Groups

1. (Algebra Comp S03) Let A, B and C be normal subgroups of a group G with $A \subseteq B$. If $A \cap C = B \cap C$ and $AC = BC$ then prove that $A = B$.

   `Answer:` *Let $b \in B$. Since $b = b1 \in BC = AC$, there are $a \in A$ and $c \in C$ such that $b = ac$. Since $a^{-1} \in A \subseteq B$, we have $c = a^{-1}b \in B$, and so $c \in B \cap C = A \cap C$. This implies that $c \in A$ and hence $b = ac \in A$. We have shown that all elements of B are in A and so $A = B$. Note that the claim is true even if the subgroups are not normal.*

2. (Algebra Comp S03) Let G be a finite group with identity e, and such that for some fixed integer $n > 1$, $(xy)^n = x^n y^n$ for all $x, y \in G$. Let $G_n = \{z \in G : z^n = e\}$ and $G^n = \{x^n : x \in G\}$. Prove that both G_n, and G^n are normal subgroups of G and that $|G^n| = [G : G_n]$.

   `Answer:` *Define $\phi : G \to G$ by $\phi(x) = x^n$ for all $x \in G$. ϕ is a homomorphism because*

   $$\phi(xy) = (xy)^n = x^n y^n = \phi(x)\phi(y)$$

   for all $x, y \in G$. The kernel of ϕ is G_n and the image is G^n. This makes G_n a normal subgroup of G, G^n a subgroup of G and $G/G_n \cong G^n$, in particular, $|G^n| = [G : G_n]$.

   It remains only to check that the subgroup G^n is normal. This follows from the equation

   $$\phi(yxy^{-1}) = (yxy^{-1})^n = \underbrace{(yxy^{-1})(yxy^{-1})(yxy^{-1})\cdots(yxy^{-1})}_{n \text{ times}} = yx^n y^{-1} = y\phi(x)y^{-1}.$$

   So, if $a \in G^n$, then $a = \phi(x)$ for some $x \in G$ and, for all $y \in G$ we have $yay^{-1} = y\phi(x)y^{-1} = \phi(yxy^{-1}) \in G^n$.

3. (Algebra Comp S03) Prove:

   (a) A group of order 45 is abelian.

   (b) A group of order 275 is solvable.

   `Answer:` *See F13 and S09.*

4. (Algebra Comp F03) Let G be an abelian group of order pq with p and q distinct primes. Show that G is cyclic. (Don't use the Classification Theorem of Finitely Generated Abelian Groups.)

   `Answer:` *By Sylow (or Cauchy), G contains a subgroup of order p and hence an element a of order p. Similarly G contains an element b of order q. We now solve the equation $(ab)^n = 1$ for n. Since a and b commute we have $1 = 1^p = ((ab)^n)^p = a^{np}b^{np} = b^{np}$. Since b has order q, this implies that q divides np, and since $p \neq q$, that q divides n. Similarly, p divides n and since $p \neq q$, pq divides n. Since the order of ab also divides $|G| = pq$, we have $|ab| = pq$ and $G = \langle ab \rangle$.*

5. (Algebra Comp F03) Show that all groups of order $3^2 \cdot 11^2$ are solvable.

   `Answer:` *Let G be a group of order $3^2 \cdot 11^2$. By Sylow, n_{11} divides $3^2 \cdot 11^2$ and n_{11} is congruent to 1 modulo 11. The only number satisfying these conditions is $n_{11} = 1$, and so G has a normal subgroup N of order 11^2. Since N has prime square order, N is abelian, and G/N has order 3^2 so is also abelian for the same reason. This means that G is solvable.*

6. (Algebra Comp F03) Let G be a p-group and $N \trianglelefteq G$, a normal subgroup of order p. Prove that N is in the center of G.

   `Answer:` *Since N is normal, it is a union of conjugacy classes of G. Such a conjugacy class has either one element, in which case the element is in $Z(G)$, or has a multiple of p elements. Since $|N| = p$, it must be a union of one-element conjugacy classes. Since an element is in $Z(G)$ if and only if it forms a one-element conjugacy class, we have $N \leq Z(G)$.*

7. (Algebra Comp F04) Let H and N be subgroups of a finite group G, N normal in G. Suppose that $|G:N|$ is finite and $|H|$ is finite, and $\gcd(|G:N|,|H|)=1$. Prove that $H \leq N$.

   `Answer:` *Let $\phi : H \to G/N$ be the restriction of the natural homomorphism $G \to G/N$. Since $H/\ker\phi \cong \phi(H) \leq G/N$, the order of $\phi(H)$ divides both $|H|$ and $|G/N| = |G:N|$. But $\gcd(|G:N|,|H|)=1$, and so $|\phi(H)|=1$, and $\phi(H)$ is the trivial subgroup of G/N. In other words H is contained in the kernel of ϕ, namely $H\cap N$. Hence $H \leq N$.*

8. (Algebra Comp F04) Assume $|G|=p^3$ with p a prime.

   (a) Show $|Z(G)|>1$.

   (b) Prove that if G is nonabelian, then $|Z(G)|=p$.

   `Answer:`

   (a) *Dummit and Foote, Theorem 8, page 125.*

   (b) *Since $|G|=p^3$, the order of $Z(G)$ is 1, p, p^2 or p^3. The case $|Z(G)|=1$ is eliminated by (a). If $|Z(G)|=p^3$, then G is abelian, contrary to assumption. If $|Z(G)|=p^2$, then $G/Z(G)$ is a cyclic group of order p. This would imply that G is abelian once again (see Algebra Comp F12), contrary to assumption. Thus we are left with $|Z(G)|=p$.*

9. (Algebra Comp F04) Let P be a Sylow p-subgroup of G. Assume that $P \trianglelefteq N \trianglelefteq G$. Show that $P \trianglelefteq G$.

