Graded

1. (14.6.15) Prove the polynomial $x^4+px+p \in \mathbb{Q}[x]$ is irreducible for every prime p and for $p \neq 3,5$ has Galois group S_4. Prove the Galois group for $p=3$ is dihedral of order 8 and for $p=5$ is cyclic of order 4.

   Proof. Let p be an arbitrary prime integer. The polynomial $f(x)=x^4+px+p \in \mathbb{Q}[x]$ is Eisenstein at the prime p, so it is irreducible.

   The resolvent cubic for $f(x)$ is $h(x)=x^3-4px+p^2$, which is irreducible if and only if it has a rational root. By the rational root theorem, the only candidates are $\pm p$ and $\pm p^2$. But $\pm p^6 \mp 4p^3+p^2 = p^2(\pm p^4 \mp 4p+1) \neq 0$ since $\pm 2^4 \mp 4(2)+1 \neq 0$ and $\pm z^4 \mp 4z+1$ is monotonic as a function on $\mathbb{R}_{\geq 2}$ (its derivative is $\pm 4z^3 \mp 4$ which has fixed sign for $z \geq 2$), so $\pm p^2$ could not be a root.

   On the other hand, $\pm p^3 \mp 4p^2 + p^2 = p^2(\pm p \mp 4+1)$ may be zero for some choices of p depending on the signs above. Observe that $p^2(p-3)$ is zero if and only if $p=3$ and $p^2(-p+5)$ is zero if and only if $p=5$. So for $p \neq 3,5$ the resolvent cubic $h(x)$ is irreducible.

   In this case ($p \neq 3,5$) we compute the discriminant D of the irreducible resolvent cubic $h(x)$, which (following the information on pages 613-615 of Dummit and Foote) is the same as the discriminant of the quartic $f(x)$. We have $D=-27p^4+256p^3$ (due to the formula on page 614). We have with $p>0$ that $\sqrt{p^3(256-27p)} = p\sqrt{p(256-27p)} \in \mathbb{Q}$ if and only if $p(256-27p)$ is the square of a rational. Observe that $x(256-27x)$ is a bounded above quadratic as a real valued function which is nonnegative in the interval $[0,256/27]$, and note $256/27 = 9+13/27$. So we only need to check that $r(p)=p(256-27p)$ is the square of a rational for primes $2,3,5,7$. We have $r(2)=404, r(3)=525, r(5)=605$, and $r(7)=469$, and none of these are perfect squares. Hence for $p \neq 3,5$, since the resolvent cubic $h(x)$ is irreducible and its discriminant D is not a square of a rational, the Galois group of $f(x)$ is S_4 (following the argument on page 615, part **a.**)

   We consider the case when $p=3$: the resolvent cubic is $h(x)=x^3-12x+9=(x-3)(x^2+3x-3)$, and see that x^2+3x-3 is irreducible since its discriminant $3^2-4(-3)=21$ is not a square in $\mathbb{Q}$ (it is prime). In this case we have that the Galois group will fix the root 3, so the Galois group of $f(x)$ is either the dihedral group or the cyclic group of order 4. We compute the discriminant of $h(x)$ (or $f(x)$) to be $D=-27(3^4)+256(3^3)=4725$, and we have $\sqrt{D}=\sqrt{4725}=15\sqrt{21}$. Following the argument on page 615, part **c2.**, we show that $f(x)=x^4+3x+3$ is irreducible over $\mathbb{Q}(\sqrt{D})=\mathbb{Q}(\sqrt{21}) \subset \mathbb{R}$ so that the Galois group must be the dihedral group. By using a computer program (so citing the email with the program output), we find that $f(x)$ is not factorizable over $\mathbb{Q}(\sqrt{21})$, so the Galois group of $f(x)$ is indeed the dihedral group of order 8.

