

# MT310 Homework 6

Your Name

Due Friday, March 19 by 5:00 pm

**Exercise 1.** Suppose  $G$  has two subgroups  $H, K$  with  $K \triangleleft G$  and that  $H \cap K = \{e\}$ . Prove that  $K \triangleleft HK$  and that  $HK/K \simeq H$ .

*Proof.* In general, if  $J$  is a subgroup of  $G$  containing  $H$ , then since  $gHg^{-1} = H$  for all  $g \in G$ , we necessarily have  $gHg^{-1} = H$  for all  $g \in J$ . Therefore  $H$  is normal in  $J$ . Taking  $J = HK$ , we have  $K \triangleleft HK$ . To show that  $HK/K \simeq H$ , define  $f : HK \rightarrow H$  by  $f(hk) = h$ . To show that  $f$  is well-defined, suppose  $hk = h'k'$ . Then  $(h')^{-1}h = k'k^{-1} \in H \cap K = \{e\}$ , so  $h = h'$  and  $f(hk) = h = h' = f(h'k')$ , hence  $f$  is well-defined. To show that  $f$  is surjective, let  $h \in H$ . Then  $f(h) = h$ , so  $f$  is clearly surjective. Finally,

$$\ker f = \{hk \in HK : f(hk) = e\} = \{hk \in HK : h = e\} = K.$$

Now  $HK/K \simeq H$  by the first isomorphism theorem.

Alternate approach: Define  $g : H \rightarrow HK/K$  by  $g(h) = hK$ . There is no need to check that  $g$  is well-defined. For surjectivity, let  $hkK \in HK/K$ . Then  $hkK = hK = g(h)$ , so  $g$  is surjective. Finally,

$$\ker g = \{h \in H : g(h) = K\} = \{h \in H : hK = K\} = \{h \in H : h \in K\} = H \cap K.$$

Since we have assumed  $H \cap K = \{e\}$ , this proves that  $g$  is injective, hence  $g : H \rightarrow HK/K$  is an isomorphism. Note this second proof did not use the first isomorphism theorem. However, if we drop the assumption that  $H \cap K = \{e\}$ , then the F.I.T comes into play: this proof shows that  $H/H \cap K = HK/K$ . This is the *Second Isomorphism Theorem*. □

**Exercise 2.** Let  $G$  be a finite group whose order is a power of a prime  $p$ . Let  $C$  be any conjugacy-class in  $G$ . Show that  $|C|$  is also a power of  $p$ . Then use this fact to prove that the center  $Z(G)$  is nontrivial.

*Proof.* We have proved, for any group  $G$  and  $a \in G$  contained in the conjugacy class  $C$ , that

$$|G| = |C| \cdot |C_G(a)|.$$

In particular, we have that  $|C|$  divides  $|G|$ . If  $|G| = p^n$  then  $|C| = p^k$  for some  $0 \leq k \leq n$ . Let  $C_0, C_1, \dots, C_h$  be the conjugacy classes in  $G$ , where  $C_0 = \{e\}$ . Then

$$|G| = 1 + |C_1| + \dots + |C_h|.$$

If  $Z(G) = \{e\}$ , then each class  $C_1, \dots, C_h$  has more than one element, so  $|C_i|$  is a positive power of  $p$  for each  $i \geq 1$ . But then  $|G| \equiv 1 \pmod{p}$ , contradicting the assumption that  $|G| = p^n$ . Hence  $Z(G)$  is nontrivial. □

**Exercise 3.** Suppose that  $G$  is a nonabelian group of order  $p^3$ , where  $p$  is a prime. Prove that  $Z(G) \simeq \mathbb{Z}_p$  and that  $G/Z(G) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ .

