1. Tétel (Egyszerű bővítés előállítása faktorgyűrűként)
Ha $K \leq L$ testek és $\alpha \in L$ algebrai K fölött, akkor $K(\alpha) \cong K[x]/(p(x))$ valamely $p(x) \in K[x]$ irreducibilis polinomra, amelyre $p(\alpha) = 0$

Biz.: Tekintsük a $\varphi : K[x] \to L$, $f(x) \mapsto f(\alpha)$ $\forall f(x) \in K[x]$ gyűrűhomomorfizmust.

$$\operatorname{Ker}\varphi = \{\, f(x) \in K[x] \mid f(\alpha) = 0 \,\} \lhd K[x],$$

és $\neq 0$, mivel α algebrai. De $K[x]$ főideálgyűrű, így van olyan $0 \neq p(x) \in K[x]$ polinom, hogy $\operatorname{Ker}\varphi = (p(x))$. A homomorfizmustétel szerint

$$K[x]/(p(x)) = K[x]/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi \leq L,$$

ezért $K[x]/((p(x))$ 0-osztómentes $\Rightarrow p(x)$ irreducibilis. De akkor $(p(x))$ maximális ideál $K[x]$-ben, tehát $K[x]/((p(x))$, és így a vele izomorf $\operatorname{Im}\varphi$ is, test.
$\forall c \in K,\ \varphi(c) = c$, és $\varphi(x) = \alpha$, így $K(\alpha) \leq \operatorname{Im}\varphi$, másrészt $\operatorname{Im}\varphi = \{\, f(\alpha) \mid f(x) \in K[x] \,\}$ nyilván benne van $K(\alpha)$-ban. Tehát

$$K(\alpha) = \operatorname{Im}\varphi \cong K[x]/((p(x)).$$

2. Tétel (Algebrai bővítések egymásutánja)
Ha $K \leq L \leq M$ testek, ahol $L|K$ és $M|L$ algebrai, akkor $M|K$ is algebrai.

Biz.: Legyen $\alpha \in M$. Mivel $M|L$ algebrai,

$$\exists\ 0 \neq f(x) = a_n x^n + \ldots + a_1 x + a_0 \in L[x],\ \text{hogy}\ f(\alpha) = 0.$$

Legyen $K_i = K(a_0, \ldots, a_i)$ $(i = 0, 1, \ldots, n)$. Ekkor $f(x) \in K_n[x]$, tehát α algebrai K_n fölött is, s mivel $K_n(\alpha)|K_n$ egyszerű bővítés, véges fokú is. Minden i-re $a_i \in L$, tehát a_i algebrai K fölött, és így K_{i-1} fölött is, amiből $(K_i : K_{i-1}) = (K_{i-1}(a_i) : K_{i-1}) < \infty$ $\forall i$, és $(K_0 : K) = (K(a_0) : K) < \infty$ is következik. A szorzattétel szerint

$$(K_n(\alpha) : K) = (K_n(\alpha) : K_n) \cdot (K_n : K_{n-1}) \cdots (K_1 : K_0) \cdot (K_0 : K) < \infty,$$

ezért α algebrai K fölött.

3. Tétel (Véges normális bővítések jellemzése)
Az $N|K$ véges fokú bővítés pontosan akkor normális, ha valamely K fölötti polinom felbontási teste.

Biz.: $\Rightarrow$: Mivel $(N : K) < \infty$, van véges sok olyan algebrai elem, $\alpha_1, \ldots, \alpha_n \in N$, hogy $N = K(\alpha_1, \ldots, \alpha_n)$. Legyen $p_i(x) \in K[x]$ az α_i minimálpolinomja minden i-re, és $f(x) = p_1(x) \cdots p_n(x) \in K[x]$. A $p_i(x)$ polinomok irreducibilisek, és van N-ben gyökük, ezért a bővítés normalitása miatt lineáris faktorokra bomlanak, és így $f(x)$ is lineáris faktorokra bomlik. Másrészt a bővítést generálja f néhány gyöke, tehát N az f felbontási teste K fölött.
$\Leftarrow$: Legyen N az $f(x) \in K[x]$ felbontási teste, tehát f felbomlik N fölött:

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n),\ \text{és}\ N = K(\alpha_1, \ldots, \alpha_n).$$

