Matrice u Isabelle

Propratni materijal

Zorana Gajić
zorana.gajic.zg@gmail.com

15. avgust 2019

Definisanje tipa

```
type_synonym mat2 = "int × int × int × int"
type_synonym mat3 = "int × int × int × int × int × int × int × int × int"
```

Definisanje konkretne matrice

```
definition test_matrix3 :: "mat3" where
  "test_matrix3 = (6,1,1,4,-2,5,2,8,7)"
```

Jednakost matrica

```
fun jednakost :: "mat3 ⇒ mat3 ⇒ bool" where
  "jednakost (a11, a12, a13, a21, a22, a23, a31, a32, a33)
             (b11, b12, b13, b21, b22, b23, b31, b32, b33) =
    (a11 = b11 ∧ a12 = b12 ∧ a13 = b13 ∧
     a21 = b21 ∧ a22 = b22 ∧ a23 = b23 ∧
     a31 = b31 ∧ a32 = b32 ∧ a33 = b33)"
```

Svojstva jednakosti matrica

1. $A = A$ *(Refleksivnost)*

```
lemma "jednakost A A"
  by (induction A) auto
```

2. $A = B \iff B = A$ *(Simetričnost)*

```
lemma "jednakost A B ↔ jednakost B A"
  by (induction A B rule: jednakost.induct) auto
```

3. $A = B, B = C \implies A = C$ *(Tranzitivnost)*

```
lemma "jednakost A B ∧ jednakost B C ⟶ jednakost A C"
  by (induction A B rule: jednakost.induct) auto
```

Sabiranje matrica

```
fun plus :: "mat3 ⇒ mat3 ⇒ mat3" where
  "zbir (a11, a12, a13, a21, a22, a23, a31, a32, a33)
        (b11, b12, b13, b21, b22, b23, b31, b32, b33) =
        (a11 + b11, a12 + b12, a13 + b13,
         a21 + b21, a22 + b22, a23 + b23,
         a31 + b31, a32 + b32, a33 + b33)"
```

Svojstva sabiranja matrica

1. $A + 0 = A$

```
lemma "zbir A (0,0,0,0,0,0,0,0,0) = A"
  by (induction A) auto
```

2. $A + B = B + A$ *(Komutativnost)*

```
lemma
  shows "zbir (a11, a12, a13, a21, a22, a23, a31, a32, a33)
              (b11, b12, b13, b21, b22, b23, b31, b32, b33)
            = zbir (b11, b12, b13, b21, b22, b23, b31, b32, b33)
                   (a11, a12, a13, a21, a22, a23, a31, a32, a33)"
proof -
  have "zbir (a11, a12, a13, a21, a22, a23, a31, a32, a33)
             (b11, b12, b13, b21, b22, b23, b31, b32, b33) =
           (a11 + b11, a12 + b12, a13 + b13,
            a21 + b21, a22 + b22, a23 + b23,
            a31 + b31, a32 + b32, a33 + b33)"
    by auto
  hence "... =  (b11 + a11, b12 + a12, b13 + a13,
                 b21 + a21, b22 + a22, b23 + a23,
                 b31 + a31, b32 + a32, b33 + a33)"
    by auto
  hence "...  = zbir (b11, b12, b13, b21, b22, b23, b31, b32, b33)
                     (a11, a12, a13, a21, a22, a23, a31, a32, a33)"
    by auto
  from this show ?thesis by auto
qed
```

3. $(A + B) + C = A + (B + C)$ *(Asocijativnost)*

```
lemma
  shows "zbir (zbir (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                    (b11, b12, b13, b21, b22, b23, b31, b32, b33))
              (c11, c12, c13, c21, c22, c23, c31, c32, c33)
        = zbir (a11, a12, a13, a21, a22, a23, a31, a32, a33)
               (zbir (b11, b12, b13, b21, b22, b23, b31, b32, b33)
                     (c11, c12, c13, c21, c22, c23, c31, c32, c33))"
proof -
  have "zbir
             (zbir (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                   (b11, b12, b13, b21, b22, b23, b31, b32, b33))
             (c11, c12, c13, c21, c22, c23, c31, c32, c33) =
          zbir (a11 + b11, a12 + b12, a13 + b13,
                a21 + b21, a22 + b22, a23 + b23,
                a31 + b31, a32 + b32, a33 + b33) (c11, c12, c13, c21, c22, c23,
                                                  c31, c32, c33)"
    by auto
  hence "... = (a11 + b11 + c11, a12 + b12 + c12, a13 + b13 + c13,
                a21 + b21 + c21, a22 + b22 + c22, a23 + b23 + c23,
                a31 + b31 + c31, a32 + b32 + c32, a33 + b33 + c33)"
    by auto
  hence "... = zbir (a11, a12, a13,
                     a21, a22, a23,
                     a31, a32, a33) (b11 + c11, b12 + c12, b13 + c13,
                                     b21 + c21, b22 + c22, b23 + c23,
                                     b31 + c31, b32 + c32, b33 + c33)"
    by auto
  hence "... = zbir (a11, a12, a13,
                     a21, a22, a23,
                     a31, a32, a33)
                     (zbir (b11, b12, b13, b21, b22, b23, b31, b32, b33)
                           (c11, c12, c13, c21, c22, c23, c31, c32, c33))"
    by auto
  from this show ?thesis by auto
qed
```