   `Answer:` *Suppose that $|G|=p^k m$ with $m,k\in\mathbb{N}$ and $p \nmid m$. Then any subgroup of order p^k is a Sylow p-subgroup of G. In particular, $|P|=p^k$. Since $P \trianglelefteq N \trianglelefteq G$, the order of N is a multiple of p^k and a divisor of $p^k m$. Thus $|N|=p^k l$ where $l|m$. This means that any subgroup of N of order p^k is a Sylow p-subgroup of N. In particular, P is a Sylow p-subgroup of N. In fact, since $P \trianglelefteq N$, P is the only Sylow p-subgroup of N. (The set of Sylow p-subgroups forms a conjugacy class. Since $P \trianglelefteq N$, P is conjugate only to itself (with respect to conjugation by elements of N).)*

   Now let $g\in G$. Then gPg^{-1} is a subgroup that is isomorphic to P, so has order p^k. Moreover, , because N is normal, $gPg^{-1} \subseteq gNg^{-1} = N$. So gPg^{-1} is a subgroup of N with order p^k, that is, a Sylow p-subgroup of N. But there is only one such subgroup, namely P. So $gPg^{-1}=P$ for all $g\in G$, which means $P \trianglelefteq G$.

10. (Algebra Comp S05) Let G be an abelian group, $H=\{a^2 \mid a\in G\}$ and $K=\{a\in G \mid a^2=1\}$. Prove that $H\cong G/K$.

    `Answer:` *Let $\phi : G\to G$ be defined by $\phi(a)=a^2$ for all $a\in G$. Since G is abelian, ϕ is a homomorphism: $\phi(ab)=(ab)^2=a^2b^2=\phi(a)\phi(b)$ for all $a,b\in G$. Since $\ker\phi = K$ and $\phi(G)=H$, we have $G/K\cong H$.*

11. (Algebra Comp S05) Assume $G=HZ(G)$, where H is a subgroup of G and $Z(G)$ is the center of G. Show:

    (a) $Z(H)=H\cap Z(G)$

    (b) $G'=H'$ (Where G' is the commutator group of G)

    (c) $G/Z(G)\cong H/Z(H)$

    `Answer:`

    (a) *Any element of H that is in $Z(G)$ commutes with all elements of G, so commutes with all elements of H. In other words, $H\cap Z(G)\subseteq Z(H)$. On the other hand, if $h\in Z(H)$ then $h\in H$ and h commutes with all elements of H and $Z(G)$. Thus h commutes with all elements of $HZ(G)=G$. Thus $Z(H)\subseteq H\cap Z(G)$.*

(b) *Since $H \leq G$, we have $H' \leq G'$. To show the opposite inclusion, it suffices to show that the generators of G' are in H'. Let $x, y \in G$. Then $x = h_1 z_1$ and $y = h_2 z_2$ for some $h_1, h_2 \in H$ and $z_1, z_2 \in Z(G)$. Then*

$$xyx^{-1}y^{-1} = h_1 z_1 h_2 z_2 z_1^{-1} h_1^{-1} z_2^{-1} h_2^{-1} = h_1 h_2 h_1^{-1} h_2^{-1} \in H'.$$

(c) *Define $\phi : H \to G/Z(G)$ by $\phi(h) = hZ(G)$ for all $h \in H$. Since ϕ is the restriction of the natural homomorphism $G \to G/Z(G)$, ϕ is a homomorphism. The image of ϕ is $G/Z(G)$ and the kernel is*

$$\ker \phi = \{h \in H \mid h \in Z(G)\} = H \cap Z(G) = Z(H).$$

Hence $H/Z(H) \cong H/\ker\phi \cong \phi(H) = G/Z(G)$.

12. (Algebra Comp S05) Prove:

   (a) A group of order 80 need not be abelian (twice) by exhibiting two non-isomorphic non-abelian groups of order 80 (with verification).

   (b) A group of order 80 must be solvable.

   `Answer:`

   (a) *It is easy to construct nonabelian groups of order 80. For example: D_{80}, $D_{40} \times \mathbb{Z}_2$, $D_8 \times \mathbb{Z}_{10}$, $D_8 \times \mathbb{Z}_5 \times \mathbb{Z}_2$, etc. The first two are nonisomorphic, for example, because D_{80} has elements of order 40 whereas all elements of $D_{40} \times \mathbb{Z}_2$ have order 20 or less.*

   (b) *We need a few facts:*

   - *If $N \trianglelefteq G$ with N and G/N solvable, then G is solvable.*
   - *All abelian groups are solvable.*
   - *All p-groups are solvable. Proof: Induction on $k \in \mathbb{N}$ where $|P| = p^k$. P has a nontrivial normal abelian subgroup, namely, $Z(P)$. The quotient $P/Z(P)$ has order p^{k-1} so is solvable by induction hypothesis. Hence P is solvable.*

   Now suppose $|G| = 80$. By the Sylow Theorems, $n_5 = 1, 16$. We consider two cases:

   - *Suppose that $n_5 = 1$. Then G has a normal subgroup N of order 5. N is abelian and G/N has order 16 so is solvable as above. This makes G solvable.*
   - *Suppose that $n_5 = 16$ and $n_2 = 5$. Then, as usual, there are $16 \cdot 4 = 64$ elements of order 5. But this leaves only 16 elements of G for the Sylow 2-subgroups, each having order 16. Thus $n_2 = 1$ and G has a normal subgroup N of order $16 = 2^4$. This subgroup is solvable as above. The quotient G/N has order 5 so is abelian. This makes G solvable.*

13. (Algebra Comp F05) Let G be a group of order 242. Prove that G contains a nontrivial normal abelian subgroup H.

   `Answer:` $242 = 2 \cdot 11^2$. *By Sylow, $n_{11} = 1$ so G contains a unique normal subgroup H of order 11^2. Since H has prime squared order H is abelian.*

14. (Algebra Comp S06) Let G be a group, and N a normal subgroup of G such that

   (a) $N \neq G$

   (b) If S is a subgroup of G and $N \subseteq S$, then $S = N$ or $S = G$.

   Show that G/N is cyclic of prime order.

