MATH 3030, Abstract Algebra
Winter 2012
Toby Kenney
Sample Midterm Examination
Model Solutions

Basic Questions

1. *Give an example of a prime ideal which is not maximal.*

   In the ring $\mathbb{Z} \times \mathbb{Z}$, the ideal $\{(0, a) | a \in \mathbb{Z}\}$ is prime but not maximal.

2. *Let $R = M_2(\mathbb{Z}_2)$, the ring of 2×2 matrices over $\mathbb{Z}_2$. What are the elements of the ideal generated by $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$?*

   We need to multiply by all 16 elements of R on each side to find all the elements of the ideal. We consider:

   $$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix}$$

   while

   $$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} b & d \\ 0 & 0 \end{pmatrix}$$

   so the entries of the ideal include all matrices of the forms

   $$\begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix}$$

   and

   $$\begin{pmatrix} b & d \\ 0 & 0 \end{pmatrix}$$

   and all sums of these matrices. Furthermore, they include all multiples of these matrices. For example,

   $$\begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ag & ah \\ cg & ch \end{pmatrix}$$

   So we get all matrices of rank 1. Finally, the ideal must be closed under addition, so we get all sums of matrices of rank 1. This gives all matrices in R.

3. *How many ring homomorphisms are there from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{90}$?*

   A ring homomorphism ϕ from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{90}$ is determined entirely by $\phi(1)$. This $\phi(1)$ must satisfy $\phi(1)^2 = \phi(1)$, and $12.\phi(1) = 0$. In $\mathbb{Z}_{90}$, the elements

that satisfy $12.x = 0$ are multiples of 15. Now in $\mathbb{Z}_{90}$, we have that $15^2 = 45$, so the squares of multiples of 15 are all multiples of 45, so the only possible values for $\phi(1)$ are 0 and 45. It is straightforward to check that these both have the required properties, so there are two homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{90}$.

4. *What is the dimension of $\mathbb{Q}(\sqrt{3}+\sqrt{2})$ as a vector space over $\mathbb{Q}(\sqrt{2})$?*

   We see that $(\sqrt{3}+\sqrt{2})^2 = 5+2\sqrt{6} = 2\sqrt{2}(\sqrt{3}+\sqrt{2})+1$, so 1 and $(\sqrt{3}+\sqrt{2})$ form a basis for $\mathbb{Q}(\sqrt{3}+\sqrt{2})$ as a vector space over $\mathbb{Q}(\sqrt{2})$, so its dimension is 2.

5. *Let α be a zero of $f(x) = x^2 - 2$ in GF(25). Find a generator of the multiplicative group of nonzero elements of GF(25).*

   We know that the multiplicative group of nonzero elements of GF(25) has 24 elements. Furthermore, we see that $\alpha^2 = 2$, $\alpha^4 = 4$ and $\alpha^8 = 1$, so α has order 8 in this group. We therefore need to find a cube root of α. We try $\alpha + 1$, and we get $(\alpha+1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1 = 2\alpha + 1 + 3\alpha + 1 = 2$ Therefore, $\alpha + 1$ has order 12. This leads us to try $\alpha(\alpha + 1) = \alpha + 2$, where we see $(\alpha + 2)^3 = \alpha^3 + \alpha^2 + 2\alpha + 3 = 4\alpha = \alpha^5$. Since 5 and 8 are coprime, α^5 has order 8, so $\alpha + 2$ has order 24, i.e. it is a generator of the multiplicative group.

6. *Show that $x^3 + x + 1$ has distinct zeros in the algebraic closure of $\mathbb{Z}_5$.*

   We know by trying all elements of $\mathbb{Z}_5$, that $x^3 + x + 1$ has no zeros in $\mathbb{Z}_5$, so it is irreducible over $\mathbb{Z}_5$. Let α be a zero of $x^3 + x + 1$ in the algebraic closure of $\mathbb{Z}_5$. Long division gives us $x^3+x+1 = (x-\alpha)(x^2+\alpha x+(\alpha^2+1))$. It is clear that α is not a zero of $x^2 + \alpha x + (\alpha^2 + 1)$, so we just need to show that its two zeros are not equal, i.e. that it is not the square of some $x - \beta$. However, since $(x - \beta)^2 = x^2 - 2\beta x + \beta^2$, the only possible β is 4α, and it is clear that this is not a zero of $x^2 + \alpha x + (\alpha^2 + 1)$.

