# Príklad rozšírených okruhov a polí

## Obsah

NTL podporuje rozšírené okruhy a polia cez konečné polia a cez polynomiálnu aritmetiku takých to rozšírení.

# 1 Príklad

```
#include <NTL/ZZ_pXFactoring.h>
#include <NTL/ZZ_pEX.h>

NTL_CLIENT

int main()
{
   ZZ_p::init(to_ZZ(17)); // definovanie GF(17)

   ZZ_pX P;
   BuildIrred(P, 10);
                    // generovanie irreducibilného polynómu
                    // P stupňa 10 nad GF(17)

   ZZ_pE::init(P);  // definovanie GF(17^10)

   ZZ_pEX f, g, h;  // deklarovanie polynómov
                    //nad GF(17^10)

   random(f, 20);   // f je náhodný, normovaný
                    //polynóm stupňa 20
   SetCoeff(f, 20);

   random(h, 20);   // h je náhodný polynóm
                    //stupňa menšieho ako 20

   g = MinPolyMod(h, f);
                    // výpočet minimálneho
                    //polynómu z h modulo f

   if (g == 0) Error("oops (1)"); // kontrola či g != 0

   if (CompMod(g, h, f) != 0) // kontrola či g(h)=0 mod f
      Error("oops (2)");
}
```

Tento program ilustruje zostavenie rozšírených okruhov cez `ZZ_p`. `ZZ_p` a GF2 môžeme taktiež použiť ako základnú triedu, syntax je úplne rovnaký.