

3. (c) No.

4. (a) False. (b) True. (c) True. (d) True. (e) True. *(f) True.

1. (a) Let $|G| = 455 = 5 \cdot 7 \cdot 13$. Let n_p denote the number of Sylow p -subgroups of G . By the Sylow III, n_7 divides $5 \cdot 13$, so $n_7 = 1, 5, 13, 65$. Among these, 1 is the only number that is congruent to 1 mod 7, so $n_7 = 1$. Similarly, $n_{13} = 1 + 13k$ divides $5 \cdot 7$, which forces $n_{13} = 1$. Let A and B be the unique Sylow 7- and 13-subgroup, respectively. Note that A and B are normal in G , by the Sylow II. Now, G/A has order $5 \cdot 13$ and 5 does not divide 12, so G/A is abelian, and hence $G' \leq A$. Likewise, $G' \leq B$ since G/B is abelian ($5 \nmid (7-1)$). Therefore, $G' \leq A \cap B = 1$, that is, G is abelian. [24.18']

(b) Let $|G| = 45 = 9 \cdot 5$. By the Sylow III, $n_3 = 1 + 3k$ divides 5, so $n_3 = 1$. Also, $n_5 = 1 + 5m$ divides 9, so $n_5 = 1$. Since the Sylow 3-subgroup A and Sylow 5-subgroup B are unique, they are normal subgroups of G . Since they have relatively prime orders, $A \cap B = 1$, hence by the *HK-Lemma*, $G = AB$. Thus, $G = A \times B$. Observe that A has order 3^2 , so A is abelian, whence $A \cong \mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$. Finally, $B \cong \mathbb{Z}_5$. We conclude that $G \cong \mathbb{Z}_9 \times \mathbb{Z}_5$ or $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. [24.44]

2. Let $|G| = 140 = 4 \cdot 5 \cdot 7$. First, n_5 is congruent to 1 mod 5 and is a divisor of $4 \cdot 7 = 28$. The divisors of 28 are 1, 2, 4, 7, 14, 28; among these, only 1 is congruent to 1 mod 5, so $n_5 = 1$. Likewise, $n_7 = 1$ since 1 is the only divisor of 20 that is congruent to 1 mod 7. So we have a normal Sylow 5-subgroup B and a normal Sylow 7-subgroup C (by the Sylow II). Since both A and B are normal subgroups, AB is also a normal subgroup of G . Since A and B have relatively prime orders, we have $|A \cap B| = 1$ and, by the *HK-Lemma*, $|AB| = |A||B|/|A \cap B| = 10$. Similar reasoning yields that AC and $ABC = (AB)C$ are normal subgroups of order 14 and 70, respectively. [24.28a']

Second proof. Consider the quotient group $\bar{G} := G/A$ and the canonical epimorphism $\pi : G \rightarrow \bar{G}$. We have $|\bar{G}| = |G/A| = |G|/|A| = 140/2 = 70 = 2 \cdot 5 \cdot 7$, and easy calculations show that $n_5(\bar{G}) = 1$ and $n_7(\bar{G}) = 1$. Let \bar{B} and \bar{C} be the unique, hence normal, Sylow 5- and 7-subgroup of \bar{G} . Then by the Correspondence Theorem, the preimages $B := \pi^{-1}(\bar{B})$ and $C := \pi^{-1}(\bar{C})$ are normal subgroups of G of order 10 and 14, respectively. We next show that G has a subgroup of order 70, which, being of index 2, is necessarily normal. Note that \bar{B} and \bar{C} are normal in \bar{G} . This implies that $\bar{B}\bar{C}$ is also a normal subgroup of \bar{G} . Since $\bar{B} \cap \bar{C} = 1$, we have $|\bar{B}\bar{C}| = |\bar{B}||\bar{C}|/|\bar{B} \cap \bar{C}| = 35$. Then $\pi^{-1}(\bar{B}\bar{C})$ is a (normal) subgroup of order 70 in G . (By the way, $\pi^{-1}(\bar{B}\bar{C}) = BC$.)

Warning. The group G/A is only a quotient, not a subgroup of G . That is the reason why we need to find some way to get a *subgroup* of G of order 70.

3. (a) Let F be a finite field. Note that F must be a finite integral domain, so it has prime characteristic p , say. Consider only the additive group $\langle F, + \rangle$. This is a finite abelian group, so by the Fundamental Theorem of Finite Abelian Groups,

$$\langle F, + \rangle \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}}.$$

Now, the crucial point: the characteristic of the ring F is nothing but the maximal order of elements of the group $\langle F, + \rangle$. It follows that all $p_i = p$ and all $e_i = 1$, that is,

$$\langle F, + \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p,$$

whence $|F| = p^n$. [13.43]

Second proof. (For those who learned vector spaces and dimension.) A finite field F contains a *prime subfield* $P = \{n \cdot 1 \mid n \in \mathbb{Z}\}$. Note that $P \cong \mathbb{Z}_p$, where $p = \text{char } F > 0$. (See 13.27.) Note also that F can be viewed as a vector space over P with the scalar multiplication being the multiplication in F . Since F is finite, the dimension $\dim_P F = n$ must be finite. Thus, $|F| = |P|^n = p^n$.