   [We can complete the factorisation — using the quadratic formula, the zeros of $x^2+\alpha x+(\alpha^2+1)$ are $3(-\alpha\pm\sqrt{2\alpha^2+1})$. The difficulty is in finding $\sqrt{2\alpha^2+1}$. However, computing powers of α we see that $2\alpha^2 + 1 = \alpha^{17}$, and $\alpha^{31} = -1$, so one square root of $2\alpha^2 + 1$ is $2\alpha^{24} = 2\alpha^2 + 2\alpha + 3$. This gives a zero of $x^2 + \alpha x + (\alpha^2 + 1)$ as $\alpha^2 + 3\alpha + 4$ and the other zero as $4\alpha^2 + 2\alpha + 2$.]

7. *Let α be a zero of $x^3 + x^2 + 2$ over $\mathbb{Z}_3$. Find $\mathrm{Irr}(\alpha + 1, \mathbb{Z}_3)$.*

   We know that the irreducible polynomial must be of degree 3, since $\mathbb{Z}_3(\alpha)$ has degree 3 over $\mathbb{Z}_3$. We look at the first three powers of $\alpha + 1$, getting

$$
\begin{aligned}
1 &= 1 \\
\alpha + 1 &= \alpha + 1 \\
(\alpha + 1)^2 &= \alpha^2 + 2\alpha + 1 \\
(\alpha + 1)^3 &= 2\alpha^2 + 2
\end{aligned}
$$

Expressing $(\alpha + 1)^3$ as a linear combination of the other powers of $\alpha + 1$ gives $(\alpha+1)^3 = 2(\alpha+1)^2+2(\alpha+1)+1$, so $\mathrm{Irr}(\alpha+1, \mathbb{Z}_3) = x^3+x^2+x+2$.

8. *Show that the set of polynomials* $\{f \in \mathbb{Z}[x] | f(0)$ *is divisible by* $3\}$ *is an ideal in* $\mathbb{Z}[x]$*. Is it principal?*

   We need to show this set of polynomials is closed under addition, and multiplication by arbitrary polynomials. This is clear, because evaluation at zero is a ring homomorphism, and so if $f(0)$ and $g(0)$ are both divisible by 3, then so is $(f + g)(0) = f(0) + g(0)$, and if g is any polynomial in $\mathbb{Z}[x]$, then $g(0)$ is an integer, so if $f(0)$ is divisible by 3, then $g(0)f(0)$ is also divisible by 3.

   It is not a principal ideal, since the only polynomial that divides both the constant polynomial 3 and x is the constant polynomial 1, which is not in the ideal.

9. *Compute a composition series for* $D_5 \times D_4$*. Is* $D_5 \times D_4$ *solvable?*

   One composition series is $\mathbb{Z}_5 \times \{e\} \leqslant D_5 \times \{e\} \leqslant D_5 \times \mathbb{Z}_2 \leqslant D_5 \times \mathbb{Z}_4 \leqslant D_5 \times D_4$, where the cyclic groups are all groups of rotations.

   It is easy to see that the order of each factor group in this composition series is prime, so the factor group must be abelian. Therefore, $D_5 \times D_4$ is solvable.

10. *Find a basis for* $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ *over* $\mathbb{Q}$*.*

    Computing powers of $\sqrt{3} + \sqrt{5}$ gives

$$
\begin{aligned}
1 &= 1 \\
\sqrt{3} + \sqrt{5} &= \sqrt{3} + \sqrt{5} \\
(\sqrt{3} + \sqrt{5})^2 &= 8 + 2\sqrt{15} \\
(\sqrt{3} + \sqrt{5})^3 &= 18\sqrt{3} + 14\sqrt{5}
\end{aligned}
$$

    From this it is easy to see that $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ is of degree at least 4 over $\mathbb{Q}$, and contains $\sqrt{3}$, $\sqrt{5}$ and $\sqrt{15}$, so $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ form a basis.