Legyen továbbá $p(x) \in K[x]$ irreducibilis, amelynek van gyöke N-ben: $p(\beta) = 0$ valamely $\beta \in N$-re. Mivel $N = K(\alpha_1, \ldots, \alpha_n)$, a β elem előáll az α_i-k polinomjaként: $\beta = g(\alpha_1, \ldots, \alpha_n)$ valamely $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ többváltozós polinomra. Legyen

$$h(x) = \prod_{\sigma \in S_n} (x - g(\alpha_{1\sigma}, \ldots, \alpha_{n\sigma})).$$

Ez a polinom invariáns az α_i-k permutációira, így az együtthatói α_i-knek szimmetrikus polinomjai, tehát α_i-k elemi szimmetrikus polinomjainak polinomjai. Ezek az elemi szimmetrikus polinomok pedig — előjeltől eltekintve — az f együtthatói, ezért $h(x) \in K[x]$. De $(x - \beta) \mid h(x) \Rightarrow h(\beta) = 0$ $\Rightarrow p(x) \mid h(x)$. De $h(x)$ felbomlik lineáris tényezők szorzatára N fölött, tehát $p(x)$ is felbomlik.

4. Tétel (Véges szeparábilis bővítés egyszerűsége)
Ha $L|K$ véges fokú szeparábilis bővítés, akkor van olyan $\gamma \in L$, hogy $L = K(\gamma)$.

Biz.: Ha K véges test, akkor L is az, és akkor az $L^\times$ ciklikus csoport generátoreleme megfelel γ-nak. Ezért a továbbiakban feltesszük, hogy K végtelen.
$L = K(\gamma_1, \dots, \gamma_k)$. Mivel $K \leq M \leq L$-re $M|K$ is szeparábilis, elég azt belátni, hogy minden $\alpha, \beta \in L$-re van olyan γ, amelyre $K(\alpha, \beta) = K(\gamma)$.
Legyen $f(x), g(x) \in K[x]$ az α, illetve β minimálpolinomja, és $F \geq L$ az $f(x)g(x)$ felbontási teste L fölött. F-ben $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ és $g(x) = (x - \beta_1) \cdots (x - \beta_m)$, ahol $\alpha = \alpha_1, \dots, \alpha_n$, illetve $\beta = \beta_1, \dots, \beta_m$ különbözők az $L|K$ szeparábilitása miatt. Mivel K végtelen, van olyan $c \in K$, amelyre $\gamma := \alpha + c\beta \neq \alpha_i + c\beta_j$ minden $(i, j) \neq (1, 1)$-re. Megmutatjuk, hogy erre a γ-ra $K(\alpha, \beta) = K(\gamma)$.
A $g(x)$, $f(\gamma - cx) \in K(\gamma)[x]$ polinomoknak a felbontási testben egyetlen közös gyöke a β, így a legnagyobb közös osztójuk $F[x]$-ben, és így $K(\gamma)[x]$-ben is, $x - \beta$. Ezért $\beta \in K(\gamma)$, amiből $\alpha = \gamma - c\beta \in K(\gamma) \Rightarrow K(\alpha, \beta) \leq K(\gamma) \Rightarrow K(\alpha, \beta) = K(\gamma)$.

5. Tétel (A körosztási polinom irreducibilitása)
$\mathbb{Q}$ fölött minden $\Phi_n(x)$ körosztási polinom irreducibilis.

Biz.: $\Phi_n(x) := \prod_{i=1}^{\varphi(n)} (x - \varepsilon_i)$, ahol $\varepsilon_1, \dots, \varepsilon_{\varphi(n)} \in \mathbb{C}$ a primitív n-edik egységgyökök. Tudjuk, hogy $\Phi_n(x) \in \mathbb{Z}[x]$ (n-re vonatkozó indukcióval n-re az $x^n - 1 = \prod_{d|n} \Phi_d(x)$ összefüggésből).
Ha $\Phi_n(x)$ reducibilis $\mathbb{Q}[x]$-ben, akkor $\mathbb{Z}[x]$-ben is felbontható irreducibilisekre:

$$\Phi_n(x) = f_1(x) \cdots f_k(x), \text{ ahol } \forall f_i(x) \in \mathbb{Z}[x] \text{ irred.}$$

