Exercise solutions to Abstract Alebra

Don't just copy solutions, but do the problems by yourself first.

Note: References may be in a mess. All outside references refer either to Dummit & Foote "Abstract Algebra" or S. Lang "Algebra" And, of course, I am not claiming that all solutions are correct. In fact, there ARE errors that I was too lazy to fix (most can be easily spotted and fixed anyway). Have fun!

Most problems come from the aforementioned books.

Throughout $|f|$ denotes the degree of the polynomial f.

Problem 1. Let α be a real number such that $\alpha = 5$. Show that:

(i) $\mathbb{Q}(i\alpha^2)$ is normal over $\mathbb{Q}$.
(ii) $\mathbb{Q}(\alpha + i\alpha)$ is normal over $\mathbb{Q}(i\alpha^2)$.
(iii) $\mathbb{Q}(\alpha + i\alpha)$ is not normal over $\mathbb{Q}$.

Solution 1. (i) Observe that $f(x) = x^2 + 5$ is irreducible over $\mathbb{Q}$ since it is Eisenstein over $\mathbb{Z}$. Further, $i\alpha^2$ is a root of this polynomial. Hence the extension $\mathbb{Q}(i\alpha^2)$ is of degree 2. But every second degree extension is normal.

(ii) Observe that $g(x) = x^2 - 2i\alpha^2 \in \mathbb{Q}(i\alpha^2)[x]$ has $\alpha + i\alpha$ as a root. Now, $\mathbb{Q}(\alpha + i\alpha)$ is an extension of degree either 1 or 2 over $\mathbb{Q}(i\alpha^2)$, depending on wether g is reducible or not over $\mathbb{Q}(i\alpha^2)$ (actually it is irreducible, but we don't need to go that far). In any case, the extension is normal.

(iii) Ovserve that the polynomial $h(x) = x^4 + 10$ is satisfied by $\alpha + i\alpha$. Hence the extension $\mathbb{Q}(\alpha + i\alpha)$ over $\mathbb{Q}$ is of degree at most 4. Now, if this extension was normal, it would contain all roots of $h(x)$. Since $\alpha + i\alpha$ is a root, and complex roots come in conjugate pairs, $\alpha - i\alpha$ would also be contained in it. But then both, α and i would be contained in the extension. That is, $\mathbb{Q}(\alpha, i) \subset \mathbb{Q}(\alpha + i\alpha)$. But this cannot be, since $\mathbb{Q}(\alpha + i\alpha)$ is of degree at most 4, but $\mathbb{Q}(\alpha, i)$ is of degree 8 over $\mathbb{Q}$. So, $\mathbb{Q}(\alpha + i\alpha)$ is not normal. □

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Problem 2. Let $\text{char}(K) = p$. Let L be a finite extension of K, and suppose that $[L : K] = q$ is relatively prime to p. Show that L is separable over K.

Solution 2. Since L is a finite extension over K, we know that $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n$ algebraic over K. It remains to show that each α_j is separable over K. Let $m(x)$ be the minimal polynomial of α_j over K. Suppose to the contrary that $m(x)$ is not separable. But then D_m, the derivative of m, and m are not relatively prime. Since m is irreducible, we must have $m|D_m$. In this case, since $|D_m| < |m|$, we must have $D_m = 0$. But then $m(x) = l(x^p)$ for some polynomial $l(x)$. In this case p divides $|m|$. But $|m|$, being the degree of α_j, divides q. So p divides q. This can't be, since by hypothesis $(p, q) = 1$. So α_j is separable. □

Problem 3. Suppose that $\text{char}(K) = p$. Let $a \in K$. If a has no p-th root in K, show that $x^{p^n} - a$ is irreducible in $K[x]$ for all positive integers n.

Solution 3.