    Alternatively, we can give the powers of $(\sqrt{3}+\sqrt{5})$ as a basis, i.e. $\{1, \sqrt{3}+\sqrt{5}, 8 + 2\sqrt{15}, 18\sqrt{3} + 14\sqrt{5}\}$, and we can confirm that $(\sqrt{3} + \sqrt{5})^4 = 124 + 32\sqrt{15}$ is a linear combination of these elements.

Theoretical Questions

Results from Notes

11. *Show that the composite of two ring homomorphisms is a ring homomorphism.*

    Let $f : R \longrightarrow S$ and $g : S \longrightarrow T$ be two ring homomorphisms. We need to show that the composite $gf : R \longrightarrow T$ is a ring homomorphism. That is, we need to show that for any $x, y \in R$, $gf(x + y) = gf(x) + gf(y)$ and $gf(xy) = gf(x)gf(y)$. Now we have $gf(x + y) = g(f(x) + f(y)) = gf(x) + gf(y)$ and $gf(xy) = g(f(x)f(y)) = gf(x)gf(y)$.

12. *Prove that for a field F, every ideal in the polynomial ring $F[x]$ is principal.*

    Let I be an ideal in $F[x]$. If I is the zero ideal, then the result is obvious. Let f be a non-zero polynomial of smallest degree n in I (i.e. all polynomials in I are of degree at least n). We will show that any other polynomial g in I is divisible by f, since by the division algorithm, we have that $g = qf + r$ where either $r = 0$ or the degree of r is less than the degree of f. However, since $g \in I$ and $f \in I$, we have that $r = g - qf \in I$, and since n is the smallest degree of a non-zero polynomial in I, and r has degree less than n, this means that $r = 0$. Therefore, $g = qf$. Since g is an arbitrary element of I, we have shown that I is the principal ideal generated by f.

13. *Prove that if R is a commutative unital ring, and I is an ideal of R, then R/I is a field if and only if I is maximal.*

    Let I be maximal. Then for any non-zero coset $x + I \in R/I$, we can consider the ideal generated by this coset — that is, the ideal $\{xa + I | a \in R\}$. The union of these cosets gives an ideal of R containing I. Since I is maximal, this must be the improper ideal. In particular, it must contain the coset $1 + I$, so we have that $1 + I = xa + I$ for some $a \in R$. This means that $a + I$ is an inverse for $x + I$ in R/I, so $x + I$ is a unit, and so R/I is a field.

    Conversely, suppose R/I is a field. Now if J is an ideal of R properly containing I, then the set $\{x + I | x \in J\}$ is a non-zero ideal of R/I. However, since R/I is a field, if K is a non-zero ideal in R/I then it contains some element $y + I$ of R/I, and for any $z + I \in R/I$, we have $z + I = (y + I)(y + I)^{-1}(z + I) \in K$. Therefore the only non-zero ideal in a field is the improper ideal. If $\{x + I | x \in J\}$ is the improper ideal, then we must have that J is the improper ideal in R. Since J was an arbitrary ideal of R properly containing I, this means that I is maximal.

14. *Prove that if R is a commutative unital ring, and I is an ideal of R, then R/I is an integral domain if and only if I is prime.*

Since R is commutative and unital, R/I is also commutative and unital, so we just need to show that R/I has no zero divisors if and only if I is prime. However, a zero divisor in R/I consists of a pair of cosets $x+I$ and $y+I$ with the property that $xy+I=I$, but neither $x+I$ nor $y+I$ is the ideal I. Asserting that no such cosets exist is exactly the definition of I being a prime ideal.

