International Journal of Sciences & Applied Research

International Journal of Sciences & Applied Research

www.ijsar.in

Realizability of Small 2-Groups

Dilpreet Kaur*

Symbiosis Institute of Technology, Pune, India.
Correspondence Address: *Dilpreet Kaur, Symbiosis Institute of Technology, Pune, India.

Abstract
A group G is said to be realizable over a field F if there exists a Galois extension K of F such that $Gal(K/F) = G$. In this expository article we study properties of a field F of characteristic different from 2 which guarantee the realizability over F of a given 2-group up to order 8.

Keywords: 2-groups, Field extension, Galois group, Realizability

Introduction

Let F be a field and K be finite extension of F. If K/F is normal and separable extension then it is called the Galois extension. For a Galois extension K/F, the set of F-automorphisms of K forms a group under the composition of automorphisms. This group is called the *Galois group of* K/F and it is denoted by $Gal(K/F)$.

It can be asked whether a given finite group is a Galois group of some extension. Emil Artin ([Lan02], pp. 264) showed that it is always possible to construct a field extension with any finite group as Galois group but in this case ground field is also constructed so the problem refers to the case in which the group G and the ground field F are both given. This is known as Inverse *Galois Problem*.

This problem is extensively studied when ground field is the field of rational numbers $\mathbb{Q}$, it is known as *Classical Inverse Galois Problem*. It was raised by *David Hilbert* in *1892*. This area is still very much open for research.

REALIZABILITY OF $\frac{\mathbb{Z}}{2\mathbb{Z}}, \frac{\mathbb{Z}}{4\mathbb{Z}}, \frac{\mathbb{Z}}{8\mathbb{Z}}, D_8$

A group is said to be 2-group if its order is 2^n for $n \in \mathbb{Z}$. Now onwards F denotes the field of characteristic not equal to 2 and F^* denotes multiplicative group of F. Group of integers modulo n, dihedral group of order 8 and quaternion group of order 8 are denoted by $\frac{\mathbb{Z}}{n\mathbb{Z}}$, D_8 and Q_8 respectively. A presentation of D_8 and Q_8 is:

$$D_8 = \langle\, c, d \mid c^4 = 1, d^2 = 1, dcd^{-1} = c^{-1} \rangle$$
$$Q_8 = \langle\, c, d \mid c^4 = 1, c^2 = d^2, dcd^{-1} = c^{-1} \rangle$$

A field F is said to be *quadratically closed* if every element of F is a square in F itself. Equivalently, F is quadratically closed if it does not have any proper quadratic extension.

Proposition 2.1. [5] The group $\frac{\mathbb{Z}}{2\mathbb{Z}}$ is realizable over field F if and only if F is not quadratically closed.

Proof: If $\frac{\mathbb{Z}}{2\mathbb{Z}}$ is realizable over field F then there exists a quadratic extension of F and F is not quadratically closed. Conversely, let $a \in F$ but $\sqrt{a}$ does not belong to F.
Consider $f(x) = x^2 + a$ then $f(x)$ is an irreducible separable polynomial over F and $F(\sqrt{a})$ is the splitting field of $f(x)$. In this case $Gal(F(\sqrt{a})/F) = \frac{\mathbb{Z}}{2\mathbb{Z}}$.
It is generated by ϕ where $\phi(\sqrt{a}) = -\sqrt{a}$.■

In Grundman et al (1995), they discuss the realizability of groups of order 4 and Dihedral group D_8 over fields of characteristic not equal to 2. The details are discussed below:

Proposition 2.2. [2] Let $f(x) = x^4 + ax^2 + b$ where $a \in F$, $b \in F^*$ be an irreducible separable polynomial and G be the Galois group of the splitting field of $f(x)$ over F.
If $\sqrt{b} \in F$ then $G \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$. If $\sqrt{b}$ does not belong to F but $\sqrt{b(a^2-4b)} \in F$ then $G \cong \frac{\mathbb{Z}}{4\mathbb{Z}}$ and if both $\sqrt{b}, \sqrt{b(a^2-4b)}$ does not belong to F then $G \cong D_8$.

