MATH 403 Winter 2018

Homework 4

Winter 2018

1. **Problem 4.2** Greatest common divisors are well defined up to units. So your answer can differ with others by a unit. All the coefficient rings are fields in this problem so we will apply Euclidean algorithm. The procedure is the same throughout the four so I only write out the first.

   (a)

$$\begin{aligned} x^3-6x^2+14x-15-(x^3-8x^2+21x-18) =& 2x^2-7x+3 \\ x^3-8x^2+21x-18-\frac{x}{2}(2x^2-7x+3) =& -\frac{9}{2}x^2+\frac{39}{2}x-18 \\ 2x^2-7x+3+\frac{4}{9}(-\frac{9}{2}x^2+\frac{39}{2}x-18) =& (\frac{5}{3})x-5 \\ -\frac{9}{2}x^2+\frac{39}{2}x-18+\frac{27}{10}x(\frac{5}{3}x-5) =& 6x-18 \\ \frac{3}{5}x-5-\frac{5}{18}(6x-18) =& 0 \end{aligned}$$

   Hence the greatest common divisor is $x-3$. Going backwards, we get $a(x)=\frac{-1}{10}x^2+\frac{11}{30}x$ and $b(x)=\frac{1}{10}x^2-\frac{1}{6}x+\frac{1}{6}$.

   (b) $a(x)=x^2+x+1$ and $b(x)=-x^2$ with greatest common divisor being 1.

   (c) $a(x)=x+4x^2$ and $b=2+x^2$ with greatest common divisor being 1.

   (d) $a(x)=\frac{324}{3007}x^2+\frac{468}{3007}x+\frac{757}{3007}$ and $b(x)=-(\frac{81}{3007}x^2+\frac{117}{3007}x+\frac{7}{3007})$ with greatest common divisor being 1.

2. **Problem 4.3**

   (a) $x^4-2x^3+2x^2+x+4=(x^2+x+1)\cdot(x^2-3x+4)$.

   (b) This is a polynomial of degree four. So if it is reducible it either has a root in $\mathbf{Q}$ or factors into a product of quadrics. If it has a root $\frac{a}{b}$ in $\mathbf{Q}$, then by corollary 17.15, it has a root $a\in\mathbf{Z}$ and $a\mid -2$. Then $\alpha=\pm1,\pm2$. But after plugging in these four values into the polynomial I did not get zero. Therefore it is impossible that it has a linear factor. Now suppose

$$x^4-5x^3+3x-2=(x^2+ax+b)(x^2+cx+d).$$

   Comparing coefficients, we get

$$\begin{aligned} a+c =& -5 \\ ac+b+d =& 0 \\ ad+bc =& 3 \\ bd =& -2 \end{aligned}$$

   Looking at the last equation, we deduce that $(|b|,|d|)=(1,2)$ or $(2,1)=(|b|,|d|)$. Plugging in four possibilities the a and c one gets is never integral. Hence we conclude that this polynomial is not reducible.

   (c) Use Eisenstein's criterion with $p=2$.

   (d) Use Eisenstein's criterion with $p=3$.

3. **Problem 4.4** A degree two polynomial with field coefficient is irreducible if and only if it has no roots. So $x^2 + x + 1$ is the only irreducible polynomial of degree 2. A degree three polynomial with field coefficient is irreducible if and only if it has no root. So the only possibilities are $x^3 + x + 1$ and $x^3 + x^2 + 1$.

4. **Problem 4.5** If a polynomial of degree greater than 2 is irreducible, it must not have any root. So the only possibilities are $x^4 + x^3 + 1$, $x^4 + x^2 + 1$, $x^4 + x + 1$, $x^4 + x^3 +^2 +x + 1$. But

$$x^4 + x^2 + 1 = (x^2 + x + 1)^2.$$

   By looking at all possible products of quadrics in $\mathbf{Z}_2[x]$, we conclude that x^4+x^3+1, x^4+x+1 and $x^4 + x^4 + x^3 + x^2 + x + 1$ are the irreducible polynomials of degree 4.

5. **Problem 4.6**

   (a) Let us write $h_i \in \mathbf{Z}$ and $g_i \in \mathbf{Z}$ as the coefficient of h and g in the i-th degree term. Then by comparing the constant terms, we get $2 = g_0 \cdot h_0$ in $\mathbf{Z}$. Since 2 is a prime integer, we have either $2 \mid g_0$ or $2 \mid h_0$. Assume $2 \mid g_0$ and $2 \mid h_0$, we get $2 = 2g_0' \cdot 2h_0'$ for some integers g_0' and h_0'. Canceling 2 on both sides, we get $2 \mid 1$, which is not possible. Hence 2 divides precisely one of the constant terms of g and h.

   (b) Combined with (c).

   (c) Suppose $2 \mid g_0$ as was hinted. We may induct on $0 \leq j < k$ for g_j. Suppose $2 \mid g_u$ for all $u \leq j$, let us prove $2 \mid g_{j+1}$. Looking at the degree $j+1 \leq k < n$ term, the left hand side is zero. The right hand side is

$$g_{j+1}h_0 + g_j h_1 + \cdots g_q h_{n-q}.$$

   Hence

$$g_{j+1}h_0 = -(g_j h_1 + \cdots g_q h_{n-q}).$$

   By induction hypothesis, $2 \mid -(g_j h_1 + \cdots g_q h_{n-q})$ so $2 \mid g_{j+1}h_0$. By part (a), $2 \nmid h_0$ so $2 \mid g_{j+1}$. This completes the induction. We have shown that $x^n - 2$ is not a factor of two strictly lower degree polynomials with integer coefficient. Since $x^n - 2$ is primitive, $x^n - 2$ is irreducible in $\mathbf{Z}[x]$. By theorem 17.14, $x^n - 2$ is irreducible in $\mathbf{Q}[x]$.

6. **Problem 4.8** By theorem 17.22, the ideal (f) is maximal hence prime. Hence if $f \mid p \cdot q$, either $f \mid p$ or $f \mid q$.

7. **Problem 4.9** Plugging $\frac{r}{s}$, we get

$$0 = a_0 + a_1\frac{r}{s} + \cdots a_n\frac{r^n}{s^n}.$$

   Multiplying s^n on both sides, we get $s^n a_0 = -r(a_1 s^{n-1} + \cdots a_n r^{n-1})$ or $a_n r^n = -s(a_0 s^{n-1} + \cdots a_{n-1} r^{n-1})$. Then the first equality says $r \mid s^n a_0$. Since r and s are relatively prime, so are r and s^n. This implies $r \mid a_0$. The second equality would allow us to deduce that $s \mid a_n$.