   `Answer:` *Let $\pi : G \to G/N$ be the natural homomorphism with $\ker \pi = N$. Suppose that $H \leq G/N$. Then $\pi^{-1}(H) = \{g \in G \mid \pi(g) \in H\}$ is a subgroup of G that contains N. By* (b), *$\pi^{-1}(H) = N$ or $\pi^{-1}(H) = G$. In the first case, H is the trivial subgroup of G/N; in the second case $H = G/N$. Thus the only subgroups of G/N are the trivial subgroup and G/N.*

To complete the proof we show that if K is a nontrivial group with the property that its only subgroups are $\{1\}$ and K, then K is cyclic of prime order. Since K is nontrivial, there is some element $1 \neq a \in K$. By construction the subgroup $\langle a \rangle$ is nontrivial and so $\langle a \rangle = K$. Now K is a cyclic group and so $K \cong \mathbb{Z}$ or $K \cong \mathbb{Z}_n$ for some $n \in \mathbb{N}$. But $\mathbb{Z}$ has infinitely many subgroups, and $\mathbb{Z}_n$ has as many subgroups as n has positive divisors. So we must have $K \cong \mathbb{Z}_n$ with $n \in \mathbb{N}$ having exactly two positive divisors. Of course this means that n is prime.

15. (Algebra Comp S06)

    (a) Identify a group of order 60 that is not solvable (You do not need to prove this).

    (b) Identify two groups of order 60 that are nonisomorphic, nonabelian, and solvable and verify that they do meet this criteria.

    `Answer:`

    (a) *Of course, A_5 is the answer. A_5 is simple and not abelian, so can't be solvable.*

    (b) *Some groups of this type:*

    $$S_3 \times \mathbb{Z}_{10} \qquad D_{12} \times \mathbb{Z}_5 \qquad D_{10} \times S_3$$

    $$D_{10} \times \mathbb{Z}_6 \qquad D_{30} \times \mathbb{Z}_2 \qquad D_{20} \times \mathbb{Z}_3$$

    To show that these are solvable groups you need to know that

    $$\{(1,1)\} \trianglelefteq H \times \{1\} \trianglelefteq H \times K$$

    for any groups H and K. To show that two of these groups are not isomorphic, you could calculate the numbers of elements of some particular order in each using $|(h,k)| = \mathrm{lcm}(|h|,|k|)$ for $(h,k) \in H \times K$. For example, $D_{12} \times \mathbb{Z}_5$ contains 8 elements of order 30, whereas $D_{10} \times S_3$ contains no elements of order 30.

16. (Algebra Comp F06) Let G be a group of order $175 = 5^2 \cdot 7$. Show that G is abelian.

    `Answer:` *By Sylow, n_5 divides 175 and n_5 is congruent to 1 modulo 5. The only number satisfying these conditions is $n_5 = 1$, and so G has a normal subgroup H of order 5^2. Similarly, n_7 divides 175 and n_7 is congruent to 1 modulo 7. The only number satisfying these conditions is $n_7 = 1$, and so G has a normal subgroup K of order 7. By the usual argument, $H \cap K = \{1\}$, and $G = HK \cong H \times K$. But, H has prime square order so is abelian, and K has prime order so is cyclic and abelian, and so G is abelian. In fact, either $G \cong \mathbb{Z}_{25} \times \mathbb{Z}_7$ or $G \cong \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7$.*

17. (Algebra Comp F06) Let G be a group and G' its commutator subgroup. Show that, if $G = G'$, then any homomorphism from G to $\mathbb{Z}$ is trivial.

    `Answer:` *Let $\phi : G \to \mathbb{Z}$ be a homomorphism. Then $G/\ker\phi \cong \phi(G) \leq \mathbb{Z}$. Since any subgroup of an abelian group is abelian, $G/\ker\phi$ is abelian. By NEED REF, $G' \leq \ker\phi \leq G$. Since $G' = G$, this implies that $\ker\phi = G$, that is, $\phi(g) = 0$ for all $g \in G$ and ϕ is trivial.*

18. (Algebra Comp S07) Show that any group of order 441 has a normal subgroup of order 49.

    `Answer:` *Let G be a group of order $441 = 3^2 \cdot 7^2$. By Sylow, n_7 divides 441 and n_7 is congruent to 1 modulo 7. The only number satisfying these conditions is $n_7 = 1$, and so G has a normal subgroup of order 7^2.*

19. (Algebra Comp S07) Let $\phi : G \to H$ be group homomorphism where G and H are finite groups such that the order of G and the order of H are relatively prime. Show that ϕ is trivial. (That is, show that $\phi(g) = e_H$ for all $g \in G$ where e_H is the identity element of H.)

`Answer:` *Let $n = |G|$ and $m = |H|$. Since $\gcd(m, n) = 1$, there are integers x, y such that $nx+my = 1$. Let $g \in G$. Then, by a corollary to Lagrange's theorem, $g^n = e_G$ and $(\phi(g))^m = e_H$. Now, using the fact that ϕ is a homomorphism, we get*

$$\begin{aligned}\phi(g) = \phi(g^1) = \phi(g^{nx+my}) = \phi(g^{nx}g^{my}) \\ = \phi(g^{nx})\phi(g^{my}) = \phi(g^n)^x(\phi(g)^m)^y = \phi(e_G)e_H = e_H.\end{aligned}$$

20. (Algebra Comp S07) Suppose that G is a group of order p^n where p is prime and $n \in \mathbb{N}$. Prove that, if the center of G has order p, then G contains no more than $p^{n-1} + p - 1$ conjugacy classes.

    `Answer:` *Since $|Z(G)| = p$, G has exactly p one-element conjugacy classes. All other conjugacy classes contain at least p elements. Since the union of these conjugacy classes contains $p^n - p$ elements, there can be at most $p^{n-1} - 1$ of these conjugacy classes. Thus G can have at most $p^{n-1} - 1 + p$ conjugacy classes in total.*

21. (Algebra Comp F07) Let G be a group of order 147. Prove that G contains a nontrivial normal abelian subgroup.