Proof: Using quadratic formula, we have

$$x^2 = \frac{-a \pm \sqrt{a^2-4b}}{2}$$

If $\sqrt{a^2-4b} \in F$ then $f(x)$ will be reducible over F so $\sqrt{a^2-4b}$ does not belong to F.

Let

$$\alpha = \frac{\sqrt{-a+2\sqrt{b}}}{2} + \frac{\sqrt{-a-2\sqrt{b}}}{2},$$

$$\beta = \frac{\sqrt{-a+2\sqrt{b}}}{2} - \frac{\sqrt{-a-2\sqrt{b}}}{2}$$

Then

$$\alpha^2 = \frac{-a + \sqrt{a^2-4b}}{2}, \qquad \beta^2 = \frac{-a - \sqrt{a^2-4b}}{2}$$

Hence $\alpha, -\alpha, \beta, -\beta$ are roots of $f(x)$ and splitting field of $f(x)$ is $F[\alpha, \beta]$

Case I: If $\sqrt{b} \in F$ then $\beta \in F[\alpha]$ as $\beta = \frac{\sqrt{b}}{\alpha}$.
Now for $\phi \in Gal(K/F)$, $\phi(\beta)$ is determined by $\phi(\alpha)$ so order of $Gal(K/F)$ is 4.
An element of $Gal(K/F)$ maps α to one of $\pm\alpha, \pm\beta$ and order of these elements is at most 2 so

$$Gal(K/F) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

Case II: If $\sqrt{b}$ does not belong to F but $\sqrt{b(a^2-4b)} \in F$ then $\sqrt{b} = \lambda\sqrt{a^2-4b}$ for some $\lambda \in F$ and field $F\left(\sqrt{a^2-4b}\right)$ is contained in $F(\alpha)$ as well as in $F(\beta)$. Hence $F(\alpha) = F(\beta)$ and action of every element of $Gal(K/F)$ to α decides its action on β so order of $Gal(K/F)$ is again 4.
Now suppose that $\phi \in Gal(K/F)$ and $\phi(\alpha) = \beta$ then $\phi(\alpha^2) = \beta^2$. This gives $\phi\left(\sqrt{a^2-4b}\right) = -\sqrt{a^2-4b}$. Now

$$\phi(\beta) = \phi\left(\frac{\lambda\sqrt{a^2-4b}}{\alpha}\right) = \frac{\lambda\phi\left(\sqrt{a^2-4b}\right)}{\phi(\alpha)} = -\alpha$$

Hence ϕ is an element of order 4 and $Gal(K/F) \cong \frac{\mathbb{Z}}{4\mathbb{Z}}$.

Case III: If $\sqrt{b}, \sqrt{b(a^2-4b)}$ does not belong to F then $F[\alpha]$ and $F[\beta]$ are not same and for each choice of $\phi(\alpha)$, there are exactly two choices of $\phi(\beta)$ because ϕ is onto and $\phi(\alpha)$ and $\phi(\beta)$ cannot be integral multiple of each other. Hence

$\phi(\alpha) = \pm\alpha \Rightarrow \phi(\beta) = \pm\beta$
$\phi(\alpha) = \pm\beta \Rightarrow \phi(\beta) = \pm\alpha$
So order of $Gal(K/F)$ is 8.
Consider $\phi_1, \phi_2 \in Gal(K/F)$,
where $\phi_1(\alpha) = \beta, \phi_1(\beta) = -\alpha$
and $\phi_2(\alpha) = \alpha, \phi_1(\beta) = -\beta$. It is easy to check that order of ϕ_1 is 4 and that of ϕ_2 is 2. Also

$$\phi_1\phi_2^3(\alpha) = \phi_1(\alpha) = \beta = \phi_2(-\beta) = \phi_2\phi_1(\alpha)$$
$$\phi_1\phi_2^3(\beta) = -\phi_1(\beta) = -\alpha = \phi_2(-\alpha) = \phi_2\phi_1(\beta)$$

Now mapping ϕ_1 to c and ϕ_2 to d, where c and d are generators of D_8 as given in presentation of D_8 in section 2, we get $Gal(K/F) \cong D_8$.■

From above proposition, it is clear that $\frac{\mathbb{Z}}{4\mathbb{Z}}$ is realizable over field F if it contains an element b which is not a square but is sum of two square elements. A field in which any sum of squares is again a square is called *Pythagorean field*. So above proposition gives that $\frac{\mathbb{Z}}{4\mathbb{Z}}$ cannot be realized over Pythagorean field.

