Dror Bar-Natan: Classes:
2025-26: MAT 347 Groups, Rings, Fields:

# Galois Summary

http://drorbn.net/25-347

## Selick.

1. **Thm 3.1.1.** The gcd in an extension field is the same as in the base field.
2. **Thm 3.1.4.** Eisenstein's Criterion). $R$ a UFD, $p \in R$ a prime, $f = \sum_0^n a_i x^i$ with $p||a_0$, $p|a_1$, …, $p|a_{n-1}$, $p \nmid a_n$. Then $f$ is irreducible in $Q(R)[x]$.
3. **Prop 3.2.2.** $[L:F] = [L:K][K:F]$.
4. **Lem 3.2.8.** The minimal polynomial is irreducible.
5. **Lem 3.2.9.** If $a$ is algebraic over $F$, then $[F(a):F]$ is the degree of the minimal polynomial of $a$.
6. **Lem 3.2.10.** Also, $F(a) = F[a]$.
7. **Cor 3.2.11.** Also, $F(a) \cong F[x]/(\text{min. poly. of } a)$.
8. **Thm 3.2.12.** The set of algebraic elements over $F$ is a field.
9. **Cor 3.2.13.** If $L/K/F$ and $K/F$ and $L/K$ are algebraic, then so is $L/F$.
10. **Def 3.3.9.** A splitting field.
11. **Thm 3.3.13.** If $E/F$, $E'/F'$, $\tau\colon F \to F'$ a morphism, $p \in F[x]$ irreducible, $p' = \tau p$, $a$, $a'$ roots of $p$, $p'$ in $E$, $E'$, then there is an extension $\tilde\tau\colon E \to E'$ of $\tau$ such that $\tilde\tau(a) = a'$. ("all roots of an irreducible polynomial are the same").
12. **Thm 3.3.15.** If $\tau\colon F \to F'$ an isomorphism, $p \in F[x]$ irreducible, $p' = \tau p$, $E$ is a splitting field of $p$ and $E'$ is a splitting field of $p'$, then there is an extension of $\tau$ to an isomorphism $\tilde\tau\colon E \to E'$.
13. **Thm 3.4.1.** Frobenius: If $\operatorname{char} F = p$ then $(a+b)^p = a^p + b^p$ and more generally, $(a+b)^{p^k} = a^{p^k} + b^{p^k}$.
14. **Thm 3.5.1.** $f$ has repeated roots iff $\gcd(f, f') \neq 1$.
15. **Cor 3.5.2.** $f \in F[x]$ irreducible. If $f$ has repeated roots then $p := \operatorname{char} f \neq 0$ and $f(x) = g(x^p)$ for some $g$.
16. **Cor 3.6.2.** A finite field has $q = p^n$ elements.
17. **Cor 3.6.3** (Fermat). In a finite field with $q$ elements, $\forall a\, a^q = 1$.
18. **Thm 3.6.4.** A finite field with $q$ elements is a splitting field of $x^q - x$ over $\mathbb{F}_p$ (and thus any two are isomorphic).
19. **Thm 3.6.7.** The roots of $x^q - x$ in its splitting field make a field, and hence $\mathbb{F}_q$ exists.
20. **Thm 3.6.8.** In a finite group, if for every $n$ there are at most $n$ elements with $g^n = e$, then $G$ is cyclic.
21. **Cor 3.6.9.** Any finite subgroup of the multiplicative group of a field is cyclic.
22. **Cor 3.6.10.** The multiplicative group of $\mathbb{F}_q$ is cyclic.
23. **Def 3.7.1.** Separable elements, separable extensions.
24. **Prop 3.7.2.** in characteristic 0, every extension is separable.
25. **Example 3.7.3.** If $\operatorname{char} F = p$ and $E = F(z)$ then $E(z^{1/p})/E$ is not separable.
26. **Thm 3.7.4.** A separable extension can be generated by a single element.
27. **Thm 3.8.2.** Distinct field automorphisms are linearly independent.
28. **Thm 3.8.3.** The fixed set $E^S$ of a set $S$ of automorphisms of $F$ is a field, "the fixed field".
29. **Def.** $\operatorname{Gal}(E/F)$.
30. **Claim** $E^{\operatorname{Gal}(E/F)} \supset F$.
31. **Thm 3.8.5.** $|\operatorname{Gal}(E/F)| \leq [E:F]$.

## Gallian.

1. **Page 557.** $\operatorname{Gal}(3x^5 - 15x + 5) \cong S_5$.

**08-401 handout "Fundamental Theorem".** Assuming $\operatorname{char} F = 0$.

1. **The Fundamental Theorem.** Given a splitting $E/F$, there is a bijection $\{K\colon E/K/F\} \longleftrightarrow \{H\colon H < \operatorname{Gal}(E/F)\}$ which is
   - (a) Inclusion reversing.
   - (b) Degree/index respecting: $[E:K] = |\operatorname{Gal}(E/K)|$ and $[K:F] = (\operatorname{Gal}(E/F) : \operatorname{Gal}(E/K))$.
   - (c) Splitting fields correspond to normal subgroups: If $K$ in $E/K/F$ is the splitting field of a polynomial in $F[x]$ then $\operatorname{Gal}(E/K)$ is normal in $\operatorname{Gal}(E/F)$ and $\operatorname{Gal}(K/F) \cong \operatorname{Gal}(E/F)/\operatorname{Gal}(E/K)$.