    `Answer:` *Note that $147 = 3 \cdot 7^2$. The number of Sylow 7-subgroups, n_7, satisfies $n_7 | 147$ and $n_7 \equiv 1 \mod 7$, and so $n_7 = 1$. Thus G has a unique normal Sylow 7-subgroup of order 7^2. Any group of prime squared order is abelian, so we are done.*

22. (Algebra Comp F07) Let p be a prime and assume G is a finite p-group.

    (a) Show that the center of G is nontrivial (i.e. $Z(G) \neq \{e\}$).

    (b) Let K be a normal subgroup of G of order p. Show that $K \subseteq Z(G)$.

    `Answer:`

    (a) Dummit and Foote, Theorem 8, p. 125.

    (b) Since K is normal, K is a union of congruence classes. The size of any congruence class must divide the order of G so is 1, p, p^2, etc. Because $\{1\}$ is a congruence class in K, and K has only p elements, all congruence classes in K must have one element. Elements that form one element congruence classes are in the center of G. Thus $K \subseteq Z(G)$.

Rings

1. (Algebra Comp S01) Let R be a ring with identity and assume that $x \in R$ has a right inverse. Prove that the following are equivalent:

    (a) x has more than one right inverse.

    (b) x is not a unit.

    (c) x is a left zero divisor.

    `Answer:` *If $R = \{0\}$ is the trivial ring with $1 = 0$. Then (a), (b), and (c) are all false for $x = 0 = 1$, and the equivalence of these conditions is true. Otherwise, we have a ring in which $1 \neq 0$. Then x has a right inverse means that $xy = 1$ for some $y \in R$. In particular, $x \neq 0$.*

    It is convenient to prove instead the equivalence of the negations of (a), (b) and (c). That is, we prove the equivalence of, (A) x has exactly one right inverse, (B) x is a unit, (C) x is not a left zero divisor.

    (A)$\Rightarrow$(B): Suppose that y is the only right inverse of x. Note that $x(y + 1 - yx) = xy + x - xyx = 1 + x - x = 1$ and so $y + 1 - yx$ is also a right inverse of x. Since there is only one right inverse we must have $y = y + 1 - yx$, which after cancellation implies that $yx = 1$. Since y is now a two sided inverse of x, x is a unit.

(B)⇒(C): Suppose that x is a unit with two sided inverse x^{-1} (In fact, given $xy = 1$, you can show that $x^{-1} = y$.) We show that x is not a left zero divisor. If $xr = 0$ for some $r \in R$, then $r = 1r = x^{-1}xr = x^{-1}0 = 0$. So x is not a left zero divisor. (Similarly, x is not a right zero divisor either.)

(C)⇒(A): Now suppose that x is not a left zero divisor. If z is a right inverse of x, then $xz = xy = 1$ and then $x(z - y) = 0$. Since x is not a left zero divisor, this implies that $z = y$, that is, y is the only right inverse of x.

Remark: The argument in S10 Rings C shows that if x has a right inverse and is not a unit, then x has infinitely many right inverses.

2. (Algebra Comp S01, F01, S02, S03 and F07) Let I be an ideal of a commutative ring R with $1 \neq 0$. Define the **radical** of I by
$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{N}\}.$$
   (a) Show that $\sqrt{I}$ is an ideal of R.
   (b) If I and J are ideals such that $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$.
   (c) $\sqrt{\sqrt{I}} = \sqrt{I}$.
   (d) If I and J are ideals, then $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

   `Answer:`

   (a) *It suffices to show that $\sqrt{I}$ is closed under addition and under multiplication by elements of R.*
   First we notice that, because $RI \subseteq I$, if $a^n \in I$, then all higher powers of a are in I. Now suppose that $a, b \in \sqrt{I}$. Then there is an integer $n \in \mathbb{N}$ such that $a^m \in I$ and $b^m \in I$ for all $m \geq n$. Then each term of the binomial expansion of $(a+b)^{2n}$ has a sufficiently high power of a or of b so that the term is in I. (Here we used $RI \subseteq I$.) Since I is closed under addition, $(a+b)^{2n} \in I$ and so $a + b \in \sqrt{I}$.
   Suppose that $a \in \sqrt{I}$ and $r \in R$. Then $a^n \in I$ for some $n \in \mathbb{N}$ and so $(ra)^n = a^n r^n \in I$. (Here we used $RI \subseteq I$.) Hence $ra \in \sqrt{I}$.

   (b) *Suppose that $r \in \sqrt{I}$. Then $r^n \in I$ for some $n \in \mathbb{N}$. Since $I \subseteq J$, we have $r^n \in J$ and hence $r \in \sqrt{J}$.*

   (c) *Note that, if $r \in I$, then $r^1 \in I$ and so $r \in \sqrt{I}$. Hence $I \subseteq \sqrt{I}$ and, by (b), $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$.*
   For the opposite inclusion, suppose that $r \in \sqrt{\sqrt{I}}$. Then $r^n \in \sqrt{I}$ for some $n \in \mathbb{N}$, and then $(r^n)^m \in I$ for some $m \in \mathbb{N}$. Since $r^{mn} \in I$, we have $r \in \sqrt{I}$. This shows that $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$.

   (d) *Since $I \cap J \subseteq I$, from (b), we get $\sqrt{I \cap J} \subseteq \sqrt{I}$. Similarly, $\sqrt{I \cap J} \subseteq \sqrt{J}$. Combing these containments we get $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$.*
   For the opposite containment, suppose that $r \in \sqrt{I} \cap \sqrt{J}$. Then there are $m, n \in \mathbb{N}$ such that $r^m \in I$ and $r^n \in J$. Since r^{mn} is in both I and in J, we have $r^{mn} \in I \cap J$ and so $r \in \sqrt{I \cap J}$.

3. (Algebra Comp S03) Let R be a commutative ring with identity 1 and let M be an ideal of R. Prove that M is a maximal ideal $\iff \forall r \in R - M, \exists x \in R$ such that $1 - rx \in M$.