4. $A + (-A) = 0$ *(Suprotna matrica)*

```
fun suprotna :: "mat3 ⇒ mat3" where
  "suprotna (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
            (-a11, -a12, -a13, -a21, -a22, -a23, -a31, -a32, -a33)"

lemma "zbir A (suprotna A) = (0,0,0,0,0,0,0,0,0)"
  by (induction A) auto
```

Množenje matrica

```
fun mnozenje2 :: "mat2 ⇒ mat2 ⇒ mat2" where
  "mnozenje2 (a11, a12, a21, a22) (b11, b12, b21, b22) =
      (a11*b11 + a12*b21, a11*b12 + a12*b22, a21*b11 + a22*b21, a21*b12 + a22*b22)"

fun mnozenje :: "mat3 ⇒ mat3 ⇒ mat3" where
  "mnozenje (a11, a12, a13, a21, a22, a23, a31, a32, a33)
            (b11, b12, b13, b21, b22, b23, b31, b32, b33) =

(a11*b11 + a12*b21 + a13*b31, a11*b12 + a12*b22 + a13*b32, a11*b13 + a12*b23 + a13*b33,
 a21*b11 + a22*b21 + a23*b31, a21*b12 + a22*b22 + a23*b32, a21*b13 + a22*b23 + a23*b33,
 a31*b11 + a32*b21 + a33*b31, a31*b12 + a32*b22 + a33*b32, a31*b13 + a32*b23 + a33*b33)"
```

Svojstva množenja matrica

1. $A * (B + C) = A * B + A * C$

```
lemma
  shows "mnozenje (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                  (zbir (b11, b12, b13, b21, b22, b23, b31, b32, b33)
                        (c11, c12, c13, c21, c22, c23, c31, c32, c33)) =
          zbir (mnozenje (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                         (b11, b12, b13, b21, b22, b23, b31, b32, b33))
               (mnozenje (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                         (c11, c12, c13, c21, c22, c23, c31, c32, c33))"
proof -
  have "mnozenje (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                 (zbir (b11, b12, b13, b21, b22, b23, b31, b32, b33)
                       (c11, c12, c13, c21, c22, c23, c31, c32, c33)) =
        mnozenje (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                 (b11 + c11, b12 + c12, b13 + c13,
                  b21 + c21, b22 + c22, b23 + c23,
                  b31 + c31, b32 + c32, b33 + c33)"
    by auto
  hence "... = (a11*(b11 + c11) + a12*(b21 + c21) + a13*(b31 + c31),
               a11*(b12 + c12) + a12*(b22 + c22) + a13*(b32 + c32),
               a11*(b13 + c13) + a12*(b23 + c23) + a13*(b33 + c33),

               a21*(b11 + c11) + a22*(b21 + c21) + a23*(b31 + c31),
               a21*(b12 + c12) + a22*(b22 + c22) + a23*(b32 + c32),
               a21*(b13 + c13) + a22*(b23 + c23) + a23*(b33 + c33),

               a31*(b11 + c11) + a32*(b21 + c21) + a33*(b31 + c31),
               a31*(b12 + c12) + a32*(b22 + c22) + a33*(b32 + c32),
               a31*(b13 + c13) + a32*(b23 + c23) + a33*(b33 + c33))"
    by auto
  hence "... = (a11*b11 + a11*c11 + a12*b21 + a12*c21 + a13*b31 + a13*c31,
               a11*b12 + a11*c12 + a12*b22 + a12*c22 + a13*b32 + a13*c32,
               a11*b13 + a11*c13 + a12*b23 + a12*c23 + a13*b33 + a13*c33,

               a21*b11 + a21*c11 + a22*b21 + a22*c21 + a23*b31 + a23*c31,
               a21*b12 + a21*c12 + a22*b22 + a22*c22 + a23*b32 + a23*c32,
               a21*b13 + a21*c13 + a22*b23 + a22*c23 + a23*b33 + a23*c33,

               a31*b11 + a31*c11 + a32*b21 + a32*c21 + a33*b31 + a33*c31,
               a31*b12 + a31*c12 + a32*b22 + a32*c22 + a33*b32 + a33*c32,
               a31*b13 + a31*c13 + a32*b23 + a32*c23 + a33*b33 + a33*c33)"
    by (simp add: algebra_simps)
  hence "... = zbir (a11*b11 + a12*b21 + a13*b31,
                    a11*b12 + a12*b22 + a13*b32,
```

```
                      a11*b13 + a12*b23 + a13*b33,

                      a21*b11 + a22*b21 + a23*b31,
                      a21*b12 + a22*b22 + a23*b32,
                      a21*b13 + a22*b23 + a23*b33,

                      a31*b11 + a32*b21 + a33*b31,
                      a31*b12 + a32*b22 + a33*b32,
                      a31*b13 + a32*b23 + a33*b33)

                     (a11*c11 + a12*c21 + a13*c31,
                      a11*c12 + a12*c22 + a13*c32,
                      a11*c13 + a12*c23 + a13*c33,

                      a21*c11 + a22*c21 + a23*c31,
                      a21*c12 + a22*c22 + a23*c32,
                      a21*c13 + a22*c23 + a23*c33,

                      a31*c11 + a32*c21 + a33*c31,
                      a31*c12 + a32*c22 + a33*c32,
                      a31*c13 + a32*c23 + a33*c33)"
    by auto
  hence "... =  zbir (mnozenje (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                               (b11, b12, b13, b21, b22, b23, b31, b32, b33))
                      (mnozenje (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                               (c11, c12, c13, c21, c22, c23, c31, c32, c33))"
    by auto
  from this show ?thesis by (simp add: algebra_simps)
qed
```