Lemma 1. *Suppose that $\phi : K[x] \to \tilde{K}[x]$ is an injective homomorphism. Then if $f(x) \in K[x]$ is irreducible, then so is $\phi(f(x))$.*

Proof. An injective homomorphism is an isomorphism onto its image. □

Suppose that $n = 1$. Suppose further that $h(x) = x^p - a = f(x)g(x)$ for polynomials $f(x)$, $g(x)$ of degrees n, m respectively, with $p > n, m \geq 1$. Now, since $D_x h = 0$, the derivative of h, we see that $0 = D_x fg = g(x)D_x f + f(x)D_x g$. Since f and g are monic of degree $< p$, we see that $D_x f$ and $D_x g$ are of degrees $n - 1, m - 1$ respectively. But then, since $g(x)D_x f + f(x)D_x g = 0$, we must have $|gD_x f| = |fD_x g|$. So $n(m-1) = m(n-1)$. So $n = m$. Hence $2n = p$. But this can only happen when $n = m = 1$ and $p = 2$. But then in this case there is a b such that $b^2 = a$. But this cannot be by assumption! So h is irreducible.

Now, suppose that $n \geq 1$. Consider the injective homomorphism $\phi : K[x] \to K[x]$ defined by $x \mapsto x^{p^{n-1}}$. By above, $x^p = a$ is irreducible in $K[x]$. But by Lemma 1, $x^{p^n} - a = \phi(x^p - a)$ must also be irreducible in $K[x]$. □

Problem 4. Let K be an algebraic extension of F. Show that every subring of E which contains F is actually a field. Is this necessarily true if E is not algebraic over F? Prove or give a counterexample.

Solution 4. Suppose that r is an element of E. Since r is algebraic over F of degree–say–n, the finite field extension $F(r)$ given by all linear combinations $f_{n-1}r^{n-1} + \cdots + f_0$, with f_j in F, is in E. Since $F(r)$ is a field containing r, we see that $1/r$ is also in E. This is true for every nonzero element of E. So E is a field.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

On the other hand, suppose that K is not algebraic over F. Then there is a transcendental element, say ξ of K over F. Consider the ring $E = F[\xi]$. Clearly this ring contains F and is contained in K. But since ξ is transcendental over F, no finite combination $f_n\xi^n + \cdots + f_0$ will equal $1/\xi$, for all n. So $1/\xi$ is not in E. A concrete example of this would be, for instance, $K = \mathbb{Q}(e)$, $F = \mathbb{Q}$, and $E = \mathbb{Q}[e]$. □

Problem 5. Show that:
(a) Let $E = F(x)$ where x is transcendental over F. Let $K \neq F$ be a subfield of E which contains F. Show that x is algebraic over K.
(b) Let $E = F(x)$. Let $y = \frac{f(x)}{g(x)}$ be a rational function, with relatively prime polynomials $f, g \in F[x]$. Let $n = \max(|f|, |g|)$. Suppose $n \geq 1$. Prove that

$$[F(x) : F(y)] = n$$

Solution 5. We solve (b) first; (a) will follow immediately from (b).

Let $h(X) \in F(y)[X]$ be given by $h(X) = f(X) - \frac{f(x)}{g(x)}g(X)$. Observe that $F(y)$ is the fraction field of $F\left[\frac{f(x)}{g(x)}\right]$. Thus h is irreducible if and only if h is irreducible in $F\left[\frac{f(x)}{g(x)}\right][X]$, by Gauss' Lemma. But $F\left[\frac{f(x)}{g(x)}\right][X] \cong F[X]\left[\frac{f(x)}{g(x)}\right]$. So it will suffice to show that $h(X)$ is irreducible in $F[X]\left[\frac{f(x)}{g(x)}\right]$ as a polynomial in $\frac{f(x)}{g(x)}$. But this is obvious, since as such, h is of degree one and its only possible factor is a divisor of $f(X)$ and $g(X)$. But since f, g are relatively prime, there is no such divisor other than a constant (which we may take to be 1). So $h(X)$ is irreducible in $F(y)[X]$. Clearly $|h| = \max(|f|, |g|)$. Further, $h(x) = 0$. This shows that $[F(x) : F(y)] = \max(|f|, |g|)$.