Legyen az $f_1(x)$ egyik gyöke ε. Belátjuk, hogy ekkor minden $p \nmid n$-re ε^p is gyöke f_1-nek.
Tegyük fel, hogy $f_1(\varepsilon^p) \neq 0$. ε^p is primitív n-edik egységgyök $\Rightarrow$
$\exists i \neq 1 : \ f_i(\varepsilon^p) = 0 \Rightarrow f_1(x)$-nek és $f_i(x^p)$-nek az ε közös gyöke $\mathbb{C}$-ben $\Rightarrow (f_1(x), f_i(x^p)) \neq 1$
$\overset{f_1 \text{ irred.}}{\Longrightarrow} f_1(x) \mid f_i(x^p)$, és az osztás $\mathbb{Z}[x]$-ben is elvégezhető, mivel $f_1(x)$ 1-főegyütthatós. Tekintsük most ezeket a polinomokat $\mathbb{Z}_p$ fölött. $\mathbb{Z}_p[x]$-ben $f_1(x) \mid f_i(x^p) = (f_i(x))^p \Rightarrow (f_1(x), f_i(x)) \neq 1 \Rightarrow$ $\Phi_n(x) = f_1(x)f_i(x) \cdots f_k(x)$ nem szeparábilis mint $\mathbb{Z}_p[x]$-beli polinom $\Rightarrow x^n - 1$ sem szeparábilis. De p nem osztója n-nek $\Rightarrow (x^n - 1)' = nx^{n-1} \neq 0$ relatív prím $(x^n - 1)$-hez, ami ellentmondás.
Azt kaptuk, hogy $f_1(x)$ gyökeinek a halmaza zárt a p-edik hatványra emelésre minden $p \nmid n$ prím esetén, így az m-edik hatványra emelésre is, ha $(m, n) = 1$. De ε^m-ként az összes primitív n-edik egységgyököt megkapjuk az f_1 egyetlen gyökéből, tehát $\Phi_n(x) = f_1(x)$, vagyis $\Phi_n(x)$ irreducibilis.

6. Tétel (Az algebra alaptétele)
$\mathbb{C}$ fölött minden nem konstans polinomnak van gyöke.

Biz.: Azt kell belátni, hogy $\mathbb{C}[x]$-ben minden irreducibilis polinom elsőfokú, azaz hogy $\mathbb{C}$-nek nincs véges fokú bővítése.
Tegyük fel, hogy nem igaz az állítás. Legyen $L \geq \mathbb{C}$ véges fokú bővítés, ahol $L \neq \mathbb{C}$. Feltehető, hogy L normális $\mathbb{R}$ fölött (és így $\mathbb{C}$ fölött is): ha nem lenne az, akkor is egyszerű bővítése $\mathbb{R}$-nek, és akkor vehetjük L helyett a bővítést adó elem $\mathbb{R}$ fölötti minimálpolinomjának felbontási testét, az is véges fokú bővítés.
Tekintsük az $\mathbb{R} \leq \mathbb{C} \leq L$ bővítéssorozatot, és a $G = \mathrm{Gal}(L|\mathbb{R})$ Galois-csoportot. Legyen $|G| = 2^k m$, ahol m páratlan. Ha $P \in \mathrm{Syl}_2(G)$, akkor $(P^* : \mathbb{R}) = |G : P| = m$ páratlan, de $\mathbb{R}$-nek nincs páratlan fokú valódi bővítése, ugyanis $\mathbb{R}$-en kívüli elemnek nem lehet páratlan fokú minimálpolinomja, mert minden páratlan fokú valós polinomnak van valós gyöke a Bolzano-tétel miatt. Tehát $m = 1 \Rightarrow$ $(L : \mathbb{R}) = |G| = 2^k \Rightarrow (L : \mathbb{C}) = 2^{k-1}$.
Legyen $G_1 = \mathrm{Gal}(L|\mathbb{C})$. Mivel G_1 2-csoport, $\exists G_2 \leq G_1$, hogy $|G_1 : G_2| = 2$. De akkor az $L|\mathbb{C}$ bővítés és G_1 közötti Galois-kapcsolatot használva azt kapjuk, hogy G_2^* a $\mathbb{C}$-nek másodfokú bővítése, holott ilyen nem létezhet, mert $\mathbb{C}$ fölött minden másodfokú egyenlet megoldható. Ezzel ellentmondásra jutottunk.