2. $\alpha(AB) = (\alpha A)B$

```
lemma
  fixes x:: "int"
  shows "mnozenje_brojem x (mnozenje (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                                     (b11, b12, b13, b21, b22, b23, b31, b32, b33))
    =
         mnozenje (mnozenje_brojem x (a11, a12, a13, a21, a22, a23, a31, a32, a33))
                  (b11, b12, b13, b21, b22, b23, b31, b32, b33)"
proof -
  have "mnozenje_brojem x
                  (mnozenje (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                            (b11, b12, b13, b21, b22, b23, b31, b32, b33)) =
        mnozenje_brojem x
          (a11*b11 + a12*b21 + a13*b31,
           a11*b12 + a12*b22 + a13*b32,
           a11*b13 + a12*b23 + a13*b33,

           a21*b11 + a22*b21 + a23*b31,
           a21*b12 + a22*b22 + a23*b32,
           a21*b13 + a22*b23 + a23*b33,

           a31*b11 + a32*b21 + a33*b31,
           a31*b12 + a32*b22 + a33*b32,
           a31*b13 + a32*b23 + a33*b33)"
    by auto
  hence "... = (x*a11*b11 + x*a12*b21 + x*a13*b31,
                x*a11*b12 + x*a12*b22 + x*a13*b32,
                x*a11*b13 + x*a12*b23 + x*a13*b33,

                x*a21*b11 + x*a22*b21 + x*a23*b31,
                x*a21*b12 + x*a22*b22 + x*a23*b32,
                x*a21*b13 + x*a22*b23 + x*a23*b33,

                x*a31*b11 + x*a32*b21 + x*a33*b31,
                x*a31*b12 + x*a32*b22 + x*a33*b32,
                x*a31*b13 + x*a32*b23 + x*a33*b33)"
    by (simp add: algebra_simps)
  hence "... = mnozenje
                  (mnozenje_brojem x (a11, a12, a13, a21, a22, a23, a31, a32, a33))
                                     (b11, b12, b13, b21, b22, b23, b31, b32, b33)"
```

```
    by (simp add: algebra_simps)
  from this show ?thesis by (simp add: algebra_simps)
qed
```

Množenje matrice brojem

```
fun mnozenje_brojem :: "int ⇒ mat3 ⇒ mat3" where
  "mnozenje_brojem x (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
       (x*a11, x*a12, x*a13, x*a21, x*a22, x*a23, x*a31, x*a32, x*a33)"
```

Svojstva množenja matrice brojem

1. $1 * A = A$ *(Neutral za množenje)*

```
definition eye :: "mat3" where
  "eye = (1,0,0,0,1,0,0,0,1)"

lemma "mnozenje eye (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
                    (a11, a12, a13, a21, a22, a23, a31, a32, a33)"
  by (simp add: eye_def)
```

2. $0 * A = A$

```
lemma "mnozenje (0,0,0,0,0,0,0,0,0) A = (0,0,0,0,0,0,0,0,0)"
  by (induction A) auto
```

