In Theorem 4, the primes covered are of the form $2^n + 1$. Such a prime number is called a **Fermat prime**. Note that if $2^n + 1$ is a prime, then n must be a power of 2 (see E15). It is not known whether there exist only finitely many, or infinitely many, Fermat primes.

Why don't you try some exercises now?

E15) If $2^n + 1$ is a prime, then show that n must be a power of 2. (The converse is not true.)

E16) Prove, or disprove, the following statements:

i) A regular 11-gon is constructible.

ii) A regular 257-gon is constructible.

Now let us look at an example of constructibilty of a regular n-gon for some composite values of n.

Example 7: Check whether or not a regular 9-gon is constructible.

Solution: A 9-gon is constructible if and only if the angle $2\pi/9$ is constructible. This is possible if and only if $e^{2\pi i/9}$ is constructible, which is possible if and only if its square root $e^{\pi i/9}$ is constructible. But that is possible if and only if $\cos(\pi/9)$ is constructible, which is the same as saying an angle of 20° is constructible. But this is not possible, in view of Corollary 4. Therefore, a regular 9-gon is not constructible.

***

There is a more general version of Gauss' theorem, proved by Pierre Wantzel in 1837, which we now state.

Theorem 5 (Gauss-Wantzel theorem): A regular n-gon is constructible by ruler and compass if and only if $\phi(n)$ is a power of 2, where ϕ is the Euler-phi function. ■

You are familiar with ϕ, from Unit 10.

We shall not prove this theorem here. However, note that **$\phi(n)$ is a power of 2 if and only if $n = 2^r p_1 p_2 \ldots p_t$, where the p_i are distinct odd primes such that $p_i - 1$ is a power of 2**.

Using Theorem 5, you can immediately see that a regular 9-gon is not constructible. What about a 20-gon? By Theorem 5, it is constructible.

Here is a word of warning, in this context.

Remark 3: In some books, or on the internet, you may come across methods to construct various regular n-gons, where n is not of the form given in Theorem 5. But these are **approximate** constructions, not exact ones. Or they have been done by using instruments other than a straightedge and compass. The constructibility discussed here is about **exact** constructions, not approximate ones, and not using any other instrument.

We end our discussion on Galois theory here. Let us summarise what you have studied in this unit.

14.5 SUMMARY

In this unit, we have discussed the following points.

1) The statement of the **Fundamental Theorem of Galois Theory**: Let L/K be a Galois extension. Let Γ be the set of all subfields F of L containing K, and Σ be the set of all subgroups of $G(L/K)$. Then the following hold:

   i) The maps $\mu : \Gamma \to \Sigma : \mu(F) = G(L/F)$, and $\nu : \Sigma \to \Gamma : \nu(H) = L^H$, are inverses of each other.

   ii) μ and ν are inclusion reversing, that is, for $F_1, F_2 \in \Gamma$, $F_1 \subseteq F_2$ if and only if $G(L/F_2) \subseteq G(L/F_1)$.

   iii) For $F \in \Gamma$, F/K is a Galois extension if and only if $G(L/F)$ is a normal subgroup of $G(L/K)$, and in that case, $G(F/K) \simeq G(L/K) \big/ G(L/F)$.

2) Illustrations of the Fundamental Theorem of Galois Theory, using diagrams for the lattices of subgroups and lattices of the corresponding subfields, in some cases.

3) The definition, and examples, of the Galois group of a polynomial.

4) The definition, and examples, of a solvable group.

5) A polynomial is solvable by radicals if and only if its Galois group is a solvable group.

6) A polynomial of degree ≤ 4 is solvable by radicals.

7) Some examples of polynomials of degree 5 which are not solvable by radicals.

8) The application of Galois theory to constructibility of a regular p-gon, where p is an odd prime number. In particular, the statement of the **Gauss-Wantzel theorem**: A regular n-gon is constructible by ruler and compass if and only if $\phi(n)$ is a power of 2, where ϕ is the Euler-phi function.

9) The following constructions are impossible:

   i) squaring a circle,

   ii) doubling a cube,

   iii) trisecting an angle of 60°.

