Крайни полета.

Ще казваме, че полето F е крайно, когато то има краен брой елементи, т.е. $|F| < \infty$.

Лема 1. *Нека F е крайно поле. Тогава*

а) ако K е подполе на F, то $|F| = |K|^n$ за някое $n \in \mathbb{N}$,

б) $|F| = p^n$ за някое просто число p и $n \in \mathbb{N}$. Още повече $\operatorname{char} F = p$.

Доказателство. а) Разглеждаме F като линейно пространство над K. Елементите от F разглеждаме като вектори и за $\forall a, b \in F$, имаме дефинирано събиране $a + b \in F$. Елементите на K разглеждаме като скалари и за $\forall a \in F, \forall \lambda \in K$ имаме дефинирано умножение $\lambda a \in F$. Т.к. $|F| < \infty$, то единствената възможност е размерността $\dim_K F = n < \infty$ също да е крайна. Нека $e_1, e_2, \ldots, e_n$ е базис на F над K. За всеки елемент $c \in F$ има изразяването $c = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n$ за елементи $\lambda_i \in K, i = 1, 2, \ldots, n$. За всеки елемент $\lambda_i \in K$ има точно $|K|$ на брой възможности и следователно за n-торката $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ има $\underbrace{|K|.|K|\ldots|K|}_{n \text{ пъти}} = |K|^n$ възможности. Така излиза, че $|F| = |K|^n$.

б) Щом $|F| < \infty$, то $\operatorname{char} F \neq 0$ (ако доупснем противното веднага получаваме противоречие). Следователно $\operatorname{char} F = p$ за някое просто число p. Знаем, че F има единствено просто подполе P, което е изоморфно на $\mathbb{Z}_p$. Следователно $P \leq F$ и $|P| = p$. От подточка а) получаваме, че $|F| = |P|^n = p^n$ за някое естествено число $n \in \mathbb{N}$. $\square$

Теорема 1. *За всяко просто число p и за всяко число $n \in \mathbb{N}$ съществува единствено (с точност до изоморфизъм) поле с p^n на брой елемента.*

Доказателство. Нека $P = \mathbb{Z}_p$ и разгледаме полинома

$$f(x) = x^{p^n} - x \in P[x].$$

Нека F е полето на разлагане на $f(x)$ над P (знаем, че то съществува) и F_1 е множеството от корените на $f(x)$. Ясно е, че $F_1 \subseteq F$. Имаме, че

$$f'(x) = p^n x^{p^n - 1} - 1 = -1,$$

защото $\operatorname{char} F = \operatorname{char} P = p$. И така $f'(x)$ няма корени, следователно $f(x)$ и $f'(x)$ нямат общ корен, което влече, че $f(x)$ няма кратни корени. Тогава $|F_1| = \deg f = p^n$. Дотук получихме, че $F_1 \subseteq F$ и $|F_1| = p^n$.

Очевидно 0 и 1 (от теоремата на Ойлер-Ферма) са корени на $f(x)$ и следователно $0, 1 \in F_1$. За проивзолни $\alpha, \beta \in F_1$, понеже $\operatorname{char} F = p$, имаме, че $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha+\beta$. Последното очевидно означава, че $\alpha + \beta$ също е корен на $f(x)$, т.е. $\alpha + \beta \in F_1$. Поради аналогични причини $\alpha - \beta \in F_1$. Освен това $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ и оттук $\alpha\beta \in F_1$. Ако $\alpha \neq 0$, то $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$ и следователно $\alpha^{-1} \in F_1$. Всичко казано дотук доказва, че F_1 е поле, а оттам и подполе на F.

И така, $\operatorname{char} F_1 = \operatorname{char} F = p$. Следователно F_1 съдържа единствено просто подполе, изоморфно на $\mathbb{Z}_p = P$. Но също единственото такова подполе в F е P. Така се оказва, че F_1 съдържа P и корените на $f(x)$, но това е дефиницията на полето F и $F_1 \leq F$, което означава, че $F_1 = F$. Останалата част от твърдението следва от Лема 1 а). $\square$

При дадени просто число p и естествено число n, единственото крайно поле с p^n елемента се означава с $GF(p^n)$ и се нарича *поле на Галоа (Galois field)*. Както видяхме в Теорема 1, $GF(p^n)$ се състои от корените на полинома $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Оттук всъщност е ясно и че $GF(p) \equiv \mathbb{Z}_p$.

Лема 2. *Нека G е група, а елементите $a, b \in G$ са от редове съответно m и n и още е изпълнено, че $ab = ba$. Тогава G има елемент от ред най-малкото общо кратно на m и n, което означаваме като $[m, n]$.*

Доказателство. Нека означим $t = [m, n]$. Да разгледаме частния случай $(m, n) = 1$. Тогава $t = mn$ и имаме $(ab)^{mn} = a^{mn}b^{mn}$ заради изискването $ab = ba$. И така, $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1^n 1^m = 1$, което означава, че елементът ab е от краен ред, който ще означим с d. Ясно е, че $d \mid mn$. Имаме, че $(ab)d = a^d b^d = 1$ и след повдигане на n-та степен получаваме, че $a^{dn}(b^n)^d = 1$, което е еквивалентно на $a^{dn} = 1$. Т.к. a беше от ред m, това всъщност означава, че $m \mid dn$, но т.к. $(m, n) = 1$ остава да е възможно единствено $m \mid d$. Поради аналогични съображения имаме и че $n \mid d$. От $m \mid d, n \mid d$ и $(m, n) = 1$ следва, че $mn \mid d$. Така доказахме, че $d = mn = [m, n]$.