3. $\alpha A = A\alpha$ *(Komutativnost)*

```
fun mnozenje_brojem_desno :: "mat3 ⇒ int ⇒ mat3" where
  "mnozenje_brojem_desno (a11, a12, a13, a21, a22, a23, a31, a32, a33) x =
       (x*a11, x*a12, x*a13, x*a21, x*a22, x*a23, x*a31, x*a32, x*a33)"

lemma "mnozenje_brojem x A = mnozenje_brojem_desno A x"
  by (induction A) auto
```

4. $(\alpha\beta)A = \alpha(\beta A)$ *(Asocijativnost)*

```
lemma
  shows "mnozenje_brojem (x*y) (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
          mnozenje_brojem x
                  (mnozenje_brojem y (a11, a12, a13, a21, a22, a23, a31, a32, a33))
    "
proof -
  have "mnozenje_brojem (x*y) (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
        ((x*y)*a11, (x*y)*a12, (x*y)*a13,
         (x*y)*a21, (x*y)*a22, (x*y)*a23,
         (x*y)*a31, (x*y)*a32, (x*y)*a33)"
    by auto
  hence "... = (x*(y*a11), x*(y*a12), x*(y*a13),
                x*(y*a21), x*(y*a22), x*(y*a23),
                x*(y*a31), x*(y*a32), x*(y*a33))"
    by auto
  hence "... = mnozenje_brojem x
                (y*a11, y*a12, y*a13, y*a21, y*a22, y*a23, y*a31, y*a32, y*a33)"
    by auto
  hence "... = mnozenje_brojem x
                (mnozenje_brojem y (a11, a12, a13, a21, a22, a23, a31, a32, a33))"
    by auto
  from this show ?thesis by auto
qed
```

5. $(\alpha + \beta)A = \alpha A + \beta B$ *(Distributivnost s obzirom na zbir brojeva)*

```
lemma
  assumes "x ≠ 0" "y ≠ 0"
  shows "mnozenje_brojem (x + y) (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
          zbir (mnozenje_brojem x (a11, a12, a13, a21, a22, a23, a31, a32, a33))
               (mnozenje_brojem y (a11, a12, a13, a21, a22, a23, a31, a32, a33))"
  using assms
proof -
  have "mnozenje_brojem (x + y) (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
                ((x+y)*a11, (x+y)*a12, (x+y)*a13,
                 (x+y)*a21, (x+y)*a22, (x+y)*a23,
                 (x+y)*a31, (x+y)*a32, (x+y)*a33)"
    by auto
  hence "... =  (x*a11 + y*a11, x*a12 + y*a12, x*a13 + y*a13,
                 x*a21 + y*a21, x*a22 + y*a22, x*a23 + y*a23,
                 x*a31 + y*a31, x*a32 + y*a32, x*a33 + y*a33)"
    by (simp add: algebra_simps)
  hence "... =
           zbir (x*a11, x*a12, x*a13, x*a21 , x*a22, x*a23, x*a31, x*a32, x*a33)
                (y*a11, y*a12, y*a13, y*a21 , y*a22, y*a23, y*a31, y*a32, y*a33)"
    by auto
  hence "... = zbir
              (mnozenje_brojem x (a11, a12, a13, a21, a22, a23, a31, a32, a33))
              (mnozenje_brojem y (a11, a12, a13, a21, a22, a23, a31, a32, a33))"
    by auto
  from this show ?thesis by (simp add: algebra_simps)
qed
```

6. $\alpha(A + B) = \alpha A + \alpha B$ *(Distributivnost s obzirom na zbir matrica)*

```
lemma
  shows "mnozenje_brojem x (zbir (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                                 (b11, b12, b13, b21, b22, b23, b31, b32, b33)) =
         zbir
              (mnozenje_brojem x (a11, a12, a13, a21, a22, a23, a31, a32, a33))
              (mnozenje_brojem x (b11, b12, b13, b21, b22, b23, b31, b32, b33))"
proof -
  have "mnozenje_brojem x (zbir (a11, a12, a13, a21, a22, a23, a31, a32, a33)
                                (b11, b12, b13, b21, b22, b23, b31, b32, b33)) =
        mnozenje_brojem x (a11 + b11, a12 + b12, a13 + b13,
                           a21 + b21, a22 + b22, a23 + b23,
                           a31 + b31, a32 + b32, a33 + b33)"
    by auto
  hence "... = (x*(a11 + b11), x*(a12 + b12), x*(a13 + b13),
                x*(a21 + b21), x*(a22 + b22), x*(a23 + b23),
                x*(a31 + b31), x*(a32 + b32), x*(a33 + b33))"
    by auto
  hence "... = (x*a11 + x*b11, x*a12 + x*b12, x*a13 + x*b13,
                x*a21 + x*b21, x*a22 + x*b22, x*a23 + x*b23,
                x*a31 + x*b31, x*a32 + x*b32, x*a33 + x*b33)"
    by (simp add: algebra_simps)
  hence "... = zbir
                 (x*a11, x*a12, x*a13, x*a21, x*a22, x*a23, x*a31, x*a32, x*a33)
                 (x*b11, x*b12, x*b13, x*b21, x*b22, x*b23, x*b31, x*b32, x*b33)"
    by auto
  hence "... = zbir
              (mnozenje_brojem x (a11, a12, a13, a21, a22, a23, a31, a32, a33))
              (mnozenje_brojem x (b11, b12, b13, b21, b22, b23, b31, b32, b33))"
    by auto
  from this show ?thesis by (simp add: algebra_simps)
qed
```