15. *Prove that given a field F, and a non-constant polynomial $f \in F[x]$, there is an extension field E of F containing a zero of f.*

    We know that f can be written as a product of irreducible polynomials, and that a zero of any one of these irreducible factors is a zero of f. Therefore, it is sufficient to prove the result for an irreducible polynomial f. In this case, we know that $\langle f \rangle$ is a maximal ideal in $F[x]$, so $F[x]/\langle f \rangle$ is a field. It is an extension field of F because the cosets of constant polynomials form a subfield isomorphic to F. In this field, the element $x+\langle f \rangle$ is a zero of f, since evaluating f at this element gives $f+\langle f \rangle = \langle f \rangle$.

16. *Prove that if E is a finite extension of F and K is a finite extension of E, then K is a finite extension of F and*

$$[K:F] = [K:E][E:F]$$

    Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for E over F and let $\{\beta_1, \ldots, \beta_m\}$ be a basis for K over E. Then it is sufficient to show that $\{\alpha_i\beta_j | 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$ is a basis for K over F. Let $x \in K$. We have $x = e_1\beta_1 + \cdots + e_m\beta_m$, for some $e_1, \ldots, e_m \in E$, since $\{\beta_1, \ldots, \beta_m\}$ is a basis for K over E. Now since $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for E over F, for each e_i we have $e_i = a_{i1}\alpha_1 + \cdots + a_{in}\alpha_n$ for some $a_{i1}, \ldots, a_{in} \in F$. Substituting these equations gives $x = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}\alpha_i\beta_j$, so these span K. suppose we have $0 = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}\alpha_i\beta_j$ for some $a_{ij} \in F$. For each j, we have that $\sum_{i=1}^{n} a_{ij}\alpha_i \in E$, so we have a linear combination of the β_j over E equal to zero. Since the β_j are linearly independent over E, this gives $\sum_{i=1}^{n} a_{ij}\alpha_i = 0$. Since the α_i are linearly independent over F, this means that each $a_{ij} = 0$. Therefore, the products $\alpha_i\beta_j$ are linearly independent over F.

17. *Prove that the number of elements in a finite field is always a prime power.*

    Let F be a finite field. The characteristic of F is not zero, so must be a prime p. Taking all elements of F which can be obtained by adding 1, we get a subfield isomorphic to $\mathbb{Z}_p$. We therefore have that F is a finite extension of $\mathbb{Z}_p$. Let the dimension be n, and let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for F over $\mathbb{Z}_p$. Every element of F can be written uniquely as $a_1\alpha_1 + \cdots + a_n\alpha_n$ for some $a_1, \ldots, a_n \in \mathbb{Z}_p$. There are p choices for each a_i, so there are p^n possible choices in total. Therefore, F has p^n elements, which is a prime power.

18. *Show that a subgroup of a solvable group is solvable.*

Let G be a solvable group, and let H be a subgroup of G. Let $\{e\} \leqslant G_1 \leqslant \cdots \leqslant G_n = G$ be a composition series for G. Now consider $\{e\} \leqslant G_1 \cap H \leqslant \cdots \leqslant G_n \cap H = H$. We know that this is a subnormal series for H. By the second isomorphism theorem applied to the subgroup $(G_{i+1} \cap H)$ of G_{i+1}, and the normal subgroup G_i, we know that $(G_{i+1} \cap H)/(G_i \cap H) \cong ((G_{i+1} \cap H)G_i)/G_i$. Now $(G_{i+1} \cap H)G_i/G_i$ is a subgroup of G_{i+1}/G_i, which is simple (since the series is a composition series), and abelian, since G is solvable. This means it is cyclic of prime order, so that either $(G_{i+1} \cap H)/(G_i \cap H) \cong G_{i+1}/G_i$ or $(G_{ı+1} \cap H)/(G_i \cap H)$ is the trivial group. Therefore, we see that, identifying equal elements in the series, we get a composition series for H. Furthermore, the quotients in this series are all quotients in the composition series for G. Therefore, they are all abelian, so H is solvable.