(a) Now, since K is a subfield of E and contains F as a proper subfield, K must contain some rational function $\frac{f(x)}{g(x)}$, with f or g of positive degree. We may take f and g to be relatively prime after factoring out all common factors. But then, as seen in part (b), E is a finite extension over $F(\frac{f(x)}{g(x)}) \subset K$. Hence in particular E is a finite extension over K. Hence E is algebraic over K. □

Problem 6. Let k be a field of characteristic p and let t, u be algebraically independent over k. Prove the following:
(a) $k(t, u)$ has degree p^2 over $k(t^p, u^p)$.
(b) There exist infinitely many extensions between $k(t, u)$ and $k(t^p, u^p)$.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Solution 6. Well, $k(t,u)$ as an extension $k(t^p,u^p)$ can be obtained by first adjoining t, and then u. So,

$$[k(t,u):k(t^p,u^p)] = [k(t^p,u^p)(t)(u):k(t^p,u^p)]$$

Problem 7. Let k be a field, $f(x)$ an irreducible polynomial in $k[x]$, and let K be a finite normal extension of k. If g,h are monic irreducible factors of $f(x)$ in $K[x]$, show that there exists an automorphism σ of K over k such that $g = h^\sigma$. Give an example when this conclusion is not valid if K is not normal over k.

Solution 7.

Problem 8. Let $f(x_1,\ldots,x_n)$ be a homogeneous polynomial of degree 2 (resp. 3) over a field k. Show that if f has a non-trivial zero in an extension of odd degree (resp. degree 2) over k, then f has a non-trivial zero in k.

Solution 8.

Problem 9. What is the Galois group over the rationals of $x^5 - 4x + 2$?

Solution 9. Well, the derivative of $f(x)$ is $5x^4 - 4$, which has precisely two real roots, namely $\alpha = (4/5)^{1/4}$ and $\beta = -(4/5)^{1/4}$. Evaluating f at α, β, and at values $< \beta$ and $< \alpha$ and $> \alpha$, one sees that f changes sign three times. So by intermediate value theorem, f has precisely 3 real roots and 2 complex.

Now, if G is the galois group of f, we know that G is isomorphically imbedded in S_5. Further, the two complex roots (conjugates) correspond to transposition (an element of order 2). Since 5 is prime, by Sylow, G contains an element of order 5, which corresponds to a $5-cycle$ in S_5. But we know that S_p, p a prime, is generated by a transposition and a p-cycle. Hence G contains S_5, hence is all of S_5. □

Problem 10. Let K/k be a finite Galois extension with group G. Let $\alpha \in K$ be such that $\{\sigma\alpha\}_{\sigma\in G}$ is a normal basis. For each subset S of G let $S(\alpha) = \sum_{\sigma\in S}\sigma\alpha$. Let H be a subgroup of G and let F be the fixed field of H. Show that there exists a basis of F over k consisting of elements of the form $S(\alpha)$.

Solution 10. Let $G = \{\sigma_1,\ldots,\sigma_n\}$. Well, F is a subspace of K over k when viewed as a vector space. Now, we know that K is generated by the basis $\sigma\alpha$ for $\sigma \in G$. But F being a vector space in its own right, there exist linearly independent $\beta_1,\ldots,\beta_m$ in K which generate F. But each β_i is of the form

$$\sum_j c_{ij}\sigma_j\alpha$$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

So the elements of the form above form a basis over F. But then, in particular,

$$\sum_j \sigma_j \alpha$$

form a basis of F over k (since k is a field, we may cancel out $c_i j$ in the sum above and isolate each $\sigma_j \alpha$. Hence F has the required basis. □

Problem 11. (a) Let k be a field of characteristic $\nmid 2n$, for some odd integer $n \geq 1$, and let ζ be a primitive n-th root of unity, in k. Show that k also contains a primitive $2n$-th root of unity.