   `Answer:` *See F08 and F12 solutions.*

4. (Algebra Comp S03) Let D be an Euclidean domain. Let a, b nonzero elements of D and d their GCD. Prove that $d = ax + by$ for some $x, y \in D$.

   `Answer:` *Dummit and Foote, Theorem 4, p. 275.*

5. (Algebra Comp F03) Let R be a ring with identity. Ideals I and J are called comaximal if $I+J=R$. Let $I_i, i=1,\ldots,n$ be a collection of ideals that are pairwise comaximal; i.e., for $i \neq j$, I_i and I_j are comaximal. Prove that for any k, $1 \leq k \leq n$, the ideals I_k and $\bigcap_{i \neq k} I_i$ are comaximal.

   `Answer:` *For notational convenience we prove the following (stronger) result: Suppose that $J, I_1, I_2, \ldots, I_n$ are ideals such that $J + I_k = R$ for all k. Then $J + (\bigcap_k I_k) = R$.*

   For each $k = 1, 2, \ldots, n$ there are elements $j_k \in J$ and $i_k \in I_k$ such that $j_k + i_k = 1$. The product of all these expressions gives $1 = \prod_k (j_k + i_k)$. Expanding this out, every term, except one, contains at least one of the j_k, and so such terms are in J. In addition, the sum of all these terms is also in J. The only term that is potentially not in J is $\prod_k i_k$. But this term is in $\bigcap_k I_k$. Thus 1 can be written as a sum of an element of J and an element of $\bigcap_k I_k$. That is, $1 = j + i$ with $j \in J$ and $i \in \bigcap_k I_k$.

   Now, if $r \in R$ we have $r = r(j+i) = rj + ri \in J + \bigcap_k I_k$. This means that $J + (\bigcap_k I_k) = R$.

6. (Algebra Comp F01 and F04) Let R be a commutative ring with identity. Assume $1 = e + f$, and $ef = 0$. Define $\Phi : R \to R$ by $\Phi(x) = ex$. Prove:

   (a) e is an idempotent (i.e. $e^2 = e$).

   (b) Φ is a ring homomorphism.

   (c) e is the identity of $\Phi(R)$ (the image of Φ).

   `Answer:`

   (a) $e = e1 = e(e+f) = e^2 + ef = e^2$.

   (b) Suppose $x, y \in R$. Then $\Phi(x+y) = e(x+y) = ex + ey = \Phi(x) + \Phi(y)$, and $\Phi(xy) = e(xy) = e^2(xy) = (ex)(ey) = \Phi(x)\Phi(y)$. Hence Φ is a ring homomorphism.

   (c) Let $x \in \Phi(R)$. Then $x = \Phi(y) = ey$ for some $y \in R$ and so $ex = e(ey) = (e^2)y = ey = x$. We have shown that $ex = x$ for all $x \in \Phi(R)$, that is, e is the identity of $\Phi(R)$.

7. (Algebra Comp F04) Let R be a nonzero ring such that $x^2 = x$ for all $x \in R$. Show that R is commutative and has characteristic 2.

   `Answer:` *Let $x, y \in R$. Then $x^2 = x$, $y^2 = y$ and $(x+y)^2 = x + y$. Expanding this last equation out and canceling gives $xy + yx = 0$. Setting $y = x$ in this equation and using $x^2 = x$ we get $x + x = 0$ for all $x \in R$. Thus R has characteristic 2 and also $x = -x$ for all $x \in R$. Going back to the equation $xy + yx = 0$, we now see that $xy - yx = 0$, or $xy = yx$ holds for all $x, y \in R$ and R is commutative.*

8. (Algebra Comp F04) Prove that if F is a field then every ideal of the ring $F[x]$ is principal.

   `Answer:` *Fraleigh, Theorem 27.24*

9. (Algebra Comp S04) Let R be the ring of functions from $\mathbb{R}$ to $\mathbb{R}$, the real numbers. Reminder: For $f, g \in R$, $f+g$ and fg are defined by $(f+g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $x \in \mathbb{R}$.

   (a) Show that $I = \{f \in R \mid f(0) = 0\}$ is an ideal of R which is maximal.

   (b) If $\mathbb{Z}[x]$ is the ring of polynomials over the integers $\mathbb{Z}$, show that $J = \{f \in \mathbb{Z}[x] \mid f(0) = 0\}$ is an ideal of $\mathbb{Z}[x]$ that is not maximal.

   `Answer:`

   (a) Let $\phi : R \to \mathbb{R}$ be defined by $\phi(f) = f(0)$. Then it is easy to check that ϕ is a surjective ring homomorphism with kernel $I = \{f \in R \mid f(0) = 0\}$. Thus I is an ideal and $R/I \cong \mathbb{R}$. Since $\mathbb{R}$ is a field, I is maximal.

   (b) Let $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ be defined by $\phi(f) = f(0)$. Then it is easy to check that ϕ is a surjective ring homomorphism with kernel $J = \{f \in \mathbb{Z}[x] \mid f(0) = 0\}$. (In fact, ϕ is an evaluation homomorphism.) Thus J is an ideal and $\mathbb{Z}[x]/J \cong \mathbb{Z}$. Since $\mathbb{Z}$ is not a field, J is not maximal.

10. (Algebra Comp S05) Let R be a subring of a field F such that, for every $x \in F$, either $x \in R$ or $x^{-1} \in R$. Prove that the ideals of R are linearly ordered; i.e., if I and J are ideals of R, then either $I \subseteq J$ or $J \subseteq I$.

`Answer:` *If $I \subseteq J$ we are done. Otherwise, $I \nsubseteq J$ and there exists some $i \in I$ such that $i \notin J$. Note that $i \notin J$ implies $i \neq 0$. We show that $J \subseteq I$.*

Suppose that $0 \neq j \in J$. Then $x = j^{-1}i$ is in F, so either $x = j^{-1}i \in R$ or $x^{-1} = ji^{-1} \in R$. In the first case, $j^{-1}i = r$ for some $r \in R$. But then $i = rj \in J$, contradicting $i \notin J$. Thus we have $ji^{-1} = r \in R$ and $j = ri \in I$. We have now shown that all nonzero elements of J are in I. Since $0 \in I$ in any case, we have $J \subseteq I$.

