Ściągawka

Marcin Kotowski, Michał Kotowski

11 czerwca 2012

Ściągawka ma charakter pomocniczy - w szczególności, zamieszczone tu zadania służą jedynie do samodzielnego zrobienia (nie trzeba ich przysyłać).

1 Wielomiany

Rozpatrzmy dowolny zbiór współczynników R (mogą to być np. liczby rzeczywiste $\mathbb{R}$ albo $\mathbb{Z}_p$). Niech $R[x]$ oznacza zbiór wielomianów o współczynnikach z R. Mając zadany dowolny wielomian $f \in R[x]$, możemy utworzyć pierścień wielomianów modulo f, oznaczany $R[x]/(f)$, w następujący sposób. Dwa wielomiany $g, h \in R[x]$ uznajemy za równoważne (ozn. $g \sim_f h$), jeśli istnieje wielomian $a \in R[x]$ taki, że $h = g + af$.

Zadanie 1.1. *Udowodnij, że relacja $\sim_f$ jest relacją równoważności, to znaczy jest: a) zwrotna: dla każdego $g \in R[x]$ zachodzi $g \sim_f g$); b) symetryczna ($g \sim_f h$ wtedy i tylko wtedy, gdy $h \sim_f g$); c) przechodnia (jeśli $g \sim_f h$ i $h \sim_f p$, to $g \sim_f p$)*

Relacja $\sim_f$ jest relacją równoważności, a więc dzieli $R[x]$ na klasy abstrakcji - klasę abstrakcji wielomianu f oznaczamy przez $[f]$. Elementami $R[x]/(f)$ są klasy abstrakcji, z działaniami zdefiniowanymi:

- $[g] + [h] := [g + h]$
- $[g] \cdot [h] := [g \cdot h]$

Zauważ, że a priori taki sposób określenia działań może nie być poprawny - prawa strona może bowiem zależeć od wyboru reprezentantów klas abstrakcji. To znaczy, jeśli dla dwóch wielomianów g, g' mamy $[g] = [g']$ (czyli $g \sim_f g'$), to powinniśmy mieć $[g + h] = [g] + [h] = [g'] + [h] = [g' + h]$, czyli $[g' + h] = [g + h]$. Należy sprawdzić, że tak istocie jest!

Zadanie 1.2. *Udowodnij, że wyżej zdefiniowane działania są dobrze określone w tym sensie, że nie zależą od wyboru reprezentantów klas abstrakcji (np. że jeśli $[g] = [g']$ i $[h] = [h']$, to $[g + h] = [g' + h']$ i tak samo dla mnożenia).*

Zadanie 1.3. *Niech $[0]$ będzie klasą abstrakcji wielomianu tożsamościowo równego 0. Jakie inne wielomiany leżą w klasie abstrakcji $[0]$? Analogicznie, niech $[1]$ będzie klasą abstrakcji wielomianu stale równego 1. Jakie inne wielomiany, leżą w klasie abstrakcji $[1]$?*

Zadanie 1.4. *Udowodnij, że* $[0]$ *pełni rolę elementu neutralnego dodawania (tzn.* $[g]+[0]=[g]$*), a* $[1]$ *elementu neutralnego mnożenia (*$[g]\cdot[1]=[g]$*).*

Możemy myśleć o $R[x]/(f)$ jako o wielomianach $R[x]$ z dodatkowo wprowadzoną relacją $f=0$ - porównaj to np. ze sposobem zdefiniowania $\mathbb{Z}_n$ jako liczb całkowitych $\mathbb{Z}$ z dodatkową relacją $n=0$ (gdzie dwie liczy a,b uznajemy za równoważne, jeśli $a=b+kn$). Załóżmy, że dla każdej klasy abstrakcji wybraliśmy (dowolnie) dokładnie jednego reprezentanta. Łatwo np. sprawdzić, że za reprezentanta $[f]$ można wybrać 0. Działania w $R[x]/(f)$ przeprowadzamy teraz w ten sposób - chcąc dodać dwa elementy $[g]$ i $[h]$ bierzemy ich reprezentantów, dodajemy ich do siebie otrzymując wielomian r, a następnie szukamy reprezentanta r; analogicznie z mnożeniem.

Aby podać konkretny przykład, rozważmy następujący sposób zdefiniowania liczb zespolonych. Wielomian $f(x)=x^2+1$ nie ma pierwiastków rzeczywistych. Rozważmy teraz pierścień wielomianów modulo f, $\mathbb{R}[x]/(f)$. Jakiej postaci są jego elementy? Nietrudno udowodnić (np. przez indukcję po stopniu wielomianu), że każdy wielomian $g\in\mathbb{R}[x]$ jest równoważny wielomianowi postaci $a+bx$ i wszystkie wielomiany tej postaci są parami nierównoważne. Wybierzmy więc wszystkie wielomiany postaci $a+bx$ jako reprezentantów. Dodawanie jest oczywiste, jak wygląda mnożenie? Niech $[g]=a+bx, [h]=c+dx$, mamy wtedy:

$$[g]\cdot[h]=[(a+bx)(c+dx)]=[ac+(ad+bc)x+bdx^2]=(ac-bd)+(ad+bc)x$$

gdzie skorzystaliśmy z relacji $x^2=-1$, więc $[x^2+1]=[0]\Rightarrow[x^2]=[-1]$. Oczywiście nietrudno zauważyć, że utożsamiając $[x]\in\mathbb{R}[x]/(f)$ z $i=\sqrt{-1}$ otrzymujemy standardową strukturę liczb zespolonych.

W ramach ćwiczenia możesz się zastanowić, co się stanie, gdy jako f weźmiemy wielomian mający pierwiastki w $\mathbb{R}$, np. $f=(x-1)(x-2)$. Czy $\mathbb{R}[x]/(f)$ będzie wtedy ciałem? (wskazówka: jeśli K jest ciałem oraz dla $a,b\in K$ mamy $a\cdot b=0$, to $a=0$ lub $b=0$)