   In the case when $p=5$, the resolvent cubic is $h(x)=x^3-20x+25=(x+5)(x^2-5x+5)$ and see that x^2-5x+5 is irreducible since its discriminant is $25-20=5$, which is not a square in $\mathbb{Q}$ (it is prime). Like before, the Galois group of $f(x)=x^4+5x+5$ is either the dihedral group of order 8 or the cyclic group of order 4. To that end, we show that $f(x)$ is not irreducible over $\mathbb{Q}(\sqrt{D})=\mathbb{Q}(\sqrt{15125})=\mathbb{Q}(\sqrt{5})$ where $D=-27(5^4)+256(5^3)=15125$ is the discriminant of $h(x)$ (or $f(x)$). We have that $f(x)=[x^2+\sqrt{5}x-$

$\sqrt{5}/2+5/2][x^2-\sqrt{5}x+\sqrt{5}/2+5/2] \in \mathbb{Q}(\sqrt{5})[x]$, so the Galois group of $f(x)$ is the cyclic group of order 4 as desired. □

2. (Universal Properties) Let F be a field and $f(x) \in F[x]$ an irreducible polynomial. Informally, a map $F[x]/(f(x))$ to a field L containing F that is the identity on F is equivalent to specifying a root of $f(x)$ in L to be the image of x.

   (i) Make this precise by formulating a universal property for $F[x]/(f(x))$. (For example, in the category of field extensions of F, although you don't even need to phrase it in terms of category theory.)

   Given an irreducible polynomial $f(x) \in F[x]$, a homomorphism $\varphi\colon F \to L$, and a root $\ell \in L$ of $f(x) \in L[x]$ (so viewing F as a subfield of L), there exists a unique map $\varphi'\colon F[x]/(f(x))$ such that φ' agrees with φ on the isomorphic image of F in $F[x]/(f(x))$ but sends x to ℓ.

$$\begin{tikzcd}
F \arrow[r, "\varphi"] \arrow[d, hook] & L \\
F[x]/(f(x)) \arrow[ur, dashed, "\varphi'"'] &
\end{tikzcd}$$

   So in particular, if a field K and maps $F \to K$, $K \to L$ exist and cause the solid arrow diagram below to commute, there is a unique map from $F[x]/(f(x))$ to K making the following diagram commute (so $F[x]/(f(x))$ is the smallest such object):

$$\begin{tikzcd}
 & & F \arrow[r, "\varphi"] \arrow[d, hook] \arrow[ddll, bend right, hook] & L \\
 & & F[x]/(f(x)) \arrow[ur, "\varphi'"'] \arrow[dll, dashed] & \\
K \arrow[uurrr, bend right] & & &
\end{tikzcd}$$

   (ii) Prove that any two fields satisfying this universal property are also isomorphic.

   Suppose H and J were fields satisfying the universal property above (so they extend φ by φ_H and φ_J respectively). Then by using the universal property above twice see that there are unique maps h, j making the below diagram commute:

$$\begin{tikzcd}
 & & & F \arrow[r, "\varphi"] \arrow[d, hook] \arrow[dl, bend right, hook] \arrow[ddll, bend right, hook] & L \\
 & & & H \arrow[ur, "\varphi_H"] \arrow[dl, dashed, "h"'] \arrow[dll, bend right, "\mathrm{id}_H"'] & \\
 & & J \arrow[uurr, bend right, "\varphi_J"'] \arrow[dl, dashed, "j"'] \arrow[dll, bend right, "\mathrm{id}_J"'] & & \\
 & H \arrow[uuurrr, bend right, "\varphi_H"'] \arrow[dl, dashed, "h"'] & & & \\
J & & & &
\end{tikzcd}$$

Since the identity maps above commute, it follows by uniqueness of the maps h and j that $hj = \mathrm{id}_J$ and $jh = \mathrm{id}_H$, from which we have that h, j are field isomorphisms (they are left and right invertible). Thus H and J are isomorphic as desired.

Additional Problems

1. (14.6.27) Let $f(x)$ be a monic polynomial of degree n with roots $\alpha_1, \alpha_2, \dots, \alpha_n$.

   (a) Show that the discriminant D of $f(x)$ is the square of the Vandermonde determinant

$$(*) \qquad \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix} = \prod_{i>j}(\alpha_i - \alpha_j).$$

   (b) Taking the Vandermonde matrix above, multiplying on the left by its transpose and taking the determinant show that one obtains

$$D = \begin{vmatrix} p_0 & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{vmatrix}$$

   where $p_i = \alpha_1^i + \cdots + \alpha_n^i$ is the sum of the i^{th} powers of the roots of $f(x)$, which can be computed in terms of the coefficients of $f(x)$ using Newton's formulas above. This gives an efficient procedure for calculating the discriminant of a polynomial.