(b) Let k be a finite extension of the rationals. Show that there is only a finite number of roots of unity in k.

Solution 11. (a) Observe that if n is odd and ζ_n is a primitive n-th root of unity, then $\sqrt{\zeta_n}$ is a primitive $2n$-th root of unity. So it will suffice to show that $\sqrt{\zeta} \in K$. Let $\mathbb{F}$ be the prime subfield of K. Then $\mathbb{F}(\zeta)$ is a subfield of K of degree $\phi(n)$. Observe also that $\mathbb{F}(\sqrt{\zeta})$ is an extension of $\mathbb{F}$ of degree $\phi(2n)$, which contains the field $\mathbb{F}(\zeta)$. But since n has no factors of 2 (n is odd), $\phi(2n) = \phi(2)\phi(n) = \phi(n)$. This shows that $\mathbb{F}(\sqrt{\zeta}) = \mathbb{F}(\zeta)$. Hence $\sqrt{\zeta}$ is also in K, hence K contains a primitive $2n$-th root of unity. □

(b) Suppose to the contrary that K contains infinitely many roots of unity. Then for all $N \in \mathbb{N}$, there exists $n \geq N$ such that $\zeta_n \in K$. Hence $\mathbb{Q}(\zeta_n)$ is a subfield of K. Now, we know that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$. Without loss of generality, we may pick $N > 6$. But then $\phi(n) \geq \sqrt{n}$ (Kendall, D. G. and Osborn, R. "Two Simple Lower Bounds for Euler's Function." Texas J. Sci. 17, 1965). Hence K contains subfields of arbitrarily large degrees over $\mathbb{Q}$. But this cannot be since K is a finite extension. Hence K contains only a finite number of roots of unity. □

Problem 12. Let ζ be a primitive n-th root of unity. Let $K = \mathbb{Q}(\zeta)$.
(a) If $n = p^r$ $(r \geq 1)$ is a prime power, show that $N_{K/\mathbb{Q}}(1 - \zeta) = p$.
(b) If n is compositive then $N_{K/\mathbb{Q}}(1 - \zeta) = 1$.

Solution 12. (a) Well, we see that (p. 280, Lang):

$$\Phi_{p^r}(x) = \Phi_p(x^{p^{r-1}})$$

Now, by change of variables from x to $1 - x$, we observe, from above, that

$$\Phi_p((1-x)^{p^{r-1}})$$

is irreducible and monic. Further, the polynomial above is satisfied by $1 - \zeta$. Hence it must be the minimal polynomial of $1 - \zeta$. Now, observe that the constant term of $(1-x)^{p^{r-1}}$ is 1, and since Φ_p is of degree $p - 1$ with constant term also 1, we see that $\Phi_p((1-x)^{p^{r-1}})$ has constant term p. This is precisely the norm of $1 - \zeta$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

(b) On the other hand, we perform the same change of variables, using the fact that:

$$\Phi_n(x) = \Phi_{p_1 \cdots p_s}(x^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$$

and changing variables:

$$\Phi_{p_1 \cdots p_s}(x^{p_1^{r_1-1} \cdots p_s^{r_s-1}}) \rightsquigarrow \Phi_{p_1 \cdots p_s}((1-x)^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$$

and $\Phi_{p_1 \cdots p_s}$ contains equal amount of negative and positive monic terms (actually, all terms are monic). For this reason, the constant term of $\Phi_{p_1 \cdots p_s}$ is precisely 1. This is the norm of $1 - \zeta$. □

Problem 13. Let $\mathbb{F}_p$ be the prime field of characteristic p. Let K be the field obtained from F by adjoining all primitive l-th roots of unity, for all prime numbers $l \neq p$. Prove that K is algebraically closed.

Solution 13. We first show the existence of a prime l such that the period of p mod l is q^r, for a given prime q and an integer $r \geq 1$.

Well, let l be a prime dividing the number

$$b = \frac{p^{q^r} - 1}{p^{q^{r-1}} - 1} = (p^{q^{r-1}} - 1)^{q-1} + q(p^{q^{r-1}} - 1)^{q-2} + \cdots + q$$

If l does not divide $p^{q^{r-1}} - 1$, then l must divide $p^{q^r} - 1$. But then the period is at least q^r, and in fact divides q^r. But since l does not divide $p^{q^{r-1}} - 1$, the period is greater than q^{r-1}. Hence it must be precisely q^r, and we're done.

On the other hand, if l divides $p^{q^{r-1}} - 1$, then l also divides q, hence $l = q$ (by primality of l and q). But then q^2 does not divide b, so there is a prime $l \neq q$ such that l does divide b, and we're back to the first case.

But then the degree of $F(\zeta_l)$ over F is q^r. Since q and r were arbitrary, we see that K contains subfields of arbitrary prime-power degrees over F. From these extensions, subfields of arbitrary degrees over F, contained in K, can be built (every natural number is a product of powers of primes). So K is algebraically closed. □

Problem 14. Let$k$ be a field such that every finite extension is cyclic. Show that there exists an automorphism σ of k^a over k such that k is the fixed field of σ.

Solution 14. □

Problem 15. Let k be a field, k^a an algebraic closure, and σ an automorphism of k^a leaving k fixed. Let F be the fixed field of σ. Show that every finite extension of F is cyclic.

Solution 15. □

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Problem 16. Let E be an algebraic extension of k such that every non-constant polynomial $f(x)$ in $k[x]$ has at least one root in E. Prove that E is algebraically closed.

Solution 16. □

Problem 17. Let F be a finite field and K a finite extension of F. Show that the norm N_F^K and the trace Tr_F^K are surjective (as maps from K into F.

Solution 17. □

Problem 18. *Page 530, #17: Let $f(x)$ be an ireeducible polynomial of degree n over a field F. Let $g(x)$ be any polynomial in $F[x]$. Prove that every irreducible factor of the composite polynomial $f(g(x))$ has degree divisible by n.*

Solution 18. Let $p(x)$ be an irreducible factor of $f(g(x))$. Now let β be a root of $p(x)$. Then clearly $f(g(\beta)) = 0$ (i.e., β is also a root of $f(g(x))$). Now, in this case, $g(\beta)$ is a root of $f(x)$. Observe that $F(\beta) \supseteq F(g(\beta)) \subseteq F$ (the containment $F(\beta) \supseteq F(g(\beta))$ follows from the fact that $g(\beta)$ is simply a polynomial expression in β). Now, due to irreducibility of $p(x)$ and $f(x)$ we konw that $[F(\beta) : F] = p$ where p is the degree of $p(x)$ and $[F(g(\beta)) : F] = n$ where n is the degree of $f(x)$. By the containment above, we have:

$$[F(\beta) : F] = [F(\beta) : F(g(\beta))][F(g(\beta)) : F] \implies p = [F(\beta) : F(g(\beta))]n$$

Hence $n|p$. This completes the proof.

Problem 19. *Page 530, #18: Let k be a field and let $k(x)$ be the field of rational functions in x with coefficients from k. Let $t \in k(x)$ be the rational function $\frac{P(x)}{Q(x)}$ with relatively prime polynomials $P(x), Q(x) \in k[x]$, with $Q(x) \neq 0$. Then $k(x)$ is an extension of $k(t)$ and to compute its degree it is necessary to compute the minimal polynomial with coefficients in $k(t)$ satisfied by x.*

(a) Show that the polynomial $P(X) - tQ(X)$ in the variable X and coefficients in $k(t)$ is irreducible over $k(t)$ and has x as a root.

(b) Show that the degree of $P(X) - tQ(X)$ as a polynomial in X with coefficients in $k(t)$ is the maximum of the degrees of $P(x)$ and $Q(x)$.