*Proof.* Since  $G$  is nonabelian, we cannot have  $G = Z(G)$ , so from the previous exercise, we have  $|Z(G)| = p$  or  $|Z(G)| = p^2$ . If  $|Z(G)| = p^2$  then  $|G/Z(G)| = p$  so  $G/Z(G) \simeq \mathbb{Z}_p$  is cyclic, which would again imply  $G$  is abelian. Hence  $|Z(G)| = p$  and  $Z(G) \simeq \mathbb{Z}_p$ . Now  $|G/Z(G)| = p^2$  so either  $G/Z(G) \simeq \mathbb{Z}_{p^2}$  or  $G/Z(G) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ . But again,  $G/Z(G)$  cannot be cyclic, so  $G/Z(G) \not\simeq \mathbb{Z}_{p^2}$ . Therefore we must have  $G/Z(G) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ . □

**Exercise 4.** Prove that the set of matrices

$$F = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$$

with entries in  $\mathbb{Z}_2$  is a field, under matrix addition and multiplication.

*Proof.* □

Write the elements of  $F$  as

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad a = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad b = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad 0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Then  $a + b = 1$ , so  $1 + a = b$  and  $1 + b = a$  and for all  $x \in F$  we have  $0 + x = x$  and  $x + x = 0$ . Also  $ab = ba = 1$ , and  $x1 = 1x = x$  for all  $x \in F$ . It follows that  $F$  is a subring of  $M_2(\mathbb{Z}_2)$ , is commutative, and the nonzero elements  $1, a, b$  in  $F$  are units. Hence  $F$  is a field.

**Exercise 5.** Prove that the subset  $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$  of  $\mathbb{C}$  is a field and that  $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}$ .

*Proof.* It is clear that  $\mathbb{Q}(\sqrt{2})$  is a subring of  $\mathbb{C}$ . To see that it is a field, Let  $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ , where  $a, b \in \mathbb{Q}$ . The inverse in  $\mathbb{C}$  is given by

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \left( \frac{a}{a^2 - 2b^2} \right) + \left( \frac{-b}{a^2 - 2b^2} \right) \sqrt{2}.$$

Since  $\sqrt{2} \notin \mathbb{Q}$ , the denominator  $a^2 - 2b^2$  is nonzero, and the coefficients lie in  $\mathbb{Q}$ , so

$$\frac{1}{a + b\sqrt{2}} \in \mathbb{Q}(\sqrt{2}).$$

This same fact shows that  $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}$ . □

**Exercise 6.** Prove that the subset  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$  of  $\mathbb{C}$  is a field and that  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$ .

*Proof.* As with the previous problem, the essential point is to show that every nonzero element of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  is a unit. Assume that  $a, b, c, d$  are not all zero and let  $\alpha = a + b\sqrt{2}$ ,  $\beta = c + d\sqrt{2}$ . Then

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = \alpha + \beta\sqrt{3},$$

so

$$\frac{1}{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}} = \frac{1}{\alpha + \beta\sqrt{3}} = \frac{\alpha - \beta\sqrt{3}}{\alpha^2 - 3\beta^2}.$$

It is clear that  $\alpha - \beta\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . And  $\frac{1}{\alpha^2 - 3\beta^2} \in \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , by the previous problem. Hence we have

$$\frac{1}{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

For the last assertion, it suffices to see that  $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ . Suppose on the contrary that  $\sqrt{3} = a + b\sqrt{2}$ , with  $a, b \in \mathbb{Q}$ . Then  $b \neq 0$  since  $\sqrt{3} \notin \mathbb{Q}$ . If  $a = 0$  then  $\sqrt{3} = b\sqrt{2}$ . Writing  $b = r/s$ , with  $r, s \in \mathbb{Z}$ , this leads to the equation

$$3s^2 = 2r^2.$$

This cannot be, since 2 divides  $2r^2$  an odd number of times, while 2 divides  $3s^2$  an even number of times. Hence  $b \neq 0$ , so  $ab \neq 0$ . But we have  $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ , so

$$\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q},$$

a contradiction. Hence  $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ . □