

## Algebra 411.2

♡

### Homework 6 [SAMPLE EXAM]

♡

All answers should be justified.

♡

Due Wednesday April 22, in class.

♡

A. Read the “Partial Notes” on the web page, edition April 15 (or anything later). You do not have to know it by heart. However, you should know what material is covered in these notes, and if you have difficulties with problems bellow then try to find the relevant material in these notes or in the book.

B. Problems from the book, section 8.2: **1,3,5,6,7.**

*Explanations related to greatest common divisor  $\gcd(A, B)$  of two polynomials  $A, B$ :* (1)  
Over any field  $F$ , the  $\gcd(A, B)$  is calculated by the following procedure:

- If  $\deg(A) \geq \deg(B)$  then divide  $A$  by  $B$ , you get  $A = BQ_1 + R_1$ .
- Now divide  $B$  by  $R_1$ , you get  $B = R_1Q_2 + R_2$ .
- Now divide  $R_1$  by  $R_2$ , get  $R_1 = R_2Q_3 + R_3$ .
- Again, divide  $R_2$  by  $R_3$ , get  $R_2 = R_3Q_4 + R_4$ . Etc.
- The procedure will stop when you get zero remainder. Then the  $\gcd(A, B)$  is the last nonzero remainder.

For instance suppose that  $R_4 \neq 0$  but in the next division  $R_3 = R_4Q_5 + R_5$  the remainder  $R_5$  is zero. Then

$$\gcd(A, B) = R_4.$$

(2) One can always write  $\gcd(A, B)$  as a sum of a multiple of  $A$  and a multiple of  $B$ , i.e.,

$$\gcd(A, B) = AU + BV \quad \text{for some } U, V \in F[X].$$

The procedure for finding  $U$  and  $V$  is to “reverse” the calculation above:

- $\gcd(A, B) = R_4$  and we get rid of  $R_4$  by writing it as a linear combination of  $R_2$  and  $R_3$ :

$$\gcd(A, B) = R_4 = R_2 - R_3Q_4.$$

- Now we get rid of  $R_3$  by expressing it as a linear combination of  $R_1$  and  $R_2$  by  $R_3 = R_1 - R_2Q_3$ . This gives  $\gcd$  as a linear combination of  $R_1$  and  $R_2$  :

$$\gcd(A, B) = R_2 - R_3Q_4 = R_2 - (R_1 - R_2Q_3)Q_4 = R_2 - R_1Q_4 + R_2Q_3Q_4 = R_2(1 + Q_3Q_4) - R_1Q_4.$$

- Now we get rid of  $R_2$  by expressing it as a linear combination of  $B$  and  $R_1$  by  $R_2 = B - R_1Q_2$ . This gives  $gcd$  as a linear combination of  $B$  and  $R_1$  :

$$\begin{aligned} gcd(A, B) &= R_2(1 + Q_3Q_4) - R_1Q_4 = (B - R_1Q_2)(1 + Q_3Q_4) - R_1Q_4 \\ &= B(1 + Q_3Q_4) - R_1Q_2(1 + Q_3Q_4) - R_1Q_4 = B(1 + Q_3Q_4) - R_1[Q_2(1 + Q_3Q_4) + Q_4]. \end{aligned}$$

- Finally, we get rid of  $R_1$  by expressing it as a linear combination of  $B$  and  $A$  by  $R_1 = A - BQ_1$ . This gives  $gcd$  as a linear combination of  $A$  and  $B$  :

$$\begin{aligned} gcd(A, B) &= B(1 + Q_3Q_4) - R_1[Q_2(1 + Q_3Q_4) + Q_4] = B(1 + Q_3Q_4) - (A - BQ_1)[Q_2(1 + Q_3Q_4) + Q_4] \\ &= B[1 + Q_3Q_4 + Q_1[Q_2(1 + Q_3Q_4) + Q_4]] - AQ_1[Q_2(1 + Q_3Q_4) + Q_4]. \end{aligned}$$

So,  $U$  and  $V$  are certain complicated combinations of quotients  $Q_1, Q_2, \dots$

In problems you will need to calculate with specific polynomials  $A$  and  $B$ . Then you will deal at every stage with concrete  $Q_1, Q_2, \dots$  and you will be able to calculate expressions that appear such as  $1 + Q_3Q_4$  rather than carry them over to the next stage. So the formulas you get will be more reasonable.

### C.

1. Recall that  $\mathbb{Q}[\sqrt{2}]$  consists of all sums  $a + b\sqrt{2}$  with  $a, b \in \mathbb{Q}$  and that this is a subfield of  $\mathbb{R}$ . Prove that

$$\mathbb{Q}[X]/(X^2 - 2) \cong \mathbb{Q}[\sqrt{2}].$$

[Hint. This is similar to  $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ . One starts with a homomorphism  $\phi = ev_{\sqrt{2}}: \mathbb{Q}[X] \rightarrow \mathbb{R}$  and shows that  $Im(\phi) = \mathbb{Q}[\sqrt{2}]$  and  $Ker(\phi) = (X^2 - 2)$ .]

2. Over the field  $F = \mathbb{Z}_3$  consider the polynomial  $P = X^2 + 1$ ,

- (1) Show that  $P$  has no roots in  $F$ .
- (2) In  $F[X]$  consider the principal ideal  $I = (X^2 + 1)$ . How many elements does the ring  $A = F[X]/(X^2 + 1)$  possess? Show that the function

$$f: F^2 \rightarrow A, f(a, b) = a + bX + I$$

is a bijection.

- (3) Show that  $A$  is an integral domain, i.e., if  $a + bX + I \neq 0_A$  and  $\alpha + \beta X + I \neq 0_A$ , then  $(a + bX + I) \cdot (\alpha + \beta X + I) \neq 0_A$ .<sup>(1)</sup>
- (4) Show that  $A$  is a finite field with 9 elements.

---

<sup>1</sup>One possible strategy is the following: First discuss the case when  $b = 0$  (easy!). Once you check the claim in this case you will know that it is also true in the case  $d = 0$ . It remains to consider the case when  $b \neq 0$  and  $d \neq 0$ , here you can factor out  $b$  and  $d$  and reduce to the case when  $b = d = 1$ . Finally, consider the case when  $b = 1 = d$ , this will use part (1).

3. Are the rings  $\mathbb{Z}_9 \times \mathbb{Z}_4$  and  $\mathbb{Z}_6 \times \mathbb{Z}_6$  isomorphic?

4. Show that the ideal  $(X^2 - 3)$  in  $\mathbb{Q}[X]$  is a maximal ideal.

4. (a) Let  $A$  be a commutative ring. Prove that the zero ideal  $I = \{0\}$  is a prime ideal iff  $A$  is an integral domain.

(b) Let  $F$  be a field. Is the zero ideal in  $F[X]$  a prime ideal?

5. Show that if  $I$  and  $J$  are ideals in a ring  $R$  and  $I \subseteq J$  then the function

$$q : R/I \rightarrow R/J, q(r + I) \stackrel{\text{def}}{=} r + J$$

is

(1) (a) well defined,

(2) (b) a homomorphism of rings,

(3) (c) surjective.

(4) (d) The kernel is  $J/I \stackrel{\text{def}}{=} \{r + I \in R/I; r \in J\}$ .

6. Prove that  $X^4 + X^3 + X^2 + X + 1 = 0$  has no solutions in  $\mathbb{Z}$ .