Determinanta 2x2 matrice

```
fun det2 :: "mat2  ⇒  int" where
  "det2 (a11,a12,a21,a22) = a11*a22 - a21*a12"
```

Determinanta 3x3 matrice

```
fun det3 :: "mat3  ⇒  int" where
  "det3 (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
      a11*a22*a33 - a11*a23*a32 - a12*a21*a33 +
      a12*a23*a31 + a13*a21*a32 - a13*a22*a31"
```

Determinanta 3x3 matrice metodom razvijanja po vrsti

```
fun det3_vrsta :: "mat3  ⇒  int" where
  "det3_vrsta (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
      a11*det2(a22,a23,a32,a33) - a12*det2(a21,a23,a31,a33) + a13*det2(a21,a22,a31,a32)"
```

Determinanta 3x3 matrice metodom razvijanja po koloni

```
fun det3_kolona :: "mat3  ⇒  int" where
  "det3_kolona (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
      a11*det2(a22,a23,a32,a33) - a21*det2(a12,a13,a32,a33) + a31*det2(a12,a13,a22,a23)"
```

Transponovana matrica

```
fun transponovana2 :: "mat2  ⇒   mat2" where
  "transponovana2 (a11, a21, a12, a22) = (a11, a21, a12, a22)"

fun transponovana :: "mat3  ⇒  mat3" where
  "transponovana (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
         (a11, a21, a31, a12, a22, a32, a13, a23, a33)"
```

Svojstva determinanata

1. Prilikom transponovanja matrice determinanta se ne menja

```
lemma det_trans:
  shows "det3 (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
          det3 (transponovana (a11, a12, a13, a21, a22, a23, a31, a32, a33))"
proof -
  have "det3 (a11, a12, a13, a21, a22, a23, a31, a32, a33) =
          det3 (a11, a21, a31, a12, a22, a32, a13, a23, a33)"
    by auto
  also have "... = a11*a22*a33 - a11*a23*a32 - a12*a21*a33 +
      a12*a23*a31 + a13*a21*a32 - a13*a22*a31"
    by auto
  also have "... = det3 (transponovana (a11, a21, a31, a12, a22, a32, a13, a23, a33
    ))"
    by auto
  from this show ?thesis by auto
qed
```

2. Ako elementi dva paralelna reda zamene mesta promeniće se znak determinante

```
lemma
  shows "det2 (a11, a12, a21, a22) = - det2 (a21,a22,a11,a12)"
proof -
  have "det2 (a11, a12, a21, a22) = a11*a22 - a12*a21"
    by auto
  also have "... = - (a12*a21 - a11*a22)"
    by auto
  also have "... = - det2 (a21,a22,a11,a12)"
    by auto
  from this show ?thesis by auto
qed
```

Svojstva transponovanih matrica

1. $(A^T)^T = A$

```
lemma "transponovana (transponovana A) = A"
  by (induction A rule: transponovana.induct) auto
```

2. $(A + B)^T = A^T + B^T$

```
lemma "transponovana (zbir A B) = zbir (transponovana A) (transponovana B)"
  by (induction A B rule: zbir.induct) auto
```

3. $(\lambda A)^T = \lambda A^T$

```
lemma "transponovana (mnozenje_brojem x A) = mnozenje_brojem x (transponovana A)"
  by (induction A) auto
```

4. $(AB)^T = B^T A^T$

```
lemma "transponovana (mnozenje A B) = mnozenje (transponovana B) (transponovana A)"
  by (induction A B rule: mnozenje.induct) auto
```

Gramova matrica: $GramA = A * A^T$

```
fun gramova :: "mat2 ⇒ mat2" where
  "gramova A = mnozenje2 A (transponovana2 A)"
```

Dokaz da je determinanta Gramove matrice uvek pozitivna vrednost

Radi jednostavnosti dokazaćemo za matrice dimenzija 2x2. Neophodna je pomoćna lema koja dokazuje narednu osobinu: $det(AB) = detA * detB$

```
lemma det_kroz_mnozenje:
  shows "det2 (mnozenje2 (a,b,c,d) (p,q,r,s)) = det2 (a,b,c,d) * det2 (p,q,r,s)"
proof -
  have "det2 (mnozenje2 (a,b,c,d) (p,q,r,s)) = det2 (a*p + b*r, a*q + b*s, c*p + d*r, c*
    q + d*s)"
    by auto
  also have "... = (a*p + b*r)*(c*q + d*s) - (c*p + d*r)*(a*q + b*s)"
    by auto
  also have "... = a*p*c*q + a*p*d*s + b*r*c*q + b*r*d*s - c*p*a*q - c*p*b*s - d*r*a*q -
     d*r*b*s"
    by (simp add: algebra_simps)
  also have "... = a*p*d*s + b*r*c*q - c*p*b*s - d*r*a*q"
    by auto
  also have "... = (a*d - c*b)*(p*s - r*q)"
    by (simp add: algebra_simps)
  also have "... = det2 (a,b,c,d) * det2 (p,q,r,s)"
    by (simp add: algebra_simps)
  from this show ?thesis
    using calculation by auto
qed

find_theorems "_ ^ 2 > 0"

lemma
  assumes "det2 A ≠ 0"
  shows "det2 (gramova A) > 0"
proof -
  have "det2 (gramova A) = det2 (mnozenje2 A (transponovana2 A))"
    by auto
  also have "... = (det2 A) * (det2 (transponovana2 A))"
    using det_kroz_mnozenje
    by (metis transponovana2.elims)
```

```
  also have "... = (det2 A) * (det2 A)"
    using det_trans
    by (metis det2.simps mult.commute transponovana2.elims)
  also have "... = (det2 A) ^ 2"
    by (simp add: power2_eq_square)
  also have "... > 0"
    using assms
    by (simp add: zero_less_power2)
  from this show ?thesis
    using calculation by linarith
qed
```

Zadatak: Dokazati da važi naredna jednakost:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

Neophodno je definisati matricu i operacije tako da se radi sa prirodnim brojevima. Prvo se definiše matrica sa prirodnim brojevima, jedinična matrica i množenje matrica 2x2.

```
type_synonym mat2_nat = "nat × nat × nat × nat"

definition eye2 :: mat2_nat where
  "eye2 = (1, 0, 0, 1)"

fun mnozenje2_nat :: "mat2_nat ⇒ mat2_nat ⇒ mat2_nat" where
 "mnozenje2_nat (a11, a12, a21, a22) (b11, b12, b21, b22) =
     (a11*b11 + a12*b21, a11*b12 + a12*b22, a21*b11 + a22*b21, a21*b12 + a22*b22)"
```

Zatim rekurzivna definicija određivanja matrice na n-ti stepen i sama lema.

```
primrec stepen2_nat :: "mat2_nat ⇒ nat ⇒ mat2_nat" where
  "stepen2_nat A 0 = eye2" |
  "stepen2_nat A (Suc n) = mnozenje2_nat A (stepen2_nat A n)"

lemma "stepen2_nat (1, 1, 0, 1) n = (1, n, 0, 1)"
proof (induction n)
case 0
  then show ?case
    by (simp only: stepen2_nat.simps(1) eye2_def)
next
  case (Suc n)
  then show ?case
  proof -
    have
    "stepen2_nat (1,1,0,1) (Suc n) = mnozenje2_nat (1,1,0,1) (stepen2_nat (1,1,0,1) n)"
      by (simp only: stepen2_nat.simps(2))
    also have "... = mnozenje2_nat (1,1,0,1) (1,n,0,1)"
      using Suc by simp
    also have "... = (1, n+1, 0, 1)"
      by simp
    finally show ?thesis by simp
  qed
qed
```

Inverz matrice 2x2

Sada se prelazi na rad sa racionalnim brojevima. Definišu se tipovi i neophodne funkcije

```
type_synonym mat2_rat = "rat  ×  rat  ×  rat  ×  rat"

fun det2_rat :: "mat2_rat  ⇒  rat" where
  "det2_rat (a11,a12,a21,a22) = a11*a22 - a12*a21"

fun mnozenje_brojem2_rat :: "rat  ⇒  mat2_rat  ⇒  mat2_rat" where
  "mnozenje_brojem2_rat x (a,b,c,d) = (x*a, x*b, x*c, x*d)"

fun inverse2_rat :: "mat2_rat  ⇒  mat2_rat" where
  "inverse2_rat (a,b,c,d) = mnozenje_brojem2_rat (1/(det2_rat (a,b,c,d))) (d, -b, -c, a)
    "

fun mnozenje2_rat :: "mat2_rat  ⇒  mat2_rat  ⇒  mat2_rat" where
  "mnozenje2_rat (a11, a12, a21, a22) (b11, b12, b21, b22) =
      (a11*b11 + a12*b21, a11*b12 + a12*b22, a21*b11 + a22*b21, a21*b12 + a22*b22)"
```

Svojstva inverza matrica

1. $(A^{-1})^{-1} = A$

```
lemma
  shows "inverse2_rat (mnozenje2_rat A B) =
            mnozenje2_rat (inverse2_rat B) (inverse2_rat A)"
proof -
  have "mnozenje2_rat (mnozenje2_rat A B)
                      (inverse2_rat (mnozenje2_rat A B)) = (1,0,0,1)"
     using inverse_mnozenje_desno
     by (metis inverse2_rat.elims)
    hence "mnozenje2_rat (inverse2_rat A)
                      (mnozenje2_rat (mnozenje2_rat A B)
                                   (inverse2_rat (mnozenje2_rat A B))) =
    mnozenje2_rat (inverse2_rat A) (1,0,0,1)"
     by metis
    hence "mnozenje2_rat (mnozenje2_rat (inverse2_rat A) A)
                      (mnozenje2_rat B (inverse2_rat (mnozenje2_rat A B))) =
    inverse2_rat A"
     using asoc_mnozenje_desno
     by (metis <mnozenje2_rat (mnozenje2_rat A B) (inverse2_rat (mnozenje2_rat A B)
    ) = (1, 0, 0, 1)> old.prod.inject prod_cases4 surj_pair)

    hence "mnozenje2_rat (1,0,0,1)
                      (mnozenje2_rat B (inverse2_rat (mnozenje2_rat A B))) =
    inverse2_rat A"
     using asoc_mnozenje_desno
     by (metis mnozenje2_rat.elims)
    hence "mnozenje2_rat B (inverse2_rat (mnozenje2_rat A B)) = inverse2_rat A"
     using asoc_mnozenje_desno neutral_mnozenje2_rat
     by metis
    hence "mnozenje2_rat (mnozenje2_rat (inverse2_rat B) B)
                      (inverse2_rat (mnozenje2_rat A B)) =
          mnozenje2_rat (inverse2_rat B) (inverse2_rat A)"
     by (metis mnozenje2_rat.elims)
    hence "mnozenje2_rat (1,0,0,1) (inverse2_rat (mnozenje2_rat A B)) =
        mnozenje2_rat (inverse2_rat B) (inverse2_rat A)"
     using inverse_mnozenje_levo
     by (metis mnozenje2_rat.elims)
    hence "inverse2_rat (mnozenje2_rat A B) =
        mnozenje2_rat (inverse2_rat B) (inverse2_rat A)"
     using asoc_mnozenje_desno
     by (metis mnozenje2_rat.elims)
    from this show ?thesis by simp
 qed
```

Pomoćne leme:

(a) $AA^{-1} = E$

```
  lemma inverse_mnozenje_desno:
  assumes "det2_rat (a,b,c,d) ≠ 0"
  shows "mnozenje2_rat (a,b,c,d) (inverse2_rat (a,b,c,d)) = (1,0,0,1)"
proof -
  have "mnozenje2_rat (a,b,c,d) (inverse2_rat (a,b,c,d)) =
          mnozenje2_rat (a,b,c,d)
             (mnozenje_brojem2_rat (1/(det2_rat (a,b,c,d))) (d, -b, -c, a))"
    by auto
  also have "... = mnozenje2_rat (a,b,c,d)
  (d/(det2_rat (a,b,c,d)), -b/(det2_rat (a,b,c,d)), -c/(det2_rat (a,b,c,d)), a
    /(det2_rat (a,b,c,d)))"
    by auto
  also have "... = mnozenje2_rat (a,b,c,d)
    (d/(a*d-b*c), -b/(a*d-b*c), -c/(a*d-b*c), a/(a*d-b*c))"
    by auto
  also have "... = (a*d/(a*d-b*c) - b*c/(a*d-b*c),
                    (-a)*b/(a*d-b*c) + a*b/(a*d-b*c),
                    c*d/(a*d-b*c) - c*d/(a*d-b*c),
                    c*(-b)/(a*d-b*c) + a*d/(a*d-b*c))"
    by auto
  also have "... = ((a*d-b*c)/(a*d-b*c), (a*b-a*b)/(a*d-b*c), (c*d-c*d)/(a*d-b
    *c), (a*d-b*c)/(a*d-b*c))"
    by (smt add_divide_distrib diff_divide_distrib mult.commute mult_minus_
    left uminus_add_conv_diff)
  also have "... = (1,0,0,1)"
    using assms
    by auto
  finally show ?thesis by simp
qed
```

