

2. Homomorphisms: $\phi : x \mapsto ax$ with $a = 0, 1, 5, 6$. The identity map is the only isomorphism.
3. $\langle x \rangle$ is maximal in $\mathbb{Q}[x]$. $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{Q}[x]$.
4. $K = \mathbb{Z}_p$ in all cases.
5. (a) 48. (b) $2\mathbb{Z} \triangleleft \mathbb{Z}$. (c) True. (d) $\mathbb{Z}_3[i]$ and $\mathbb{Z}_7[i]$ are fields. (e) False. (f) False.

1. (a) Sylow's Third Theorem asserts that the number n_p of Sylow p -subgroups of a group G satisfies $n_p \equiv 1 \pmod{p}$ and $n_p \mid |G|$. [24.Thm.5]
- (b) Let $|G| = 96 = 2^5 \cdot 3$. The number n_2 of Sylow 2-subgroups has the form $n_2 = 1 + 2k$ and $n_2 \mid 3$. So $n_2 = 1$ or 3. If $n_2 = 1$, then, by Sylow's Second Theorem, the unique Sylow 2-subgroup is normal (certainly, nontrivial and proper) in G , whence G is not a simple group. Assume now that $n_2 = 3$. Let A and B be two distinct Sylow 2-subgroups. Let $C = A \cap B$. Note that $|C| = |A||B|/|AB| \geq (32)^2/96 = 32/3$, so $|C| = 16$. This implies that C is normal both in A and in B , and consequently $N := N_G(C)$ contains both A and B . Since A is already maximal in G , we have $N = G$. This says that C is normal in G , and so G is not simple. [Cf. 24.12]
2. Let ϕ be a ring homomorphism from \mathbb{Z}_{10} to \mathbb{Z}_{10} and $\phi(1) = a$. Since ϕ preserves the addition, for $x \in \mathbb{Z}_{10}$, we have $\phi(x) = \phi(x \cdot 1) = x \cdot \phi(1) = ax$. Moreover, ϕ sends an idempotent to an idempotent, we see that a is also an idempotent, i.e, a satisfies $a^2 = a$. By inspection, there are only four idempotents in \mathbb{Z}_{10} , viz. 0, 1, 5, and 6, and these yields all of the "possible" ring homomorphisms: [15.16 + 15.18; Cf. 15.8 + 15.48]

$$\phi_a : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, \quad \text{where } a = \phi_a(1) = 0, 1, 5, 6.$$

Indeed, these are ring homomorphisms since

$$\phi_a(xy) = \phi_a(xy \cdot 1) = xy\phi_a(1) = axy = (ax)(ay) = \phi_a(x)\phi_a(y),$$

where the fact that a is an idempotent plays a role. For ϕ_a to be an isomorphism, we need $a = \phi_a(1)$ be a generator of \mathbb{Z}_{10} . Among the above four candidates, only $a = 1$ is a generator, so there is only one isomorphism, namely ϕ_1 , i.e., the identity map.

3. (a) Let u be a unit and $u \in I$. For any $r \in R$, since I is an ideal, we have $r = (ru^{-1})u \in I$. This shows that $I = R$. [14.17]
- (b) If R is a field and $I \neq 0$ is an ideal, then I contains a nonzero element u , which must be a unit since R is a field. By (a), $I = R$. Conversely, assume that 0 and R are the only ideals of R . For any $0 \neq u \in R$, the ideal $\langle u \rangle$ is nonzero, hence $\langle u \rangle = R$. In particular, $1 \in \langle u \rangle$, so $1 = uv$ for some $v \in R$. This shows that u is a unit, and that R is a field. [14.25 + 12-14.19]
- (c) Note that R/M is also commutative with unity (given by $1 + M$). Let I be an ideal of R/M . Consider $N := \pi^{-1}(I) \subseteq R$, where $\pi : r \mapsto r + M$ is the natural homomorphism from R onto R/M . Note that N is an ideal of R that contains M . Since M is maximal in R , one has $N = M$ or R , and this gives $I = 0$ or R/M . By (b), this shows that R/M is a field. [14.Thm.4]
- (d) $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$, which is not a field, so $\langle x \rangle$ is not a maximal ideal of $\mathbb{Z}[x]$. As a contrast, $\mathbb{Q}[x]/\langle x \rangle \cong \mathbb{Q}$, which is a field, so $\langle x \rangle$ is maximal in $\mathbb{Q}[x]$. Note that the ideal $\langle x^2 + 1 \rangle$ contains $x^2 + 1 = (x + 1)^2$ but not $x + 1$ (why?), so it is not prime, whence not maximal, in $\mathbb{Z}_2[x]$. However, $\mathbb{Q}[x]/\langle x^2 + 1 \rangle \cong \mathbb{Q}[i]$ and the latter is indeed a field, so $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{Q}[x]$. [14.Exmp.17 + 16.18 + 14.Exmp.16 + Cf. 14.Exmp.15 or 16.Exmp.3]
4. (a) First, $K = \{x \in F \mid x^p = x\}$ is nonempty since it (at least) contains 0 and 1. To show that it is a subfield, one must check that if $x^p = x$ and $y^p = y$, then $(x - y)^p = x - y$ and $(xy)^p = xy$ and that every nonzero $x \in K$ is a unit in K . The first two are easy: For, by Freshman's dream (#13.41a), $(x - y)^p = x^p - y^p = x - y$ and $(xy)^p = x^p y^p = xy$. If $x \neq 0$ and $x^p = x$, then we can cancel x from both sides by multiplying by the inverse $x^{-1} \in F$ and we get $x^{p-1} = 1$. So $x \cdot x^{p-2} = 1$, and $x^{-1} = x^{p-2} \in K$. [13.55]

