- We reviewed construction and some properties of finite fields.

Theorem 1. *Let $E = F[\gamma]$ be a simple extension of F. Then there are only finitely many intermediate fields M, i.e.*

$$F \subset M \subset E.$$

Exercise 2. *Let $E = F[\gamma]$ be a simple Galois extension over F. How many intermediate fields are there in between E and F ? (Hint: Use fundamental theorem of Galois theory.)*

Theorem 3 (Converse of Theorem 1)**.** *Let E/F be a finite extension of fields. If there are only finitely many intermediate fields M, i.e. $F \subset M \subset E$ then E/F is a simple extension, i.e. there exists $\gamma \in E$ such that $E = F[\gamma]$.*

Remark 4. Theorem 1 and Theorem 3 do not require separability assumption. Recall that the primitive element theorem required some separability assumption.

Remark 5. We can describe all the intermediate fields of a simple extension $E = F(\gamma)/F$. Let $f(X) \in F[X]$ be the irreducible polynomial for the primitive element γ. Every intermediate field is generated over F by the coefficient of a factor $g(X)$ of $f(X)$ in $E[X]$.

Example 6. We list all the intermediate fields for the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. We have already seen $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Let $f(X) \in \mathbb{Q}[X]$ be the minimal polynomial for the primitive element $\sqrt{2} + \sqrt{3}$ of the extension $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$. Note that the degree of $f(X)$ is 4. We find the irreducible factors of $f(X) \in \mathbb{Q}(\sqrt{2}, \sqrt{3})[X]$,

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

(a) There are four linear factors. If we take any of the linear factor out of $X - (\sqrt{2} + \sqrt{3})$, $X - (\sqrt{2} - \sqrt{3})$, $X - (-\sqrt{2} + \sqrt{3})$ and $X - (-\sqrt{2} - \sqrt{3})$, then the corresponding intermediate field is $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ itself.

(b) There are 6 quadratic factors which are product of any two linear factors. For example, if we take a quadratic factor $(X - (\sqrt{2} + \sqrt{3}))(X - (\sqrt{2} - \sqrt{3})) = (X - \sqrt{2})^2 - 3 = X^2 - 2\sqrt{2}X - 1$. The coefficients of this polynomial are $1, -2\sqrt{2}, -1$ and hence the field generated by these coefficients is $\mathbb{Q}(2\sqrt{2}) = \mathbb{Q}(\sqrt{2})$.
Similarly, the coefficients of the remaining five polynomials of degree 2 will either generate $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{6})$ (check!).

(c) There are 4 polynomials of degree 3 which are factor of $f(X)$. If we take

$$\begin{aligned} & (X - (\sqrt{2} + \sqrt{3}))(X - (\sqrt{2} - \sqrt{3}))(X - (-\sqrt{2} + \sqrt{3})) \\ = \; & (X^2 - 2\sqrt{2}X - 1)(X - (-\sqrt{2} + \sqrt{3})) \\ = \; & X^3 - (\sqrt{2} + \sqrt{3})X^2 + (3 + 2\sqrt{6})X - (-\sqrt{2} + \sqrt{3}). \end{aligned}$$

Then the field generated by the coefficient of these polynomials is $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.
Similarly, the coefficients of other degree 3 polynomials will also generate the field $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ (check!).

(d) There is only one polynomial of degree 4 which is $f(X)$ itself which is a factor of $f(X)$ itself. In this case the intermediate field generated by the coefficients is $\mathbb{Q}$.

Remark 7. In the above example the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is a Galois extension. In this case, describing the intermediate field is much easier using the fundamental theorem of Galois theory.