Нека в общия случай $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ и $n = p_1^{l_1} p_2^{l_2} \dots p_r^{l_r}$, където $p_i, i = 1, \dots, s$ са разлини прости числа, а k_i, l_i са неотрицателни цели числа. Тогава $t = [m, n] = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$, където $u_i = \max(k_i, l_i), i = 1, 2, \dots, r$. Елементът $a^{\frac{m}{p_i^{k_i}}}$ има ред $p_i^{k_i}$, а елементът $b^{\frac{n}{p_i^{l_i}}}$ има ред $p_i^{l_i}$. Т.к. или $u_i = p_i$, или $u_i = l_i$, то или $p_i^{u_i} = p_i^{k_i}$, или $p_i^{u_i} = p_i^{l_i}$. Така се оказва, че G има елемент c_i от ред $p_i^{u_i}$ за всяко $i = 1, 2, \dots, r$. И така, елементите $c_1, c_2, \dots, c_r \in G$ имат редове $p_1^{u_1}, p_2^{u_2}, \dots, p_r^{u_r}$, които са два по два взаимно прости, т.к. p_i са различни прости числа. От частния случай следва, че $c = c_1 c_2 \dots c_r \in G$ е от ред $p_1^{u_1} p_2^{u_2} \dots p_r^{u_r} = t = [m, n]$. $\square$

Теорема 2. *Нека F е произволно поле, а G е крайна подгрупа на мултипликативната група F^* на F. В частност, ако F е крайно, то $GF(p^n)^*$ е циклична група.*

Доказателство. Знаем, че $F^* = F\{0\}$ е абелева група относно операцията умножение в F. Имаме, че $G \leq F^*$ и $|G| < \infty$. Нека $a \in G$ е елемент от най-голям ред m, а $b \in G$ е произволен елемент от ред n. Тогава $m \mid |G|$ и $m \leq |G|$. Ако допуснем, че $n \nmid m$, то $[m, n] > m$, а според Лема 2 в G има елемент от ред $[m, n]$. Това противоречи на максималността на m като ред на елемент от G. Следователно $n \mid m$ и $b^m = 1$. По този начин всъщност доказахме, че $b^m = 1$ за всеки елемент $b \in G$. Разглеждаме полинома $f(x) = x^m - 1 \in F[x]$. Имаме, че $f(b) = 0$ за $\forall b \in G$, което означава, че f има поне $|G|$ на брой корени. Същевременно f може да има не повече от $\deg f = m$ корена в $|G|$, което означава, че $|G| \leq m$. С това $|G| = m$. Още, $\langle a \rangle \leq G$ също е от ред m, което означава, че просто $G = \langle a \rangle$ и G е циклична група.

Ако $F = GF(p^n)$, то $F^* = F \backslash \{0\}$ е циклична група от ред $p^n - 1$ и се поражда от елемент $a \in F$ от същия ред, т.е.

$$F^* = \langle a \rangle = \{a, a^2, \dots, a^{p^n - 1} = 1\}.$$

$\square$

Теорема 3. *Нека $F = GF(p^n)$. Ако K е подполе на F, то $|K| = p^m$ (т.е. $K = GF(p^m)$) и $m \mid n$. Обратно, ако $m \in \mathbb{N}$ и $m \mid n$, то F има единствено подполе K с $|K| = p^m$.*

Доказателство. Нека K е подполе на F. От Лема 1 имаме, че $|F| = |K|^t$ за някое $t \in \mathbb{N}$. Така $|K|^t = p^n$ или още $|K| = p^m$ за някое $m \in \mathbb{N}$ и $p^{tm} = p^n$, т.е. $n = tm$ и $m \mid n$.

Обратно, нека $m \in \mathbb{N}$ и $m \mid n$. Означаваме

$$K = \Big\{a \in F | a^{p^m} = a\Big\} \subseteq F.$$

Директно се проверява (точно както в Теорема 1), че $K \leq F$ е подполе на F. Ще докажем, че $|K| = p^m$. Очевидно имаме, че $0 \in K$. За ненулев елемент $a \in F$ имаме, че $K \iff a^{p^m-1} = 1$. От $m \mid n$ следва, че $p^m - 1 \mid p^n - 1$ и F^* е циклична група от ред $p^n - 1$ според Теорема 2. Знаем, че F^* има единствена подгрупа от ред $p^m - 1$ и тя се изчерпва с елементи $a \in F$, за които $a^{p^m-1} = 1$, т.е. в F^* има $p^m - 1$ елемента. Сега $|K| = p^m - 1 + 1 = p^m$ (заради $0 \in K$). Така K е подполе на F и $|K| = p^m$, т.е. $K = GF(p^m)$. Ако и L е подполе на F с $|L| = p^m$, то $L^* = L\{0\}$ е подгрупа на F^* и $|L^*| = p^m - 1$. Т.к. F^* има единствена подгрупа от ред $p^m - 1$, то $L^* = K^*$, а оттам и $L = K$, т.е. K е единственото подполе на F с p^m елемента. $\square$

Пример: Подполетата на $GF(3^7)$ са само цялото $GF(3^7)$ и $GF(3) = \mathbb{Z}_3$. Подполетата на $GF(2^{12})$ са $GF(2^m)$ за $m = 1, 2, 3, 4, 6, 12$.