Kuyk and Lenstra (1975) proved that the realizability of group $\frac{\mathbb{Z}}{4\mathbb{Z}}$ gives the realizability of $\frac{\mathbb{Z}}{n\mathbb{Z}}$ for all $n \in \mathbb{Z}, n \geq 2$. In particular it gives the realizability of $\frac{\mathbb{Z}}{8\mathbb{Z}}$.

Moreover Smith (2009) has shown that a field F has Galois extension K with Galois group D_8 if and only if F^*contains element a, b independent of $mod(F^{*2})$ and the equation $ax^2 + by^2 = z^2$ has a nontrivial solution over F.

Remark: The characteristic of F is not equal to 2 is a necessary condition.

Let $\mathbb{F}_2$ be prime field of characteristic 2 then it is quadratically closed as well as a Pythagorean field, but groups $\frac{\mathbb{Z}}{2\mathbb{Z}}$ and $\frac{\mathbb{Z}}{4\mathbb{Z}}$ are realizable over $\mathbb{F}_2$. The Galois group of splitting field of polynomial $h(x) = x^2 + x + 1$ over $\mathbb{F}_2$ is $\frac{\mathbb{Z}}{2\mathbb{Z}}$.
The polynomial $f(x) = x^4 + x + 1$ is irreducible over $\mathbb{F}_2$ and if α is one root of $f(x)$ then $\alpha+1, \alpha^2, \alpha^2+1$ are other roots of $f(x)$. Hence $\mathbb{F}_2(\alpha)$ is splitting field of $f(x)$ and order of $Gal(\mathbb{F}_2(\alpha)/\mathbb{F}_2)$ is 4. Also the element $\phi \in Gal(\mathbb{F}_2(\alpha)/\mathbb{F}_2)$ which maps α to α^2 is of order4. Thus $Gal(\mathbb{F}_2(\alpha)/\mathbb{F}_2) \cong \frac{\mathbb{Z}}{4\mathbb{Z}}$.

REALIZABILITY OF $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}, \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}, \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$

Using Galois Theory (see [4], pp. 268), it is clear that group $G \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ is realizable over field F if and only if there exist a Galois extension K of F such that $Gal(K/F) = G$ and an element $a \in F$ such that $\sqrt{a}$ does not belong to K. Then $Gal(K(\sqrt{a}/F)) = G \times \frac{\mathbb{Z}}{2\mathbb{Z}}$.
Thus groups $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ and $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ are realizable on fields which are not quadratically closed and contains sufficiently large number of square classes. Similarly group $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ is realizable over non-Pythagorean field having sufficient number of square classes.

For example, let $\mathbb{F}_5$ denote the prime field of characteristic 5. Using proposition 2.2, one can check that the Galois groups of splitting fields K_1, K_2 of irreducible polynomials $f_1(x) = x^4 + x^2 + 4$ and $f_2(x) = x^4 + x^2 + 2$ are $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ and $\frac{\mathbb{Z}}{4\mathbb{Z}}$, respectively. But $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ and $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ are not realizable over $\mathbb{F}_5$ since there does not exist $\gamma \in \mathbb{F}_5$ such that $\sqrt{\gamma}$ does not belong to K_1, K_2. But if we consider the polynomial $f(x) = x^4 + 4x^2 + 2$ over field of rationals $\mathbb{Q}$ then Galois group of splitting field K of polynomial $f(x)$ over $\mathbb{Q}$ is $\frac{\mathbb{Z}}{4\mathbb{Z}}$ and there are many rational numbers, for example 3, whose square root does not belong to the field K so the field K has a quadratic extension whose Galois group over $\mathbb{Q}$ is $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$.

