• Answer to questions:
— In a ring A (commutative with unity), the group of units $A^\times$, irreducible elements: definition, examples: fields, $\mathbb{Z}$, $K[X]$, $\mathbb{Z}[X]$. Irreducible elements in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$.
— Order of an element x in a group G: kernel of the homomorphism $\mathbb{Z} \to G$ which maps n to x^n.
— Cyclic groups. Subgroups. Direct products of cyclic groups. Finite groups of order ≤ 7 (already done in fourth course – it seemed necessary to repeat).
— The group $\mathrm{GL}_2(\mathbb{Q})$.
— The quartic extension $E = \mathbb{Q}(i, \sqrt{2})$ of $\mathbb{Q}$. Galois group, subgroups, subfields, Galois correspondence between subfields of E and subgroups of the Galois group.
— Given a Galois extension E/F and a subfield M of E containing F, necessary and sufficient condition for M to be Galois over F.

• The Galois group of a separable polynomial of degree n as a subgroup of $\mathfrak{S}_n$. Transitive subgroups of $\mathfrak{S}_n$. The Galois group of f over F is transitive if and only if f is irreducible over F. Example: the Galois group of $(X^2 - 2)(X^2 + 1)$ over $\mathbb{Q}$.

`Reference`: J.S. Milne, Fields and Galois Theory Version 4.52 March 17, 2017.