Proof. In $(*)$, observe that by squaring $\prod_{i>j}(\alpha_i - \alpha_j)$ we obtain $\prod_{i>j}(\alpha_i - \alpha_j)^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2$ since negating the quantity inside the parentheses nets no effect since everything is squared anyways. As α_i are roots of $f(x)$, it follows that the square of the Vandermonde determinant in $(*)$ is the discriminant of $f(x)$.

Observe that

$$\left[\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}^{\mathsf{T}} \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}\right]_{ij} = \sum_{k=1}^{n} \alpha_k^{i+j} = p_{i+j}.$$

Since the determinant is invariant under transposition and is multiplicative, we have that the determinant of the matrix product above is the same as the square of the Vandermonde determinant in $(*)$, given by D.

As a result,

$$D = \begin{vmatrix} p_0 & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{vmatrix}$$

as desired. □

2. (14.7.7) (*Kummer Generators for Cyclic Extensions*) Let F be a field of characteristic not dividing n containing the n^{th} roots of unity and let K be a cyclic extension of degree d dividing n. Then $K = F(\sqrt[n]{a})$ for some nonzero $a \in F$. Let σ be a generator for the cyclic group $\mathrm{Gal}(K/F)$.

   (a) Show that $\sigma(\sqrt[n]{a}) = \zeta\sqrt[n]{a}$ for some primitive d^{th} root of unity ζ.

   (b) Suppose $K = F(\sqrt[n]{a}) = F(\sqrt[n]{b})$. Use (a) to show that $\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \left(\frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}\right)^i$ for some integer i relatively prime to d. Conclude that σ fixes the element $\frac{\sqrt[n]{a}}{(\sqrt[n]{b})^i}$ so this is an element of F.

   (c) Prove that $K = F(\sqrt[n]{a}) = F(\sqrt[n]{b})$ if and only if $a = b^i c_1^n$ and $b = a^j c_2^n$ for some $c_1, c_2 \in F$, i.e., if and only if a and b generate the same subgroup of $F^\times$ modulo n^{th} powers.

Proof. (a) The element σ permutes the roots of the irreducible polynomial $x^n - a$, and has to do so with order d. Hence there is some primitive d-th root of unity ζ (here d needs to divide n) such that $\sigma(\sqrt[n]{a}) = \zeta\sqrt[n]{a}$ (also note $\sigma^d(\sqrt[n]{a}) = \zeta^d\sqrt[n]{a} = \sqrt[n]{a}$ as expected).

(b) For $F(\sqrt[n]{b})$, repeat the same argument as in a to see that $\sigma(\sqrt[n]{b}) = \xi\sqrt[n]{b}$ for some d-th primitive root of unity; note that $\zeta = \xi^i$ for some i relatively prime to d. Hence $\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \zeta = \xi^i = \left(\frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}\right)^i$. It follows since σ is a field homomorphism that $\sigma\left(\frac{\sqrt[n]{a}}{(\sqrt[n]{b})^i}\right) = \frac{\sqrt[n]{a}}{(\sqrt[n]{b})^i}$ (with some algebra the original equality can be massaged to obtain this one), so $\frac{\sqrt[n]{a}}{(\sqrt[n]{b})^i} \in F$. By symmetry (of the above arguments) $\frac{\sqrt[n]{b}}{(\sqrt[n]{a})^j} \in F$ for some j coprime with d.

(c) If $a = b^i c_1^n$ and $b = a^j c_2^n$, then the fields $F(\sqrt[n]{a}), F(\sqrt[n]{b})$ are mutually contained in each other hence equal, so we consider the converse. Suppose that $K = F(\sqrt[n]{a}) = F(\sqrt[n]{b})$. Then since $\frac{\sqrt[n]{a}}{(\sqrt[n]{b})^i} \in F$, let $\frac{\sqrt[n]{a}}{(\sqrt[n]{b})^i} = c_1$ so that $a = b^i c_1^n$ as desired. Similarly, $b = a^j c_2^n$ by repeating the same argument for $\frac{\sqrt[n]{b}}{(\sqrt[n]{a})^j} \in F$. □

Feedback

1. None.

2. Things are okay so far; same as usual I think.