(b) $A(BC) = (AB)C$

```
  lemma asoc_mnozenje_desno:
  shows "mnozenje2_rat (a11,a12,a21,a22)
                        (mnozenje2_rat (b11,b12,b21,b22) (c11,c12,c21,c22)) =
  mnozenje2_rat (mnozenje2_rat (a11,a12,a21,a22)
                               (b11,b12,b21,b22)) (c11,c12,c21,c22)"
proof -
  have "mnozenje2_rat (a11,a12,a21,a22)
                      (mnozenje2_rat (b11,b12,b21,b22) (c11,c12,c21,c22)) =
        mnozenje2_rat (a11,a12,a21,a22)
 (b11*c11+b12*c21, b11*c12 + b12*c22, b21*c11 + b22*c21, b21*c12 + b22*c22)"
    by auto
  also have "... = (a11*(b11*c11+b12*c21) + a12*(b21*c11+b22*c21),
                    a11*(b11*c12+b12*c22) + a12*(b21*c12+b22*c22),
                    a21*(b11*c11+b12*c21) + a22*(b21*c11+b22*c21),
                    a21*(b11*c12+b12*c22) + a22*(b21*c12+b22*c22))"
    by auto
  also have "... = (a11*b11*c11 + a11*b12*c21 + a12*b21*c11 + a12*b22*c21,
                    a11*b11*c12 + a11*b12*c22 + a12*b21*c12 + a12*b22*c22,
                    a21*b11*c11 + a21*b12*c21 + a22*b21*c11 + a22*b22*c21,
                    a21*b11*c12 + a21*b12*c22 + a22*b21*c12 + a22*b22*c22)"
    by (simp add: algebra_simps)
  also have "... = ((a11*b11 + a12*b21)*c11 + (a11*b12 + a12*b22)*c21,
                    (a11*b11 + a12*b21)*c12 + (a11*b12 + a12*b22)*c22,
                    (a21*b11 + a22*b21)*c11 + (a21*b12 + a22*b22)*c21,
                    (a21*b11 + a22*b21)*c12 + (a21*b12 + a22*b22)*c22)"
    by (simp add: algebra_simps)
  also have "... = mnozenje2_rat
                   (a11*b11 + a12*b21, a11*b12 + a12*b22,
                    a21*b11 + a22*b21, a21*b12 + a22*b22) (c11, c12, c21, c22)
    "
    by (simp add: algebra_simps)
  also have "... =  mnozenje2_rat (mnozenje2_rat (a11,a12,a21,a22)
                                                 (b11,b12,b21,b22))
                                 (c11,c12,c21,c22)"
    by auto
```

```
  finally show ?thesis by simp
qed
```

(c) $A * E = A$

```
  lemma neutral_mnozenje2_rat:
      shows "mnozenje2_rat (1,0,0,1) A = A"
      by (induction A) auto
```

(d) $A^{-1}A = E$

```
  lemma inverse_mnozenje_levo:
  assumes "det2_rat (a,b,c,d) ≠ 0"
  shows "mnozenje2_rat (inverse2_rat (a,b,c,d)) (a,b,c,d) = (1,0,0,1)"
proof -
  have "mnozenje2_rat (inverse2_rat (a,b,c,d)) (a,b,c,d) =
        mnozenje2_rat (mnozenje_brojem2_rat (1/(det2_rat (a,b,c,d)))
                                          (d, -b, -c, a))
                      (a,b,c,d)"
    by auto
  also have "... = mnozenje2_rat
    (d/(det2_rat (a,b,c,d)), -b/(det2_rat (a,b,c,d)), -c/(det2_rat (a,b,c,d)),
     a/(det2_rat (a,b,c,d)))
    (a,b,c,d)"
    by auto
  also have "... = mnozenje2_rat
    (d/(a*d-b*c), -b/(a*d-b*c), -c/(a*d-b*c), a/(a*d-b*c))
    (a,b,c,d)"
    by auto
  also have "... = (a*d/(a*d-b*c) - b*c/(a*d-b*c),
                    (-a)*b/(a*d-b*c) + a*b/(a*d-b*c),
                    c*d/(a*d-b*c) - c*d/(a*d-b*c),
                    c*(-b)/(a*d-b*c) + a*d/(a*d-b*c))"
    by auto
  also have "... = ((a*d-b*c)/(a*d-b*c), (a*b-a*b)/(a*d-b*c), (c*d-c*d)/(a*d-b
    *c), (a*d-b*c)/(a*d-b*c))"
    by (smt add_divide_distrib diff_divide_distrib mult.commute mult_minus_
    left uminus_add_conv_diff)
  also have "... = (1,0,0,1)"
    using assms
    by auto
  finally show ?thesis by simp
qed
```