

MATH 340 Assignment 4, Fall 2007

Michael Monagan

This assignment is due Wednesday October the 17th at the beginning of class. For problems involving Maple, please submit a printout of a Maple worksheet. Late penalty: -20% for up to one day late. Zero for more than one day late.

Section 2.2: Subrings and Subfields

Exercises 1, 3(iv), 6, 7, 8, 14, 16.

Section 2.3: Review of Vector Spaces

Exercises 2, 9.

Also exercise 12 of section 1.7 and exercise 18 of section 2.1.

Section 2.4: Polynomials

Exercises 1, 3, 12, 13, 14, 16.

Do questions 12 and 13 by hand. Check your answers using Maple. For part (i) of questions 12 and 13, use the `quo`, `rem` and `gcd` commands. For parts (ii) and (iii) use the `Quo(...)` mod `p`, `Rem(...)` mod `p` and `Gcd(...)` mod `p` commands.

For question 14 (which will be marked) do not do it by hand. First use the `gcdex(...)` command in Maple to answer part (i) and then the `Gcdex(...)` mod `p` command to answer parts (ii) and (iii). Indicate what the $\lambda(x)$ and $\mu(x)$ polynomials are.

Now use Maple to answer question 14 as follows: Write a loop in Maple that implements the extended Euclidean algorithm to compute the polynomials q_i, r_i, x_i and y_i as illustrated in the table on page 90. Recall from section 1.3 that $r_i = r_{i-2} - q_i r_{i-1}$, $x_i = x_{i-2} - q_i x_{i-1}$ and $y_i = y_{i-2} - q_i y_{i-1}$ where q_i is the quotient of r_{i-2} divided by r_{i-1} . Print out the q_i, r_i, x_i , and y_i polynomials using the `printf` command.

For part (i) use the Maple commands `quo` and `expand` to divide and to multiply polynomials in $\mathbb{Q}[x]$ respectively. For parts (ii) and (iii) use the Maple commands `Quo(...)` mod `p` and `Expand(...)` mod `p` to divide and multiply polynomials in $\mathbb{Z}_p[x]$ respectively. So you need two versions of the code, one for $\mathbb{Q}[x]$ and one for $\mathbb{Z}_p[x]$.