19. *Show that a field of characteristic $p \neq 0$ contains a subfield isomorphic to $\mathbb{Z}_p$.*

Let F be a field of characteristic $p \neq 0$. Consider the set of elements $\{s_n = \underbrace{1 + \cdots + 1}_{n} | n = 0, 1, \ldots, p-1\}$. This set is closed under addition, and as an additive subgroup is isomorphic to $\mathbb{Z}_p$. This set is also closed under multiplication, since $1^2 = 1$, so by applying the distributive law, we get that $s_n s_m = s_{nm}$, with the remainder modulo p being taken if necessary. This multiplication agrees with the multiplication in $\mathbb{Z}_p$, so this subset is a subfield isomorphic to $\mathbb{Z}_p$.

20. *Show that for an extension field E of F, and an element $\alpha \in E$, algebraic over F, there is an irreducible polynomial $p \in F[x]$ such that $p(\alpha) = 0$, and that this p is unique up to multiplication by a constant.*

Evaluation at α is a homomorphism, so the set of polynomials of which α is a zero is the kernel of this homomorphism, so is an ideal in $F[x]$. Since α is algebraic over F, it is a non-zero ideal. All ideals in $F[x]$ are principal, so this set of polynomials is $\langle f \rangle$, for some $f \in F[x]$. We want to show that this f is irreducible. Suppose we have that $f = gh$, then we must have that α is a zero of g or α is a zero of h. W. l. o. g., suppose that α is a zero of g. This means that $g \in \langle f \rangle$, or f divides g. Since g divides f, this gives that g is a constant polynomial times f, so f is irreducible. Since all polynomials of which α is a zero are divisible by f, the only irreducible such polynomials are constant multiples of f.

21. *Show that any finite extension field E of a field F is algebraic over F.*

Let the dimension of E over F be n. Let $\alpha \in E$, and consider the set $\{1, \alpha, \ldots, \alpha^n\}$. Since this has $n+1$ elements, it can't be linearly independent, so there is some linear combination $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, where $a_0, \ldots, a_n \in F$. This means that α is a zero of $a_0 + a_1 x + \cdots + a_n x^n$ in $F[x]$, so α is algebraic over F. Therefore, E is algebraic over F.

22. *(a) Show that if K is an algebraic extension of E, and E is an algebraic extension of F, then K is an algebraic extension of F.*

Let $\alpha \in K$. Since K is algebraic over E, α is algebraic over E. Let $\mathrm{Irr}(\alpha, E) = \beta_0 + \beta_1 x + \cdots + \beta_n x^n$. Since E is algebraic over F, each β_i is algebraic over F, so $F(\beta_0, \beta_1, \ldots, \beta_n)$ is a finite extension of F. Since α is a zero of $\beta_0 + \beta_1 x + \cdots + \beta_n x^n$, it is algebraic over $F(\beta_0, \ldots, \beta_n)$, so $F(\beta_0, \ldots, \beta_n, \alpha)$ is a finite extension of F, and therefore an algebraic extension of F. Since α is in an algebraic extension of F, it is algebraic over F. Every $\alpha \in K$ is algebraic over F, so K is algebraic over F.

(b) Deduce that if M is a maximal algebraic extension of F (i.e. M is not a proper subfield of any other algebraic extension of F) then M is algebraically closed.

Let $f \in M[x]$ be a non-constant polynomial. By Kronecker's theorem, there is an extension field N of M containing a zero α of f. Now $M(\alpha)$ is an algebraic extension of M. Since M is algebraic over F, $M(\alpha)$ is also algebraic over F. Since M is a maximal algebraic extension of F, it cannot be properly contained in $M(\alpha)$, so we deduce that $M(\alpha) = M$, or equivalently, $\alpha \in M$. This means that f has a zero in M. Since every non-constant f has a zero in M, M is algebraically closed.

23. *Show that it is not possible to construct a line segment of length $\sqrt[3]{2}$, starting from a line segment of length 1, and using only a straight-edge and compass.*

A single construction with a straight-edge and compass produces either an element of the current field of constructed numbers, or in an extension field of degree 2. Therefore, the field F generated by any finite set of constructible numbers has degree 2^n over $\mathbb{Q}$, for some n. Any constructible length α lies in a subfield $\mathbb{Q}(\alpha)$, which must satisfy

$$2^n = [F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

so $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ must divide 2^n, so it must be a power of 2. However, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ is not a power of 2, so $\sqrt[3]{2}$ is not a constructible length.