11. (Algebra Comp F06) Let $\mathbb{Z}_n[x]$ denote the ring of polynomials in x with coefficients in the ring of integers modulo n. Let $R = \mathbb{Z}_6[x]$. Let $I = (4) \subseteq R$. (In other words, I is the ideal in R generated by the constant 4.) Prove that:

    (a) The ring R/I is isomorphic to the ring $\mathbb{Z}_2[x]$

    (b) I is a prime ideal

    (c) I is not a maximal ideal.

`Answer:`

(a) There are reduction homomorphisms from $\mathbb{Z}[x]$ to $\mathbb{Z}_6[x]$ and from $\mathbb{Z}[x]$ to $\mathbb{Z}_2[x]$. Since the kernel of the first of these homomorphisms (6) is contained in the kernel of the second homomorphism (2), there is an induced surjective homomorphism from $\mathbb{Z}_6[x]$ to $\mathbb{Z}_2[x]$. This is essentially the Third Isomorphism Theorem of Dummit and Foote, Theorem 8, p. 246. The kernel of the homomorphism from $\mathbb{Z}_6[x]$ to $\mathbb{Z}_2[x]$ is $I = (2) = (4)$ and so $\mathbb{Z}_6[x]/I \cong \mathbb{Z}_2[x]$.

(b) Since $\mathbb{Z}_2$ is a field and a domain, $\mathbb{Z}_2[x]$ is a domain and I is a prime ideal. See Fraleigh, Theorem 27.15.

(c) Since $\mathbb{Z}_2[x]$ is not a field, I is not a maximal ideal. See Fraleigh, Theorem 27.9.

12. (Algebra Comp S07) Let R be a ring with indentity 1 and $a, b \in R$ such that $ab = 1$. Let $X = \{x \in R \mid ax = 1\}$. Show the following:

    (a) If $x \in X$, then $b + 1 - xa \in X$.

    (b) If $\phi : X \to X$ is defined by $\phi(x) = b + 1 - xa$ for $x \in X$, then ϕ is injective (one-to-one).

    (c) X contains either exactly one element or infinitely many elements. Hint: Recall the Pigeonhole Principle—an injective (one-to-one) function from a finite set to itself is surjective (onto).

`Answer:`

(a) If $x \in X$, then $ax = 1$. Hence $a(b+1-xa) = ab+a+axa = 1-a+1a = 1$, and so $b+1-xa \in X$.

(b) Suppose $\phi(x) = \phi(y)$ for some $x, y \in X$. Then $b+1-xa = b+1-ya$ and so $xa = ya$. Multiplying this by b, we get $xab = yab$, and, since $ab = 1$, $x = y$.

(c) First we note that if a is invertible, then $x \in X$ implies $ax = 1$ and hence $x = a^{-1}ax = a^{-1}$. So, in this case, $X = \{a^{-1}\}$.

Now suppose that a is not invertible. We show that there is no $x \in X$ such that $\phi(x) = b$. Solving $\phi(x) = b$, we get $xa = 1$. But since $ax = 1$ (because $x \in X$), this would imply that x is a^{-1}, contrary to our assumption that a is not invertible.

Since $b \in X$, this means that ϕ is not surjective (onto). Since ϕ is injective, this is only possible if X is infinite.

13. (Algebra Comp F07) Let R be a finite commutative ring with more that one element and with no zero divisors. Prove that R is a field.

`Answer:` *For each nonzero $a \in R$, define a function $\phi_a : R \to R$ by $\phi_a(x) = ax$ for all $x \in R$. We show that ϕ_a is injective. Suppose that $\phi_a(x) = \phi_a(y)$ for some $x, y \in R$. Then $ax = ay$ and so $a(x-y) = 0$. Since $a \neq 0$ and R has no zero divisors, this can only happen if $x - y = 0$, that is, $x = y$. Because R is finite and ϕ_a is injective, ϕ_a is also surjective. In particular, there is some $e \in R$ such that $\phi_a(e) = a$ that is $ae = a$.*

We show that e is the multiplicative identity element of R. Indeed, if $x \in R$, then $a(x - ex) = ax - aex = ax - ax = 0$, and, once again since a is not a zero divisor, we get $x = ex$. This shows that e is the multiplicative identity element of R, and so R is an integral domain. Finally, since ϕ_a is surjective, there is some element $b \in R$ such that $ab = e$, thus a has a multiplicative inverse. Since this is true of any nonzero element of R, R is a field.

Fields

1. (Algebra Comp S00) (Corrected from original!) Let E be an algebraic extension of a field F. Let $\alpha \in E$ and let $p(x)$ be the minimal polynomial of α over F with $\deg p(x) = 5$. Prove:

   (a) $F(\alpha^2) = F(\alpha)$.

   (b) If $\beta \in E$ and $[F(\beta) : F] = 3$, then $p(x)$ is the minimal polynomial for α over $F(\beta)$.

   `Answer:`

   (a) Since $\alpha^2 \in F(\alpha)$, we have $F \subseteq F(\alpha^2) \subseteq F(\alpha)$. Because $[F(\alpha) : F] = \deg_F \alpha = 5$, we have either $[F(\alpha^2) : F] = 5$ or $[F(\alpha^2) : F] = 1$. But $[F(\alpha^2) : F] = 1$ implies that $\alpha^2 \in F$, that is, $\alpha^2 - r = 0$ for some $r \in F$, and this means that $\deg_F \alpha \leq 2$, a contradiction. Hence $[F(\alpha^2) : F] = 5$, $[F(\alpha) : F(\alpha^2)] = 1$ and $F(\alpha^2) = F(\alpha)$.

