental over Φ, since ξ is algebraic over $\Phi(\eta)$; hence η algebraic over Φ implies ξ algebraic over Φ, contrary to assumption. The ring $\Phi[\eta, x] = \Phi[\eta][x]$ is the polynomial ring in two indeterminates η, x and we know that this ring is Gaussian, that is, the theorem on unique factorization into irreducible elements holds in $\Phi[\eta, x]$ (Vol. I, p. 126). We recall also that a polynomial in $\Phi[\eta, x]$ of positive degree in x is irreducible in $\Phi(\eta)[x]$ if it is irreducible in $\Phi[\eta, x]$ Now $f(\eta, x) = \Sigma(\alpha_i - \eta\beta_i)x^i = f(x) - \eta g(x)$ is of degree 1 in η. Hence if $f(\eta, x)$ is reducible in $\Phi(\eta)[x]$, then it has a factor $h(x)$ of positive degree in x. This implies that $f(x)$ and $g(x)$ are divisible by $h(x)$ contrary to assumption. We have therefore shown that

$f(\eta, x)$ is irreducible in $\Phi(\eta)[x]$. Thus ξ is algebraic of degree n over $\Phi(\eta)$. This proves

Theorem 7. *Let* $\mathrm{P} = \Phi(\xi)$, ξ *transcendental over* Φ *and let* η *be an element of* P *not in* Φ. *Write* $\eta = f(\xi)g(\xi)^{-1}$ *where* $f(\xi)$ *and* $g(\xi)$ *are polynomials in* ξ *with no common factor of positive degree in* ξ. *Let* $n = \max(\deg f, \deg g)$. *Then* ξ *is algebraic over* $\Phi(\eta)$ *and* $[\Phi(\xi):\Phi(\eta)] = n$. *Moreover,* $f(x, \eta) = f(x) - \eta g(x)$ *is irreducible in* $\Phi(\eta)[x]$.

This result enables us to determine the automorphisms of $\Phi(\xi)$ over Φ. Such an automorphism is completely specified by the image η of the generator ξ. For, if $\xi \to \eta$, then $u(\xi)v(\xi)^{-1} \to u(\eta)v(\eta)^{-1}$ for u, v polynomials in ξ. It is clear also that, if η is the image of ξ under an automorphism, then $\Phi(\eta) = \Phi(\xi)$. If $\eta = f(\xi)g(\xi)^{-1}$ as above, then $[\Phi(\xi):\Phi(\eta)] = n = \max(\deg f, \deg g)$. This shows that $\Phi(\eta) = \Phi(\xi)$ if and only if $\max(\deg f, \deg g) = 1$. Then we have

$$\eta = \frac{\alpha\xi + \beta}{\gamma\xi + \delta}, \tag{2}$$

where $\alpha \neq 0$ or $\gamma \neq 0$ and $\alpha\xi + \beta$, $\gamma\xi + \delta$ have no common factor of positive degree. It is easy to see that these conditions are equivalent to the single condition:

$$\alpha\delta - \beta\gamma \neq 0. \tag{3}$$

If this condition holds, then $\Phi(\eta) = \Phi(\xi)$ and the mapping $u(\xi)v(\xi)^{-1} \to u(\eta)v(\eta)^{-1}$ is an automorphism of P/Φ.

The condition (3) is equivalent to the requirement that the matrix

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \tag{4}$$

is non-singular. With each such matrix we associate the automorphism of $\Phi(\xi)$ over Φ such that $\xi \to \eta$ given by (2). One verifies directly that the mapping of the non-singular matrix into the corresponding automorphism is a group homomorphism. The kernel is the set of matrices $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ such that $(\alpha\xi + \beta)(\gamma\xi + \delta)^{-1} = \xi$ or $\alpha\xi + \beta = \xi(\gamma\xi + \delta)$. This implies $\gamma = 0$, $\beta = 0$, $\alpha = \delta$.

Hence the kernel is the set of scalar matrices $\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} \neq 0$. It is now clear that the group of automorphisms of $\Phi(\xi)$ is isomorphic to the factor group of the group $L(\Phi, 2)$ of 2×2 non-singular matrices relative to the subgroup of scalar matrices. This factor group is called the *projective group* $PL(\Phi, 2)$.