14.6 SOLUTIONS / ANSWERS

E1) From Unit 13, you know that $L/\mathbb{Q}$ is a Galois extension, with $G(L/\mathbb{Q}) = \{I, \sigma_1, \sigma_2, \sigma_3, \sigma_1\sigma_2, \sigma_1\sigma_3, \sigma_2\sigma_3, \sigma_1\sigma_2\sigma_3\}$, isomorphic to

$C_1 \times C_2 \times C_3$, where $C_1 = G(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, $C_2 = G(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$, $C_3 = G(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$. The C_i are cyclic groups of order 2, generated by σ_i, where $\sigma_1(\sqrt{2}) = -\sqrt{2}$, $\sigma_2(\sqrt{3}) = -\sqrt{3}$, $\sigma_3(\sqrt{5}) = -\sqrt{5}$.

$G(L/\mathbb{Q})$ is abelian. It can have subgroups of order 1, 2, 4 and 8 as it is of order 8. We write down the subgroups and the corresponding subfields.
The unique subgroup of order 1 is $\{1\}$, which corresponds to the fixed field L.
Similarly, the fixed field of the unique subgroup of order 8, i.e., the whole group, is the field $\mathbb{Q}$.
There are seven subgroups of index 4 (and hence order 2):

$H_1 = <\sigma_1>, H_2 = <\sigma_2>, H_3 = <\sigma_3>, H_4 = <\sigma_1\sigma_2>, H_5 = <\sigma_1\sigma_3>,$
$H_6 = <\sigma_2\sigma_3>, H_7 = <\sigma_1\sigma_2\sigma_3>.$

The corresponding fixed fields are of degree 4 over $\mathbb{Q}$, and are:

$F_1 = \mathbb{Q}(\sqrt{3},\sqrt{5}), F_2 = \mathbb{Q}(\sqrt{2},\sqrt{5}), F_3 = \mathbb{Q}(\sqrt{2},\sqrt{3}), F_4 = \mathbb{Q}(\sqrt{5},\sqrt{6}),$
$F_5 = \mathbb{Q}(\sqrt{3},\sqrt{10}), F_6 = \mathbb{Q}(\sqrt{2},\sqrt{15}), F_7 = \mathbb{Q}(\sqrt{15},\sqrt{10})$, respectively.

Finally, we write down subgroups of index 2, i.e., of order 4. There are 7 of them too, namely, $H_8 = <\sigma_1,\sigma_2>, H_9 = <\sigma_1,\sigma_3>, H_{10} = <\sigma_2,\sigma_3>,$
$H_{11} = <\sigma_1,\sigma_2\sigma_3>, H_{12} = <\sigma_2,\sigma_1\sigma_3>, H_{13} = <\sigma_3,\sigma_1\sigma_2>,$
$H_{14} = <\sigma_1\sigma_2,\sigma_1\sigma_3>.$

The corresponding fixed fields are of degree 2 over $\mathbb{Q}$, and are:

$F_8 = \mathbb{Q}(\sqrt{5}), F_9 = \mathbb{Q}(\sqrt{3}), F_{10} = \mathbb{Q}(\sqrt{2}), F_{11} = \mathbb{Q}(\sqrt{15}), F_{12} = \mathbb{Q}(\sqrt{10}),$
$F_{13} = \mathbb{Q}(\sqrt{6}), F_{14} = \mathbb{Q}(\sqrt{30}).$

E2) i) You know that every permutation can be written as a product of transpositions. Also, the transposition $(i\ j) = (1\ i)\ (1\ j)\ (1\ i)$. Hence S_n is generated by $(1\ 2), (1\ 3), \ldots, (1\ n)$.

ii) $(1\ n) = (1\ 2 \ldots n)\ (1\ 2)\ (1\ 2 \ldots n)^{-1}$.
Similarly, by conjugating $(1\ n)$ by $(1\ 2 \ldots n)$, and so on, we can obtain $(1\ i)\ \forall\ i = 3, \ldots, n$.
Hence, $(1\ 2 \ldots n)$ and $(1\ 2)$ generate S_n.