   (b) Since $3 = \deg_F \beta$ and $5 = \deg_F \alpha$ are relatively prime, $[F(\alpha, \beta) : F] = 3 \cdot 5$ (see Algebra Comp S14), and we have

   $$\begin{array}{c} F \subseteq F(\beta) \subseteq F(\alpha, \beta) \\ \llcorner\, 3 \,\lrcorner\llcorner\, 5 \,\lrcorner \\ \llcorner\quad 15 \quad\lrcorner \end{array}$$

   Because $\deg_{F(\beta)} \alpha = [(F(\beta))(\alpha) : F(\beta)] = [F(\alpha, \beta) : F(\beta)] = 5$, the minimal polynomial for α over $F(\beta)$ has degree 5. But $p(x)$ has degree 5, has coefficients in $F(\beta)$, is monic and has α as a root, so $p(x)$ must be the minimal polynomial for α over $F(\beta)$.

2. (Algebra Comp S03) For some prime p, let $f(x)$ be an irreducible polynomial in $\mathbb{Z}_p[x]$, the ring of polynomials with coefficients in $\mathbb{Z}_p$. Prove that $f(x)$ divides $x^{p^n} - x$ for some n.

   `Answer:` *The splitting field F for f over $\mathbb{Z}_p$ is a finite field with characteristic p so has p^n elements for some $n \in \mathbb{N}$. (That is, $F = \mathbb{F}_{p^n}$.) The set of nonzero elements of F is a group (over multiplication) of order $p^n - 1$ and so $a^{p^n - 1} = 1$ for all nonzero $a \in F$. Multiplying this by a gives $a^{p^n} = a$, an equation that holds for all $a \in F$. Thus every element of F is a zero of $x^{p^n} - x$. In particular, every zero of f is a zero of $x^{p^n} - x$ and so f divides $x^{p^n} - x$.*

3. (Algebra Comp S04) Find a complex number α such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$. Prove your claim.

   `Answer:` *Almost any number in $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$ would do. But the claim is easiest to prove for $\alpha = \sqrt{3}\sqrt[3]{2}$. Certainly $\alpha \in \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$ and so $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$. Also $\sqrt{3} = \alpha^3/6 \in \mathbb{Q}(\alpha)$ and $\sqrt[3]{2} = \alpha^4/18 \in \mathbb{Q}(\alpha)$, and so $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) \subseteq \mathbb{Q}(\alpha)$.*

OR

Let $\alpha = \sqrt{3} + \sqrt[3]{2}$. Then, since $\alpha \in \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$, we get $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$. To prove the opposite inclusion, we notice that $(\alpha - \sqrt{3})^3 = 2$. That is, $\alpha^3 - 3\sqrt{3}\alpha^2 + 9\alpha - 2 - 3\sqrt{3} = 0$. Because $\alpha \in \mathbb{R}$, we have $\alpha^2 + 1 > 0$, and so the above equation can be solved for $\sqrt{3}$:

$$\sqrt{3} = \frac{\alpha^3 + 9\alpha - 2}{3(\alpha^2 + 1)} \in \mathbb{Q}(\alpha).$$

Then $\sqrt[3]{2} = \alpha - \sqrt{3}$ is also in $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) \subseteq \mathbb{Q}(\alpha)$.

4. (Algebra Comp F04) Show that the group of automorphisms of the rational numbers $\mathbb{Q}$ is trivial.

   `Answer:` *Let $\phi : \mathbb{Q} \to \mathbb{Q}$ be an automorphism. Let F be the fixed field of ϕ, that is, $F = \{q \in \mathbb{Q} \mid \phi(q) = q\}$. Then $1 \in F$ since 1 is fixed by any automorphism. Then, since F is an additive subgroup of $\mathbb{Q}$, the group generated by 1 is contained in F, that is, $\mathbb{Z} \subseteq F$. Further, since F is a field, F is closed under multiplication and division of nonzero elements, and so $\mathbb{Q} \subseteq F$. This means $F = \mathbb{Q}$, $\phi(q) = q$ for all $q \in \mathbb{Q}$, and the only automorphism is the identity function.*

5. (Algebra Comp S05) Let F be a finite field of $n = p^m$ elements. Find necessary and sufficient conditions to insure that $f(x) = x^2 + 1$ has a root in F; i.e., f is not irreducible over F.

   `Answer:` *Suppose first that p is an odd prime. Let F^* be the group of nonzero elements of F under multiplication. If $\alpha \in F$ is a root of f, then $\alpha \neq 1$ (because $p \neq 2$), $\alpha^2 = -1 \neq 1$ (because $p \neq 2$) and $\alpha^4 = 1$. That means α has order 4 in the group F^*. Conversely, if $\alpha \in F^*$ has order 4, then $\alpha \neq 1$, $\alpha^2 \neq 1$ and and $\alpha^4 = 1$. Since $0 = \alpha^4 - 1 = (\alpha^2 - 1)(\alpha^2 + 1)$ and $\alpha^2 - 1 \neq 0$, we have $\alpha^2 + 1 = 0$ and α is a root of f.*

   Thus f has a root if and only if F^* has an element of order 4. (This is all a consequence of f being the fourth cyclotomic polynomial.) Since F^* is a cyclic group (Fraleigh Corollary. 23.6), F^* has an element of order 4 if and only if its order is a multiple of 4, if and only if 4 divides $p^m - 1$, if and only if $p^m \equiv 1 \mod 4$. Now suppose that $p = 2$. Then F has characteristic 2 and $f(1) = 1^2 + 1 = 0$. So 1 is a root of f (and f is reducible: $f(x) = (x + 1)^2$).

6. (Algebra Comp S05) Find the minimal polynomial for $\alpha = \sqrt{5 + \sqrt{2}}$ over the field of rationals $\mathbb{Q}$ and prove it is minimal.

   `Answer:` *Since $\alpha^2 = 5 + \sqrt{2}$ and $(\alpha^2 - 5)^2 = 2$, α is a root of $f(x) = (x^2 - 5)^2 - 2 = x^4 - 10x^2 + 23 \in \mathbb{Q}[x]$. To show that f is irreducible over $\mathbb{Q}$ it suffices to notice that $f(x - 1) = x^4 - 4x^3 - 4x^2 + 16x + 14$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$. Hence f is the minimal polynomial for α over $\mathbb{Q}$.*

7. (Algebra Comp F05) Produce an explicit example of a field with 4 elements. Give its complete multiplication table. Hint: $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$.

