

NAME:

Write your answers in the space provided. Do not hand in loose sheets. You are allowed a letter size two-sided aid sheet. You may use any facts in the book, proved in class or in homework assignments. You have 80 minutes. Since most of the problems have restriction on how much you can write, you must carefully judge what is essential to include, before writing up your final answer. Clarity and brevity will be rewarded, while extraneous statements and redundancies will be penalized.

1. Put  $\alpha = \sqrt{2} + \sqrt{-1}$ .

[10] (a) Show that  $(\alpha^2 - 1)^2 = -8$ .

[10] (b) Show that  $1, \alpha, \alpha^2, \alpha^3$  are linearly independent over  $\mathbb{Q}$ .

[10] (c) What is the dimension of  $\mathbb{Q}(\alpha)$  over  $\mathbb{Q}$ ? Prove your answer in no more than 3 lines.

(a)  $\alpha^2 = 1 + 2\sqrt{2}i$ . So,  $(\alpha^2 - 1)^2 = -8$ .

(b)  $\alpha^3 = -\sqrt{2} + 5i$ . Let  $a_0, \dots, a_3 \in \mathbb{Q}$  and  $\sum_j a_j \alpha^j = 0$ . The real and imaginary parts say that

$$a_0 + a_1\sqrt{2} + a_2 - a_3\sqrt{2} = 0, \quad a_1 + a_22\sqrt{2} + 5a_3 = 0.$$

Since  $\sqrt{2}$  is irrational, the second equation implies that  $a_2 = 0$  and  $a_1 + a_3 = 0$ . The first equation then implies that  $a_0 = 0$  and  $a_1 - a_3 = 0$ . It follows that  $a_1 = a_3 = 0$  as well. This shows that  $1, \alpha, \alpha^2, \alpha^3$  are independent over  $\mathbb{Q}$ .

(c) By (a),  $\alpha$  is algebraic over  $\mathbb{Q}$  of degree at most 4, and so the  $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) \leq 4$ . By (b),  $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) \geq 4$  by the Dimension Theorem. So, the dimension is 4.

2. [15] (a) Complete the statement of the Degree Factorization Theorem:

*Let  $E$  be a finite extension of a field  $F$ , and  $K$  be a finite extension of a field  $E$ . Then*

---

$K$  is a finite extension of  $F$ , and  $[K : F] = [K : E][E : F]$ .

[20] (b) Let  $r$  and  $s$  be positive integers which are coprime, and put  $\alpha = \sqrt[r]{2}$  and  $\beta = \sqrt[s]{2}$ . In no more than 20 lines, prove that

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = rs.$$

(Hint: Show that  $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] \leq r$ .)

$\alpha$  is algebraic over  $\mathbb{Q}$  of degree  $r$ , since it is a root of  $x^r - 2$ , which is irreducible over  $\mathbb{Q}$ , by the Eisenstein criterion. Likewise,  $\beta$  is algebraic over  $\mathbb{Q}$  of degree  $s$ . It follows that  $\mathbb{Q}(\alpha, \beta)$  is a finite extension of  $\mathbb{Q}(\beta)$ , of degree  $\leq r$ . By DFT,

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] \leq rs$$

and the left side is divisible by  $[\mathbb{Q}(\beta) : \mathbb{Q}] = s$ . Likewise, it is also divisible by  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = r$ . Since  $(r, s) = 1$ ,  $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$  is divisible by  $rs$ . Thus it must be exactly  $rs$ .

3. [15] (a) Complete the statement of the Third Sylow Theorem:

*Let  $G$  be a finite group whose order is divisible by the prime  $p$ , and let  $m$  be number of Sylow  $p$ -subgroups of  $G$ . Then \_\_\_\_\_.*  
 *$m \equiv 1 \pmod{p}$ , and  $m$  divides  $|G|$ .*

[20] (b) In no more than 10 lines, prove that there is no simple group of order  $56 = 2^3 \cdot 7$ . (Hint: Show that there is just one Sylow 7-subgroup.)

Let  $K$  be a Sylow 2-subgroup of  $G$ . Then the orders of elements of  $K$  and their conjugates are powers of 2. If  $K$  is normal, then we are done. So, assume not, say  $xKx^{-1} \neq K$  for some  $x \in G$ . Therefore, the number of elements whose orders are powers of 2 is  $\geq |xKx^{-1} \cup K| > |K| = 8$ .

By (a),  $G$  has one or eight Sylow 7-subgroups. Assume eight. Each one is cyclic of order 7, so, the intersection of any two of them is  $\{e\}$ . Thus, there are exactly  $8 \cdot 6 = 48$  elements of order 7 in  $G$ . This implies that  $|G| > 8 + 48 = 56$ , a contradiction. So,  $G$  has just one Sylow 7-subgroup. But this implies that it is normal in  $G$ , and we are done.

4. (Bonus) Prove that the regular 15-gon is constructible. (Hint:  $120-72=48$ .)

In a homework problem, you have shown that  $\theta = 36^\circ$  is constructible, i.e.  $e^{i\theta}$  is constructible. So,  $e^{2i\theta}$  is constructible, which means that  $72^\circ$  is constructible. But we also know that  $120^\circ = 2 \cdot 60^\circ$  is constructible. So, the difference, which is  $48^\circ$  is constructible. Bisecting this, we see that  $24^\circ$  is constructible. To construct the regular 15-gon, we divide  $360^\circ$  by 15, which gives  $24^\circ$ , which is constructible.