Solution to Exercise 1.5.4

Part a): We abbreviate $\zeta := \boldsymbol{\zeta}_n = \boldsymbol{\zeta}_{2k}$. The statements we have to prove follow from the observation that ζ is a root of $X^{2k} - 1$ and ζ^k is a root of $X^k + 1$, i.e., $\zeta^{2k} = 1$ and hence $\zeta^k = -1$. Explicitly

$$\begin{aligned} f(\zeta^{2i}) &= (\zeta^{2ki} - 1) q_1(\zeta^{2i}) + r_1(\zeta^{2i}) \\ &= r_1(\zeta^{2i}) \end{aligned}$$

and

$$\begin{aligned} f(\zeta^{2i+1}) &= (\zeta^{2ik+k} + 1) q_2(\zeta^{2i+1}) + r_2(\zeta^{2i+1}) \\ &= (\zeta^k + 1) q_2(\zeta^{2i+1}) + r_2(\zeta^{2i+1}) \\ &= r_2(\zeta^{2i+1}). \end{aligned}$$

Part b): We use GAP. The problem leaves us a choice for ζ so we choose $\zeta := \zeta_{10}$ since $\deg(f) + \deg(g) < 10$. Since we are not asked to do the transform in the most efficient way, we are going to solve this problem by multiplying the coefficient vectors of f and g first by the the matrix of the discrete Fourier transform DFT with regard to the basis $X^i + ((X^{10} - 1))$, for $i = 0 \ldots, 9$ and the standard basis of $\mathbb{C}^{10}$. In the GAP-code we will generate the matrix of DFT and its inverse IDFT first and then compute the transforms of f and g. Finally, we form their product in the $\mathbb{C}$-algebra $\mathbb{C}^{10}$ and apply the inverse IDFT of the discrete Fourier transform DFT. In the last part we compare the result with regular product of polynomials in GAP.

```
gap> dft10:=List([0..9],x->List([0..9],y->(E(10)^(x*y))));;
gap> dft10i:=1/10*List([0..9],x->List([0..9],y->(E(10)^(-x*y))));
gap> f:=[1,1,3,1,0,0,0,0,0,0];
[ 1, 1, 3, 1, 0, 0, 0, 0, 0, 0 ]
gap> g:=[1,1,3,0,1,0,0,0,0,0];
[ 1, 1, 3, 0, 1, 0, 0, 0, 0, 0 ]
gap> ft:=f*dft10;
[ 6, 2*E(5)-E(5)^2-2*E(5)^3-2*E(5)^4, 2*E(5)^2-E(5)^4,
  -E(5)-2*E(5)^2+2*E(5)^3-2*E(5)^4, -E(5)^3+2*E(5)^4, 2, 2*E(5)-E(5)^2,
  -2*E(5)+2*E(5)^2-2*E(5)^3-E(5)^4, -E(5)+2*E(5)^3,
  -2*E(5)-2*E(5)^2-E(5)^3+2*E(5)^4 ]
gap> gt:=g*dft10;
[ 6, 2*E(5)-2*E(5)^3-E(5)^4, 2*E(5)^2-E(5)^3, -E(5)^2+2*E(5)^3-2*E(5)^4,
  -E(5)+2*E(5)^4, 4, 2*E(5)-E(5)^4, -2*E(5)+2*E(5)^2-E(5)^3, -E(5)^2+2*E(5)^3,
  -E(5)-2*E(5)^2+2*E(5)^4 ]
gap> prod:=List([1..10],x->ft[x]*gt[x]);;
gap> prodi:=prod*dft10i;
[ 1, 2, 7, 7, 11, 4, 3, 1, 0, 0 ]
gap> fp:=UnivariatePolynomial(Rationals,f);
x_1^3+3*x_1^2+x_1+1
gap> gp:=UnivariatePolynomial(Rationals,g);
x_1^4+3*x_1^2+x_1+1
gap> res:=fp*gp;
```

```
x_1^7+3*x_1^6+4*x_1^5+11*x_1^4+7*x_1^3+7*x_1^2+2*x_1+1
gap> CoefficientsOfUnivariatePolynomial(res);
[ 1, 2, 7, 7, 11, 4, 3, 1 ]
```