We now consider an arbitrary subfield E of $\Phi(\xi)/\Phi$. We may assume $E \neq \Phi$. Then E contains an element η not in Φ so $P = \Phi(\xi)$ is algebraic over $\Phi(\eta)$ and hence is algebraic over $E \supseteq \Phi(\eta)$. Let the minimum polynomial of ξ over E be $f(x) = x^n + \gamma_1 x^{n-1} + \cdots + \gamma_n$. The γ_i have the form $\mu_i(\xi)\nu_i(\xi)^{-1}$ where μ_i, ν_i are polynomials in the transcendental element ξ. Multiplication of $f(x)$ by a suitable polynomial in ξ will give a polynomial

$$f(\xi, x) = c_0(\xi)x^n + c_1(\xi)x^{n-1} + \cdots + c_n(\xi) \tag{5}$$

in $\Phi[\xi, x]$, ξ, x indeterminates, which is a primitive polynomial in x in the sense that the highest common factor of the $c_i(\xi)$ is 1. Also we have $\gamma_i = c_i(\xi)c_0(\xi)^{-1} \in E$ and not all of these are in Φ since ξ is transcendental over Φ. Thus one of the γ's has the form $\gamma = g(\xi)h(\xi)^{-1}$ where $g(\xi)$, $h(\xi)$ have no common factor of positive degree in ξ and $\max(\deg g, \deg h) = m > 0$. We have seen before that $g(x) - \gamma h(x)$ is irreducible in $\Phi(\gamma)[x]$ and $[P:\Phi(\gamma)] = m$. Since $E \supseteq \Phi(\gamma)$ and $[P:E] = n$, clearly $m \geq n$. We shall show that $m = n$ and this will prove that $E = \Phi(\gamma)$.

Since ξ is a root of $g(x) - \gamma h(x) = 0$ and the coefficients of this polynomial are contained in E, we have $g(x) - \gamma h(x) = f(x)q(x)$ in $E[x]$. We have $\gamma = g(\xi)h(\xi)^{-1}$ and we can replace the coefficients of f and q by their rational expressions in ξ and then multiply by a suitable polynomial in ξ to obtain a relation in $\Phi[\xi, x]$ of the form

$$k(\xi)[g(x)h(\xi) - g(\xi)h(x)] = f(\xi, x)q(\xi, x), \tag{6}$$

where $f(\xi, x)$ is the primitive polynomial given in (5). It now follows that $k(\xi)$ is a factor of $q(\xi, x)$ and so cancelling this we may assume the relation is

$$g(x)h(\xi) - g(\xi)h(x) = f(\xi, x)q(\xi, x). \tag{7}$$

Now the degree in ξ of the left-hand side is at most m. Since

$\gamma = g(\xi)h(\xi)^{-1}$ with $(g(\xi), h(\xi)) = 1$ and $\max(\deg g, \deg h) = m$, the ξ-degree of $f(\xi, x)$ is at least m. It follows that it is exactly m and $q(\xi, x) = q(x) \in \Phi[x]$. Then the right hand side of (7) is primitive as a polynomial in x. This holds also for the left hand side. By symmetry, the left hand side is primitive as a polynomial in ξ also, and this implies that $q(x) = q$ is a non-zero element of Φ. Then (7) implies that the x-degree and ξ-degree of $f(\xi, x)$ are the same. Thus $m = n$ and $\mathrm{E} = \Phi(\gamma)$. As we saw before, $\mathrm{E} \supset \Phi$ implies that γ is transcendental. We have proved the following

Theorem 8 (Lüroth). *If* $\mathrm{P} = \Phi(\xi)$, ξ *transcendental over* Φ, *then any subfield* $\mathrm{E} \supset \Phi$ *is also a simple transcendental extension:* $\mathrm{E} = \Phi(\gamma)$, γ *transcendental.*

The theorem of Lüroth is not valid for purely transcendental extensions P/Φ of transcendency degree $r > 1$. The best positive result in this direction is a theorem of Castelnuovo-Zariski which states that, if Φ is algebraically closed and $r = 2$, then a subfield E/Φ of tr. d. 2 such that P/E is separable is a purely transcendental extension.*

EXERCISES

1. Show that, if $\mathrm{P} = \Phi(\xi, \eta)$ where ξ is transcendental and $\eta^2 + \xi^2 = 1$, then P is purely transcendental.

2. Let Φ be a finite field, $|\Phi| = q = p^m$. Determine the order of the Galois group of $\Phi(\xi)/\Phi$, ξ transcendental.

3. Give an example of a subalgebra of $\Phi[\xi]$, ξ transcendental, which does not have a single generator.

5. Linear disjointness and separating transcendency bases. Let Φ be of characteristic $p \neq 0$ and let $\mathrm{P} = \Phi(\xi, \eta)$ where ξ is transcendental and $\eta^p = \xi$. Then $\{\xi\}$ is a transcendency basis for P/Φ and P is inseparable over $\Phi(\xi)$. On the other hand, $\mathrm{P} = \Phi(\eta)$ is separable over P. This simple example shows that certain transcendency bases B for an extension may be preferable to others in that $\mathrm{P}/\Phi(B)$ is separable algebraic. We remark also that such bases may not always exist, as is shown by the example

* See O. Zariski, *On Castelnuovo's criterion of rationality* $p_a = P_2 = 0$, *Illinois Jour. of Math.*, Vol. 2 (1958), pp. 303–315.