REALIZABILITY OF Q_8

Witt (1936) proved if F is a field of characteristic not equal to 2 then an extension $L = F(\sqrt{a}, \sqrt{b})$, where $a, b \in F$, can be embedded in a Galois extension K of F with $Gal(K/F) = Q_8$ if and only if the quadratic form $ax_1^2 + bx_2^2 + abx_3^2$ can be converted to $y_1^2 + y_2^2 + y_3^2$ by a linear change of variables over F. In the following, we study this fact in detail for the fields of rational numbers.

Consider the quadratic form $2x_1^2 + 3x_2^2 + 6x_3^2$ over $\mathbb{Q}$. It can be converted to $y_1^2 + y_2^2 + y_3^2$ by the following change of variables.

$$x_1 = \frac{1}{2}y_2 - \frac{1}{2}y_3$$

$$x_2 = -\frac{5}{9}y_1 - \frac{1}{9}y_2 - \frac{1}{9}y_3$$

$$x_3 = \frac{1}{9}y_1 - \frac{5}{18}y_2 - \frac{5}{18}y_3$$

This gives that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be embedded in a Galois extension of $\mathbb{Q}$, whose Galois group is Q_8 as shown in following example (see [1], pp. 584).

Consider the polynomial $f(x) = x^8 - 24x^6 + 48x^4 - 288x^2 + 144$. It is irreducible over $\mathbb{Q}$ and its roots are $\pm\sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})}$.

Denote

$$\alpha = \sqrt{(2 + \sqrt{2})(3 + \sqrt{3})}$$

$$\beta = \sqrt{(2 - \sqrt{2})(3 + \sqrt{3})}$$

$$\gamma = \sqrt{(2 + \sqrt{2})(3 - \sqrt{3})} \qquad \delta = \sqrt{(2 - \sqrt{2})(3 - \sqrt{3})}$$

then it can be shown that all roots of $f(x)$ lie in $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subsetneq \mathbb{Q}(\alpha)$. Thus order of $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ is 8.

The elements of $Gal\left(\frac{\mathbb{Q}(\alpha)}{\mathbb{Q}}\right)$ are the $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\alpha)$ that map α to any of the eight roots of $f(x)$. Let $\phi_1, \phi_2 \in Gal\left(\frac{\mathbb{Q}(\alpha)}{\mathbb{Q}}\right)$ and $\phi_1(\alpha) = \beta$, $\phi_2(\alpha) = \gamma$. Now we show that ϕ_1 is an element of order 4, $\phi_1(\alpha^2) = \beta^2$, gives that $\phi_1(\sqrt{2}) = -\sqrt{2}$ and $\phi_1(\sqrt{3}) = 3$. Thus $\phi_1(\alpha\beta) = -\alpha\beta$, this implies $\phi_1^2(\alpha) = \phi_1(\beta) = -\alpha$. On similar lines one can show that ϕ_2 is also an element of order 4 and $\phi_2^2(\alpha) = \phi_2(\gamma) = -\alpha$. Hence $\phi_1^2 = \phi_2^2$.

Now

$\phi_2\phi_1^3(\alpha) = -\phi_2\phi_1(\beta) = -\delta = \phi_1(\gamma) = \phi_1\phi_2(\alpha)$

Mapping ϕ_1 to c and ϕ_2 to d, where c and d are generators of Q_8 as given in presentation of Q_8 in section 2, we get \$Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong Q_8$.

References

[1] David S. Dummit and Richard M. Foote, (2004), Abstract algebra, third ed., John Wiley & Sons Inc., Hoboken, NJ.

[2] Helen G. Grundman, Tara L. Smith, and John R. Swallow, (1995), Groups of order 16 as Galois groups, Exposition. Math. 13, 4, 289-319.

[3] W. Kuyk and H. W. Lenstra, Jr., (1975), Abelian extensions of arbitrary fields, Math. Ann. 216 , 2, 99-104.

[4] Serge Lang, (2002), Algebra, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York.

[5] Tara L. Smith, (1994), Galois groups and quadratic forms, Mat. Contemp. 7, 129-179.

[6] E. Witt, (1936), Konstruktion von galoisschen krpen der charakteristik p zu vorgegebener gruppe der ordnung pf, J. Reine Angew.Math. 174, 237-245.