E3) i) If $N \lhd G$, then $N \cap H \lhd H$.
Thus, let $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{e\}$ be a solvable series for G.
Now, as G_{i-1}/G_i is abelian $\forall\ i = 1, \ldots, n$,
$xyx^{-1}y^{-1} \in G_i \cap H\ \forall\ x, y \in G_{i-1} \cap H$. Hence $(G_{i-1} \cap H)/(G_i \cap H)$ is also abelian. Thus,
$H = (G_0 \cap H) \supseteq (G_1 \cap H) \supseteq \ldots \supseteq (G_n \cap H) = \{e\}$ is a solvable series for H.

ii) If G is solvable, you can show that H and G/H are solvable.
For the converse, let $H = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_n = \{e\}$ be a solvable series for H and $G/H = \overline{G}_0 \supseteq \overline{G}_1 \supseteq \ldots \supseteq \overline{G}_n = H$ be a solvable

series for G/H, where $\overline{G}_i = G_i/H$ with $H \lhd G_i \leq G$.

Now consider the series

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_n = \{e\} \quad \ldots(2)$$

Here each $H_i \lhd H_{i-1}$ and H_{i-1}/H_i is abelian.

Also, $\overline{G}_i \lhd \overline{G_{i-1}} \Rightarrow G_i \lhd G_{i-1}$. Further,

$G_{i-1}/G_i \simeq \dfrac{(G_{i-1}/H)}{(G_i/H)} = \overline{G}_{i-1}/\overline{G}_i$, which is abelian.

Thus, (2) is a solvable series for G.

E4) If $|G| = p$, or $|G| = p^2$, then G is abelian, and hence solvable.

Assume that any group of order p^r is solvable for $r \leq m$.

Now let G be a group of order p^{m+1}. If G is abelian, it is solvable.

Suppose G is non-abelian.

Then $Z(G) \leq G$, $Z(G) \neq \{e\}$ and $Z(G) \neq G$.

Also, $Z(G)$ is abelian, and hence solvable.

Consider $G/Z(G)$. This is a p-group of order p^r for some $r \leq m$. Hence $G/Z(G)$ is solvable.

Thus, by E3, G is solvable.

Hence, by the principle of induction, any p-group is solvable.

E5) i) Regarding S_5, from Unit 2 you know that A_5 is simple and non-abelian. Hence it is not solvable. You also know that if S_5 were solvable, then, by E3(i), A_5 would be solvable, which is not true. Hence, S_5 is not solvable.

Since $S_n \hookrightarrow S_{n+1}$, S_n can be considered a subgroup of $S_m \forall\ m \geq n$. Further, since a subgroup of a solvable group is solvable, and S_5 is **not** solvable, S_n cannot be solvable for $m \geq 5$.

ii) Since $A_n \leq S_n \forall\ n$, and S_n is solvable for $n \leq 4$, A_n is solvable for $n \leq 4$.

Since A_5 is simple and non-abelian, it is not solvable.

Also $A_n \leq A_m \forall\ n \leq m$.

Hence A_m is not solvable for $m \geq 5$.

E6) You have seen that S_5 is finite and not simple. Also S_5 is not solvable. Hence the statement is false.

E7) i) $D = \prod_{i<j} (\alpha_i - \alpha_j)^2$, where α_i are the roots of $f(x)$.

For any $\sigma \in G$, σ permutes the α_i. Hence, $\sigma(D) = D$. Since this is true for any $\sigma \in G$, D is in the fixed field of G, which is K.

ii) According to the Fundamental theorem of Galois theory, $\sqrt{D} \in K$ if and only if $\sigma(\sqrt{D}) = \sqrt{D}$ for all $\sigma \in G$. Now, a transposition (i, j) changes $\alpha_i - \alpha_j$ to $\alpha_j - \alpha_i = -(\alpha_i - \alpha_j)$ and leaves all other terms in $\sqrt{D}$ unchanged. Thus, if σ is a transposition,

$\sigma(\sqrt{D}) = -\sqrt{D}$. Therefore, $\sigma(\sqrt{D}) = \sqrt{D}$ if and only if σ is an even permutation. This proves that $\sqrt{D}$ is fixed by every element of G if and only if $G \subset A_n$.

