

## REVIEW FOR MATH 3231

Read the initial chapters of Beachy and Blair before the start of class.

Section 1.1: Know how to use the Euclidean algorithm to find  $(a, b)$ . Note Theorem 1.1.4 (page 6) says every subgroup of  $\mathbf{Z}$  has the form  $a\mathbf{Z}$  for some  $a \geq 0$ .

Exercises: 3c, 5, 15

Section 1.2: Understand Proposition 1.2.2. This is used in Proposition 1.2.3 to show several results (with slightly different notation):

- if  $a|bc$  and  $(a, b) = 1$  then  $a|c$ ,
- if  $a|c$ ,  $b|c$ , and  $(a, b) = 1$  then  $a|bc$ .
- if  $(a, b) = 1$  and  $(a, c) = 1$  then  $(a, bc) = 1$ .

These are discussed in the course handout on divisibility and greatest common divisors.

Ignore page 18–22.

Exercises: 1c, 8

Section 1.3: Compare Prop. 1.3.4 to Prop. 1.4.5a. Ignore pages 28–29. Be able to solve simultaneous congruences as in Theorem 1.3.6 using the method of Example 1.3.5.

Section 1.4: Know the meaning of  $\mathbf{Z}_n^\times$  and  $\varphi(n)$ . (For instance, can you see why  $\varphi(7) = 6$  and  $\varphi(9) = 6$  directly from the definition of  $\varphi$ ?) Knowing when numbers are invertible modulo  $n$  is important. I will not make a fuss about zero divisors in  $\mathbf{Z}_n$ , but cancellation ( $ab \equiv ac \pmod{n} \Rightarrow b \equiv c \pmod{n}$ ) is generally invalid unless  $a \pmod{n}$  is invertible, and don't forget that. Ignore Prop. 1.4.8.

Exercises: 9, 11, 12

Section 2.1: The issue of well-definedness is important, so read Examples 2.1.3 and 2.1.4 carefully. Know what it means for a function to be one-to-one or onto, that these properties are preserved by composition (Prop. 2.1.5 and 2.1.6), and that invertibility of a function is equivalent to it being one-to-one and onto (Prop. 2.1.7).

Section 2.2: Skip

Section 2.3: Skip

Section 3.1: Everyone should know what a group is, so just skim over this section quickly.

Exercises: 2 (one case has answer “yes”), 10, 11

Section 3.2: Compare Examples 3.2.8 and 3.2.9 on page 108. Definition 3.2.7 and Prop. 3.2.8 are crucial. Read the proofs of Prop. 3.2.8b,c carefully.

Exercises: 1, 9, 12

Section 3.3: Know what a direct product is (and Prop 3.3.4.) and skip the rest (especially pages 119–122).

Exercises: 7, 11 (visualize  $G_1 \times G_2$  as a plane with  $G_1$  as the  $x$ -axis and  $G_2$  as the  $y$ -axis).

Section 3.4: Read all the examples and notice Prop. 3.4.5 on p. 132 is a deeper version of Theorem 1.3.6.

Exercises: 10, 18, 21 (this is like Prop. 3.4.5, but using  $\mathbf{Z}_n^\times$  and multiplication instead of  $\mathbf{Z}_n$  and addition).

Section 3.5: Read this section carefully, especially Prop. 3.5.2b, 3.5.3, 3.5.4a. Skip pages 138 – 140, *except* for Lemma 3.5.8. (Where in the proof of Lemma 3.5.8 do they use  $ab = ba$  and relative primality of the orders of  $a$  and  $b$ ?)

Exercises: 1, 2

Section 3.6: Just know what  $A_n$  and  $D_n$  are.

Exercises: 17, 23.

Section 3.7: The key result here is Prop. 3.7.4. Skip pages 158–160.

Exercises: 7, 8

Section 3.8: The key result is Theorem 3.8.9. Compare Prop. 3.8.4 and Prop. 1.3.3. In Prop. 3.8.7a, an example is reduction mod  $n$  from  $\mathbf{Z}$  and  $\mathbf{Z}_n$ , which uses  $G = \mathbf{Z}$  and  $N = n\mathbf{Z}$ .

Exercises: 3, 6, 16. (It's easier to construct the isomorphism in exercise 16 with a function  $H \times K \rightarrow G$  rather than the inverse  $G \rightarrow H \times K$ . In this spirit, look back at the last paragraph of Section 3.4.)