24. *Describe how to construct a finite field with p^n elements for a prime p as a subfield of $\overline{\mathbb{Z}_p}$, and explain what steps are needed to show that this is indeed a field with p^n elements.*

Let F be a finite field with p^n elements. We know that since the multiplicative group of non-zero elements of F has order $p^n - 1$, every element of this group must have order dividing $p^n - 1$, so it must be a zero of $x^{p^n - 1} - 1$. Therefore, every element of F is a zero of $x^{p^n} - x$. Therefore, F must be the subset of zeros in $\overline{\mathbb{Z}_p}$ of $x^{p^n} - x$. We need to show that this is a field with p^n elements. We need to show that for two zeros α and β of $x^{p^n} - x$, $-\alpha$, $\alpha + \beta$, $\alpha\beta$ and if $\alpha \neq 0$, α^{-1} are zeros of $x^{p^n} - x$. These are all easy, except for $\alpha + \beta$, where we use the binomial expansion and the

fact that $\overline{\mathbb{Z}_p}$ has characteristic p to show that $(\alpha+\beta)^p = \alpha^p + \beta^p$, then use induction on n. We also need to show that it has p^n elements. We know that, counting multiplicities, $x^{p^n} - x$ has p^n zeros in $\overline{\mathbb{Z}_p}$, so we just need to show that it has no repeated zeros. This can be done using long division — if α is a zero, then $x - \alpha$ is a factor, so we divide through by $x - \alpha$, and show that α is not a zero of the quotient.

25. State and prove the second isomorphism theorem.

Theorem 1 (Second isomorphism theorem)**.** *Let G be a group, let H be a subgroup of G, and let N be a normal subgroup of G. Then $H \cap N$ is a normal subgroup of H, and we have an isomorphism*

$$HN/N \cong H/(H \cap N)$$

Proof. A coset of HN/N is represented by an element x of HN. We can write x as hn for some $h \in H$ and $n \in N$. The isomorphism we are looking for is $\phi : HN/N \longrightarrow H/(H \cap N)$ that sends the coset hnN to the coset $h(H \cap N)$. We need to show that this is a well-defined function, i.e. that if hnN and $h'n'N$ are the same coset of N, then $h(H \cap N)$ and $h'(H \cap N)$ are the same coset of $H \cap N$. If hnN and $h'n'N$ are the same coset of N, then we have that $hnn'^{-1}h'^{-1} \in N$. Since N is normal, and $nn'^{-1} \in N$, we have that $nn'^{-1}h'^{-1} = h'^{-1}n''$ for some $n'' \in N$. This gives that $hh'^{-1} \in N$. We also know that $hh'^{-1} \in H$, since both h and h' are. This means that $hh'^{-1} \in H \cap N$, so $h(H \cap N)$ and $h'(H \cap N)$ are the same coset of $H \cap N$. Thus ϕ is a well-defined function. It is easy to check that it is a group homomorphism, since $\phi(h_1n_1Nh_2n_2N) = \phi(h_1n_1h_2n_2N) = \phi(h_1h_2n_3n_2N)$, for some $n_3 \in N$. By definition, $\phi(h_1h_2n_3n_2N) = h_1h_2(H \cap N) = h_1(H \cap N)h_2(H \cap N) = \phi(h_1n_1N)\phi(h_2n_2N)$. Finally, we need to check that ϕ is one-to-one and onto. Suppose $phi(hnN) = H \cap N$, then we have that $h(H \cap N) = (H \cap N)$, so $h \in H \cap N$. This means that $hn \in N$, so $hnN = N$. Therefore, $\ker(\phi) = \{N\}$, so ϕ is one-to-one. Consider a coset $h(H \cap N)$ in $H/(H \cap N)$. We know that $h = he \in HN$, and we have $\phi(hN) = h(H \cap N)$, so ϕ is onto. □