E8) We apply E7 (ii) to check this. Also, from Unit 13, Section 2, you know that if $f(x) = x^3 + px^2 + qx + r$, then $D = -(27B^2 + 4A^3)$, where

$A = q - \frac{p^2}{3}$ and $B = \frac{2p^3}{27} - \frac{pq}{3} + r$.

i) Here $A = -3, B = 1$. So $D = 81$. Hence $\sqrt{D} \in \mathbb{Q}$. Hence $G \subseteq A_3$.

ii) Here $A = 3, B = 1$. So $D = -135$. Thus, $\sqrt{D} \notin \mathbb{Q}$. Hence $G \not\subseteq A_3$.

Hence $G \simeq S_3$.

iii) Here $A = 1, B = 5$. So $D = -679$. Thus, $\sqrt{D} \notin \mathbb{Q}$. Hence $G \not\subseteq A_3$. Hence $G \simeq S_3$.

E9) i) We know that $g(x)$ is irreducible over $\mathbb{Q}$, using Eisenstein's criterion. Now, $g(x)$ has five distinct roots. As in Example 6, $G \simeq S_5$. Since S_5 is not solvable, $g(x)$ is not solvable by radicals.

ii) Use the same process to show that $h(x)$ is not solvable by radicals.

E10) You know that the splitting field of $x^5 - 1$ is $\mathbb{Q}(\zeta)$, where ζ is a primitive 5^{th} root of unity. From Sec.13.5, you know that the Galois group of $x^5 - 1$ is of order 4, and is cyclic. Thus, it is solvable.

E11) Suppose α is constructible. Then $\alpha \in K_m$ for some m, where the fields K_i are as described in Theorem 3. Now take $K_{m+1} = K_m(\sqrt{\alpha})$. With m replaced by $m+1$, the conditions of Theorem 3 are satisfied for $\sqrt{\alpha}$. Hence $\sqrt{\alpha}$ is constructible.
Conversely, if $\sqrt{\alpha}$ is constructible, then $\alpha = (\sqrt{\alpha})^2$ is constructible, since the product of constructible numbers is constructible (by Remark 2).

E12) To prove a cubic polynomial is reducible over any field K, it is necessary and sufficient to prove that it has a linear factor over K. Here $K = \mathbb{Q}$. On simplification, the given polynomial becomes $8x^3 - 6x - 1$. This is a primitive polynomial over $\mathbb{Z}$, and if it has a rational root it must have an integer root. But it does not have any integer root, because if it has one, say α, then 2α will be a root of $x^3 - 3x - 1$. But this polynomial is irreducible over $\mathbb{Z}$, as the only possible integers satisfying it are factors of the constant term, which is 1, i.e., ± 1. Neither of them is a root. Thus, the given polynomial is irreducible over $\mathbb{Z}$, and hence, over $\mathbb{Q}$.

E13) $\cos(\theta/3)$ is $\sqrt{3}/2$ when θ is 90°, and $\sqrt{3}/2$ is constructible as $\sqrt{3}$ and $\frac{1}{2}$ are constructible.

E14) This follows since α is constructible if and only if $\sqrt{\alpha}$ is constructible. Here $\alpha = e^{i\theta}$.

E15) Suppose n is not a power of 2. Let $n = 2^r.d$ where $d > 1$ is odd, and $r \geq 1$. Then $2^n + 1 = (2^{2^r})^d + 1$. Let $x = 2^{2^r}$. Then
$2^n + 1 = x^d + 1 = (x+1)(x^{d-1} - x^{d-2} + x^{d-3} - \cdots + 1)$.
Hence $x + 1 = 2^{2^r} + 1$ is a proper factor of $2^n + 1$, a contradiction.
Thus, n is a power of 2.

E16) i) $p = 11$ is not a Fermat prime. Therefore, a regular 11-gon is not constructible.

ii) $p = 257 = 2^{2^3} + 1$ is a Fermat prime. By Theorem 4, a regular p-gon is constructible in this case.