   `Answer:` *Since $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$, $F = \mathbb{Z}_2[x]/(x^2 + x + 1)$ is a field. The elements of this field are $\bar{0} = 0 + (x^2 + x + 1)$, $\bar{1} = 1 + (x^2 + x + 1)$, $\bar{x} = x + (x^2 + x + 1)$ and $\bar{1} + \bar{x} = 1 + x + (x^2 + x + 1)$. The multiplication table is*

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{1} + \bar{x}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{1} + \bar{x}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{1} + \bar{x}$	$\bar{1}$
$\bar{1} + \bar{x}$	$\bar{0}$	$\bar{1} + \bar{x}$	$\bar{1}$	$\bar{x}$

8. (Algebra Comp F05) Let R be the ring of matrices of the form $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$ with $a, b \in \mathbb{Q}$ and usual matrix operations. Prove that R is isomorphic to $\mathbb{Q}(\sqrt{2})$.

`Answer:` *We know that every element of* $\mathbb{Q}(\sqrt{2})$ *can be written uniquely in the form* $a + b\sqrt{2}$ *with* $a, b \in \mathbb{Q}$. *So the function* $\phi : R \to \mathbb{Q}(\sqrt{2})$ *defined by*

$$\phi\left(\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}\right) = a + b\sqrt{2}$$

for $a, b \in \mathbb{Q}$ *is a bijection. It remains to show that* ϕ *is a homomorphism. The additive property is easy, so we confirm just the multiplicative property:*

$$\begin{aligned}
\phi\left(\begin{bmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{bmatrix}\right) &= \phi\left(\begin{bmatrix} a_1a_2 + 2b_1b_2 & a_1b_2 + b_1a_2 \\ 2(a_1b_2 + b_1a_2) & a_1a_2 + 2b_1b_2 \end{bmatrix}\right) \\
&= (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} \\
&= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) \\
&= \phi\left(\begin{bmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{bmatrix}\right)\phi\left(\begin{bmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{bmatrix}\right)
\end{aligned}$$

for all $a_1, a_2, b_1, b_2 \in \mathbb{Q}$.

9. (Algebra Comp S07) Let K be an extension field of F and $\alpha \in K$. Show that, if $F(\alpha) = F(\alpha^2)$, then α is algebraic over F.

   `Answer:` *If* $\alpha \in F(\alpha^2)$, *then* $\alpha = g(\alpha^2)/h(\alpha^2)$ *for some polynomials* $g, h \in F[x]$ *(with* $h \neq 0$*). Clearing denominators, we have* $\alpha h(\alpha^2) - g(\alpha^2) = 0$ *and so* α *is a zero of the polynomial* $f(x) = xh(x^2) - g(x^2) \in F[x]$. *Since the degree of* $g(x^2)$ *is even and the degree of* $xh(x^2)$ *is odd,* f *cannot be zero. Hence* α *is algebraic over* F.

10. (Algebra Comp S07) Let $\sigma = e^{2\pi i/7} \in \mathbb{C}$, and $F = \mathbb{Q}(\sigma)$. Describe the Galois group of F over $\mathbb{Q}$. Explain what theorems you are using. (Here $\mathbb{C}$ denotes the field of complex numbers, and $\mathbb{Q}$ denotes the field of rational numbers.)

    `Answer:` *The minimum polynomial for* σ *over* $\mathbb{Q}$ *is the seventh cyclotomic polynomial* $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. *The other zeros of this polynomial are* σ^k *with* $k = 2, 3, 4, 5, 6$, *and these zeros are all in* F. *This means that* F *is the splitting field for* Φ_7, *and that* F *is Galois over* $\mathbb{Q}$. *Since* Φ_7 *is irreducible over* $\mathbb{Q}$ *(as are all cyclotomic polynomials), all these zeros are conjugates of each other.*

    Each automorphism of F *over* $\mathbb{Q}$ *sends* σ *to one of its conjugates and is uniquely determined by this conjugate. Thus there six automorphisms. Let* ϕ *be the automorphism of* F *over* $\mathbb{Q}$ *that sends* σ *to* σ^3. *Then* $\phi^2(\sigma) = \phi(\sigma^3) = \sigma^2$, $\phi^3(\sigma) = \sigma^6$, $\phi^4(\sigma) = \sigma^4$, $\phi^5(\sigma) = \sigma^5$ *and* $\phi^6(\sigma) = \sigma$. *Thus each of the six automorphisms is a power of* ϕ. *In other words, the Galois group is cyclic of order 6 with* ϕ *as generator.*

11. (Algebra Comp F07) Let E be an extension field of F with $[E : F] = 7$.

    (a) Show that $F(\alpha) = F(\alpha^3)$ for all $\alpha \in E$.

    (b) Show that $F(\alpha) = F(\alpha^9)$ for all $\alpha \in E$.

    `Answer:` *Reminder:* $\deg(\alpha, F) = [F(\alpha) : F]$ *divides* $[E : F] = 7$. *So either* $\deg(\alpha, F) = [F(\alpha) : F] = 1$ *with* $F(\alpha) = F$ *and* $\alpha \in F$, *or* $\deg(\alpha, F) = [F(\alpha) : F] = 7$ *with* $F(\alpha) = E$ *and* $\alpha \notin F$.

    (a) If $\alpha \in F$, *then* $\alpha^3 \in F$ *and* $F(\alpha) = F(\alpha^3) = F$. *Otherwise,* α *is not in* F *and so* $\deg(\alpha, F) = 7$. *Because of this,* α^3 *cannot be in* F *either. (If* $\alpha^3 \in F$ *then the degree of* α *would be three or less.) Thus* $\deg(\alpha^3, F) = 7$ *and* $F(\alpha) = F(\alpha^3) = E$.

    (b) By (a), $F(\alpha) = F(\alpha^3) = F((\alpha^3)^3) = F(\alpha^9)$.