26. State and prove the third isomorphism theorem.

Theorem 2 (Third isomorphism theorem)**.** *Let G be a group, let N be a normal subgroup of G, and let K be a subgroup of N that is normal in G. Then we have an isomorphism*

$$G/N \cong (G/K)/(N/K)$$

Proof. We define the isomorphism $\phi : G/N \longrightarrow (G/K)/(N/K)$ by $\phi(xN) = xK(N/K)$. We need to show that this is a well-defined function, a homomorphism, and one-to-one and onto. Suppose $xN = yN$, we need to show

that $xK(N/K) = yK(N/K)$, that is, we need to show that $(xK)(yK)^{-1} \in N/K$. We know that $(xK)(yK)^{-1} = xy^{-1}K$, and since $xN = yN$, we know that $xy^{-1} = n \in N$, so since $n \in N$, we have that $nK \in N/K$, and ϕ is well-defined. We also know that $\phi(xNyN) = \phi(xyN) = xyK(N/K) = (xK)(yK)(N/K) = (xK(N/K))(yK(N/K)) = \phi(xN)\phi(yN)$, so ϕ is a homomorphism. Finally, if $\phi(xN) = N/K$, then $xK(N/K) = N/K$, so $xK \in N/K$, so $xK = nK$ for some $n \in N$, and therefore, $xn^{-1} \in K \subseteq N$. This give that $x \in N$, so $xN = N$. Therefore, $\ker(\phi) = \{N\}$, so ϕ is one-to-one. Finally, let $xK(N/K) \in (G/K)/(N/K)$, then we have that $\phi(xN) = xK(N/K)$, so ϕ is onto. □

New questions

27. Let E be an extension of F. Let $\alpha \in E$ be algebraic over F, and let $\beta \in E$ be transcendental over F. Must β be transcendental over $F(\alpha)$? Give a proof or a counterexample.

β must be transcendental over $F(\alpha)$. If it were algebraic, then $[F(\alpha, \beta) : F(\alpha)]$ would be finite, and since $[F(\alpha) : F]$ is also finite, we would have $[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F]$ is also finite, and since $F(\beta)$ is a subspace of $F(\alpha, \beta)$ over F, it would also be finite, making β algebraic over F, contradicting the given condition.

28. Let E be algebraically closed. Let F be a subfield of E. Show that the algebraic closure of F in E is algebraically closed.

Let K be the algebraic closure of F in E and let $f \in K[x]$. Since E is algebraically closed, it contains a zero of f. Let α be a zero of f in E. Then we have that $K(\alpha)$ is algebraic over K, and therefore, algebraic over F. This implies that α is algebraic over F, but since K is the algebraic closure of F in E, we must have $\alpha \in K$. That is, any polynomial in $K[x]$ has a zero in K, i.e. K is algebraically closed.

29. Prove that the only irreducible polynomials in $\mathbb{R}[x]$ have degree at most 2. [You may assume the fundamental theorem of algebra — the complex numbers are algebraically closed.]

Let f be an irreducible polynomial in $\mathbb{R}[x]$. Since $\mathbb{C}$ is algebraically closed, f factors into a product of linear polynomials in $\mathbb{C}[x]$. By adjoining the zeros of f to $\mathbb{R}$, we get a subfield of $\mathbb{C}$ isomorphic to $\mathbb{R}[x]/\langle f \rangle$. Since $[\mathbb{C} : \mathbb{R}] = 2$, we must have $[\mathbb{R}[x]/\langle f \rangle : \mathbb{R}] \leqslant 2$, i.e. the degree of f is at most 2.

30. Show that no finite field is algebraically closed.

Let F be an algebraically closed finite field. Suppose F has p^n elements. We know that F is isomorphic to the subfield of $\overline{\mathbb{Z}_p}$ consisting of the zeros of $x^{p^n} - x$. We also know that there is a field E with p^{2n} elements, consisting of all the zeros of $x^{p^{2n}} - x$ in $\overline{\mathbb{Z}_p}$. Since $p^n - 1$ divides $p^{2n} - 1$,

we have that $x^{p^n-1}-1$ divides $x^{p^{2n}-1}-1$, so $x^{p^n}-x$ divides $x^{p^{2n}}-x$. Therefore E is an extension of F, and since E is finite, it is a finite extension of F, and therefore an algebraic extension. However, if F were algebraically closed, the only algebraic extension would be F itself. This is a contradiction, so F cannot be algebraically closed.