- (b) The elements of K are roots of the polynomial $f(x) = x^p - x$. By Lagrange's Theorem (Corollary 3 to Theorem 16.2), there are at most p such elements in F . On the other hand, the prime subfield P of F is isomorphic to \mathbb{Z}_p , so by Fermat's Little Theorem, the elements of P satisfy $f(x) = 0$. We have therefore proved that there are exactly p roots of $f(x)$ in F , that is, $K = P$. In the three cases $F = \mathbb{Z}_p, \mathbb{F}_{p^n},$ or $\mathbb{Z}_p[x]$, the prime subfields are all isomorphic to \mathbb{Z}_p . [16.Thm.2.Cor.3]
5. (a) $|G| = 168 = 7 \cdot 3 \cdot 8$. We have $n_7(G) = 1$ or 8 . If G is simple, $n_7 = 8$ and every Sylow 7-subgroup is $\cong \mathbb{Z}_7$, so there are $8(7-1) = 48$ elements of order 7 in G . [24.11]
- (b) Let $R = \mathbb{Z}$ and $I = \langle 2 \rangle = 2\mathbb{Z}$. Then $I[x]$ consists of polynomials with all coefficients even. Clearly, $x \notin I[x]$, so $I[x]$ is properly contained in the proper ideal $I[x] + \langle x \rangle$, i.e., $I[x] \subsetneq I[x] + \langle x \rangle \subsetneq R$. [16.37 + 12.20]
- (c) Consider the natural epimorphism $\pi : S \rightarrow S/A$ and the composition map $f := \pi \circ \phi : R \rightarrow S/A$. Since both ϕ and π are onto, so is f . Note that $\text{Ker } f = \phi^{-1}(\pi^{-1}(0+A)) = \phi^{-1}(A)$. By the First Isomorphism Theorem, $R/\phi^{-1}(A) \cong S/A$. Since A is maximal in S , S/A is a field, so is $R/\phi^{-1}(A)$, and thus $\phi^{-1}(A)$ is maximal in R . [15.41b]
- (d) $i = \sqrt{-1}$. Note that -1 is not a square in \mathbb{Z}_3 and in \mathbb{Z}_7 since $\square \equiv 0, 1 \pmod{3}$ and $\square \equiv 0, 1, 2, 4 \pmod{7}$; while -1 is indeed a square in \mathbb{Z}_5 and in \mathbb{Z}_{17} since $-1 = 4 = 2^2$ in \mathbb{Z}_5 and $-1 = 16 = 4^2$ in \mathbb{Z}_{17} . It follows that $\mathbb{Z}_3[i]$ and $\mathbb{Z}_7[i]$ are fields, while $\mathbb{Z}_5[i]$ and $\mathbb{Z}_{17}[i]$ are not. [Cf. 12-14.47 and 13.36]
Remark. -1 is not a square in $F \iff x^2 + 1$ has no roots in $F \iff \langle x^2 + 1 \rangle$ is maximal in $F[x] \iff F[i] \cong F[x]/\langle x^2 + 1 \rangle$ is a field.
- (e) As rings, $2\mathbb{Z} \not\cong 5\mathbb{Z}$. Let $\phi : 2\mathbb{Z} \rightarrow 5\mathbb{Z}$ be a ring homomorphism and $a = \phi(2)$. Note that $2 + 2 = 4 = 2 \cdot 2$, so we must have $a + a = a \cdot a$, or $a^2 = 2a$. Solving for a in \mathbb{Z} , we get $a = 0$ or 2 . Thus, we get only one homomorphism $2 \mapsto 0$, that is, the zero map. [15.44]
Remark. As groups, $2\mathbb{Z} \cong 5\mathbb{Z} \cong \mathbb{Z}$.
- (f) As rings, $\mathbb{Q}[\sqrt{2}] \not\cong \mathbb{Q}[\sqrt{5}]$. Suppose $\phi : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{5}]$ is ring (field) homomorphism and let $x = \phi(\sqrt{2})$. Note that $(\sqrt{2})^2 = 2$ in $\mathbb{Q}[\sqrt{2}]$, so $x^2 = 2$ in $\mathbb{Q}[\sqrt{5}]$. However, this is impossible because if $x = a + b\sqrt{5}$, $a, b \in \mathbb{Q}$, then $x^2 = 2$ would yield $2 = (a + b\sqrt{5})^2 = a^2 + 5b^2 + 2ab\sqrt{5}$. If $ab = 0$, then $a^2 + 5b^2 = 2$, and we further have $a^2 = 2$ or $5b^2 = 2$, which are absurd. If $ab \neq 0$, then we would get $\sqrt{5} = (2 - a^2 - 5b^2)/(2ab) \in \mathbb{Q}$, which is absurd, either. [15.50]
- *6. (a) By Fermat's Little Theorem and Lagrange's Theorem for domains, the polynomial $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$ has $1, 2, \dots, p-1$ as all of its roots in \mathbb{Z}_p . This proves the factorization in $\mathbb{Z}_p[x]$: [16.31]

$$x^{p-1} - 1 = (x-1)(x-2) \cdots (x-(p-1)).$$

- (b) If $p = 2$, then $1! = 1 \equiv -1 \pmod{2}$, and Wilson is right. For any odd prime p , we substitute x by 0 in (a) and get [16.32]

$$-1 \equiv (-1)(-2) \cdots (-(p-1)) = (p-1)!(-1)^{p-1} = (p-1)! \pmod{p}.$$

- (c) Note that $p-a \equiv -a \pmod{p}$, so by Wilson, [16.35]

$$-1 \equiv 40! = 1 \cdot 2 \cdots 20 \cdot (-20) \cdot (-19) \cdots (-2) \cdot (-1) = (20!)^2(-1)^{20} = (20!)^2 \pmod{41}.$$