(b) $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$. This is clearly a commutative ring with 1. We shall show that this is a field by exhibiting a multiplicative inverse for every nonzero element $a + bi$ of $\mathbb{Z}_3[i]$. Observe that $(a + bi)(a - bi) = a^2 + b^2$, so the inverse must be

$$\frac{1}{a + bi} := (a + bi)^{-1} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i,$$

provided that $a^2 + b^2$ is a unit in \mathbb{Z}_3 . This is the case because $a + bi \neq 0$ in $\mathbb{Z}_3[i]$ implies that $3 \nmid a$ or $3 \nmid b$, hence $3 \nmid (a^2 + b^2)$, that is, $a^2 + b^2 \neq 0$ in \mathbb{Z}_3 , which amounts to saying that $a^2 + b^2 \in U(\mathbb{Z}_3)$ since \mathbb{Z}_3 is a field. [13.Exmp.9]

Second proof. Just calculate: $2 \cdot 2 = 4 = 1$, $i(2i) = -2 = 1$, $(1+i)(2+i) = 1+3i = 1$, $(1+2i)(2+2i) = -2+6i = 1$. The above computations show that every nonzero element is a unit, thus, $\mathbb{Z}_3[i]$ is a field.

(c) $\mathbb{Z}_5[i]$ is not a field since it is not an integral domain. There are zero-divisors: $(2+i)(2-i) = 5 = 0$. [13.18]

*(d) $\mathbb{Z}_5[\sqrt{k}] = \{a + b\sqrt{k} \mid a, b \in \mathbb{Z}_5\}$ is a field if and only if $k \in \mathbb{Z}$ is not a square in \mathbb{Z}_5 : For $a + b\sqrt{k} \neq 0$ with $b \neq 0$,

$$\frac{1}{a + b\sqrt{k}} = \frac{a - b\sqrt{k}}{a^2 - kb^2} = \frac{a}{a^2 - kb^2} + \frac{-b}{a^2 - kb^2}\sqrt{k}$$

exists if and only if $a^2 - kb^2 \in U(\mathbb{Z}_5) = \mathbb{Z}_5^* \iff kb^2 \not\equiv a^2 \pmod{5} \iff k \not\equiv (a/b)^2 \pmod{5} \iff k \not\equiv \square \pmod{5}$.

For example, $\mathbb{Z}_5[\sqrt{2}]$, $\mathbb{Z}_5[\sqrt{3}]$, $\mathbb{Z}_5[\sqrt{7}]$, $\mathbb{Z}_5[\sqrt{-2}]$, $\mathbb{Z}_5[\sqrt{-3}]$, $\mathbb{Z}_5[\sqrt{-7}]$ are all fields of order 25. [13.36]

4. (a) False. A finite integral domain is necessarily a field, so must have prime power order (Problem #3(a)). [13.28, 13.Thm.2+13.43]

Second proof. Let D be an integral domain of order 10 and $\text{char } D = p$. Note that p is a prime and, by the Lagrange Theorem (for groups), $p \mid 10$. So $p = 2$ or 5 . By the Cauchy Theorem, D contains elements a and b of additive order 2 and 5, respectively. If $p = 2$, then $2b = 0$ and $5b = 0$, so $b = 3(2b) - 5b = 0$, which is absurd. Similarly, if $p = 5$, then $5a = 0$ and $2a = 0$, so $a = 3(2a) - 5a = 0$, a final contradiction.

(b) True. In a commutative ring, the binomial theorem holds: For $a, b \in R$ and $n \in \mathbb{N}$,

$$(a + b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n. \quad (*)$$

If $n = p$ is a prime, then $\binom{p}{j} = \frac{p!}{j!(n-j)!}$ is a multiple of p when $1 \leq j < p$ because p appears only in the numerator, but not in the denominator. Now, since $\text{char } R = p$, all the middle terms on the right-hand side of (*) vanish, and we get $(a + b)^p = a^p + b^p$, as required. [13.41a]

(c) True. For any $a \in R$, we have $-a = (-a)^2 = a^2 = a$, which implies that $2a = 0$. Thus, $\text{char } R = 2$. [12.50]

Second proof. For $a \in R$, $2a = (2a)^2 = (a + a)^2 = 4a^2 = 4a$, whence $2a = 0$.

(d) True. $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. If $(a+bi)(c+di) = 1$ in $\mathbb{Z}[i]$, then by taking absolute values and squaring, $|a+bi|^2|c+di|^2 = 1$. This brings us to an equation over \mathbb{Z} : $(a^2+b^2)(c^2+d^2) = 1$. Thus, $a^2 + b^2 = 1$. The only solutions in \mathbb{Z} are: $(a, b) = (\pm 1, 0)$ or $(0, \pm 1)$, which yield the four units in $\mathbb{Z}[i]$, namely ± 1 and $\pm i$. [12.23]

(e) True. $U(\mathbb{Z}[x]) = \{\pm 1\}$, i.e., the constant polynomials $f(x) \equiv 1$ and $g(x) \equiv -1$. The degree formula, $\deg(fg) = \deg(f) + \deg(g)$, tells us that $U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{\pm 1\}$. [12.25]

*(f) True. Observe that $(1 + \sqrt{2})(\sqrt{2} - 1) = 1$. Thus, $1 + \sqrt{2}$ is a unit, and so are $(1 + \sqrt{2})^n$ for $n \in \mathbb{Z}$. (Note that *the units form a group under multiplication.*) [Cf. 12.22]