31. *Show that for any n, and any prime p, there is an irreducible polynomial of degree n in $\mathbb{Z}_p$.*

    We know there is a field of p^n elements, and this field is an extension of degree n of $\mathbb{Z}_p$. We also know that the multiplicative group of this field is cyclic. Let α be a generator of this multiplicative group. We know that $\mathrm{Irr}(\alpha, \mathbb{Z}_p)$ is an irreducible polynomial of degree $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n$ over $\mathbb{Z}_p$.

32. *Show that any non-zero ring homomorphism between two fields is one-to-one.*

    If $\phi : F \longrightarrow E$ is a non-zero ring homomorphism between two fields, then we know that the kernel of ϕ is an ideal of F. Since F is a field its only ideals are the trivial ideal and the improper ideal. If the kernel of ϕ were the improper ideal, ϕ would be the zero homomorphism, so the kernel of ϕ must be the trivial ideal, which means that ϕ is one-to-one.

33. *Show that any algebraic extension of $\mathbb{R}$ is either $\mathbb{R}$, or else is isomorphic to $\mathbb{C}$. [Hint: the only irreducible polynomials in $\mathbb{R}$ are quadratic or linear.]*

34. *Show that the direct product of two solvable groups is solvable.*

    Let G and H be solvable groups. Let $\{e\} \leqslant G_1 \leqslant \cdots \leqslant G_n = G$, and $\{e\} \leqslant H_1 \leqslant \cdots \leqslant H_m = H$ be composition series for G and H. $G \times \{e\}$ is a normal subgroup of $G \times H$, and for two subgroups K and L of H, if K is a normal subgroup of L, then $G \times K$ is a normal subgroup of $G \times L$. Therefore

    $$\{e\} \leqslant G_1 \times \{e\} \leqslant \cdots \leqslant G \times \{e\} \leqslant G \times H_1 \leqslant \cdots \leqslant G \times H$$

    is a subnormal series for $G \times H$. (In fact it is a composition series). Furthermore, the quotient groups are all quotient groups from either the composition series of G, or the composition series of H, so they are abelian and simple, so this series is a composition series, and all the groups are abelian. Therefore, $G \times H$ is solvable.

35. *Show that the set of elements x satisfying $x^n = 0$ for some n is an ideal in any commutative ring R.*

    We need to show that this set is closed under addition, additive inverses, and multiplication by arbitrary elements of R. If $x^n = 0$ and $y^m = 0$ in R, then we have $(-x)^n = 0$ and $(x+y)^{n+m-1} = 0$ by the binomial expansion — each term is divisible by either x^n or y^m. Finally, if a is any element of R, since R commutes, we have $(ax)^n = a^n x^n = 0$. Therefore the set of elements x satisfying $x^n = 0$ for some n is an ideal.

36. Let R be a commutative ring, and let $a \in R$. Show that the set $\{x \in R | ax = 0\}$ is an ideal in R.

We need to show that this set is closed under addition, additive inverses, and multiplication by arbitrary elements of R. If $ax = 0$ and $ay = 0$, then the distributive law gives $a(x + y) = ax + ay = 0 + 0 = 0$ and $a(-x) = -ax = 0$. Finally, for any $z \in R$, we have $a(xz) = (ax)z = 0z = 0$, so the set $\{x \in R | ax = 0\}$ is an ideal in R.

37. Let α be a primitive root of unity in GF(p^n). Show that $\deg(\alpha, \mathbb{Z}_p) = n$.

Since α is a primitive root of unity, we have that $\mathbb{Z}_p(\alpha) \cong \mathrm{GF}(p^n)$, so we have $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n$, but this is $\deg(\alpha, \mathbb{Z}_p)$.