(c) Show that $[k(x) : k(t)] = [k(x) : k\left(\frac{P(x)}{Q(x)}\right)] = \max\{\deg(P), \deg(Q)\}$.

Solution 19. (a) Per the hint in the book, we see that $(k(t))[X] = (k[X])[t]$. For convenience let us write $p(X) = P(X) - tQ(X)$. Then $p(x)$ is irreducible in $(k(t))[X]$ if, and only if, it is irreducible in $(k[X])[t]$. But we see that in $(k[X])[t]$ this

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

is a polynomial of degree 1. Hence it can be written only as $R(X)(P'(X)-tQ'(X))$ for some polynomials $R, P', Q' \in k[X]$. Since P and Q are relatively prime, we see that R must be a unit. But the units of $k[X]$ are precisely the units of k. Hence the polynomial $p(x)$ is irreducible in $(k[X])[t]$, thereby irreducible in $(k(t))[X]$.

Now, since $t = \frac{P(x)}{Q(x)}$ we see that $tQ(x) = P(x)$. Hence $p(x) = 0$. Hence x is a root of $p(X)$.

(b) Let us put $n = \deg(P)$ and $m = \deg(Q)$ for convenience. In the case $n \neq m$ it is obvious that the degree of $p(x)$ is $\max\{n, m\}$. The only case requiring consideration is $n = m$. So suppose $n = m$. ..... OK, I am having difficulty with this one. I am just not seeing it. I think I am getting too tangled up in the coefficients in different fields. There must be an easier way that I am just not seeing.

(c) This follows immediately from (a) and (b) since the polynomial $p(x)$ that we defined in (a) is irreducible and has as its root x, and the degree of $p(x) = \max\{\deg(P), \deg(Q)\}$.

Problem 20. *Page 531, #19: Let K be an extension of F of degree n.*

(a) For any $\alpha \in K$ prove that α acting by left multiplication on K is an $F-$linear transformation of K.

(b) Prove that K is isomorphic to a subfield of the ring of $n \times n$ matrices over F, so the ring of $n \times n$ matrices over F contains an isomorphic copy of every extension of F of degree $\leq n$.

Solution 20. (a) Consider any $a, b \in K$ and $f \in F$. Observe that, by distributivity of multiplication in the field K, and since F is a subfield of K we have,

$$\alpha(fa + b) = \alpha(fa) + \alpha(b) = f(\alpha(b)) + \alpha(b)$$

Hence the transformation defined by left multiplication by any element of K is an $F-$ linear transformation. Let us denote such a transformation, for any fixed α by T_α.

(b) Let $[T_\alpha]$ denote the matrix representing the linear transformation T_α considered in part (a). Consider now the map,

$$\phi : K \longrightarrow M_n(F)$$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

given by $\phi(\alpha) = [T_\alpha]$ for all $\alpha \in K$. Consider now $T_{\alpha+\beta}$. According to the definition of T_x it is trivial to verify that $T_{\alpha+\beta}$ is a linear transformation, and in fact $T_{\alpha+\beta} = T_\alpha + T_\beta$, the matrix representation of which is the sum of matrices representing T_α and T_β.

Now, ϕ also preserves multiplication. Indeed, it is trivial to verify (via laws of multiplication in a field) that $T_{\alpha\beta} = T_\alpha(T_\beta)$. The matrix of the composition of linear transformations is the product of their respective matrix representations.

This shows that ϕ is a ring homomorphism. Since ϕ is not the zero homomorphism (indeed the identity is not mapped to zero), we conclude (since K is a field) that ϕ is an isomorphism onto its image (which is a subset of $M_n(F)$). This completes the proof.

Problem 21. *Page 531, #20: Show that if the matrix of the linear transformation :multiplication by α" considered in the previous exercise is A then α is a root of the characteristic polynomial for A. This gives an effective procedure for determining an equation of degree n satisfied by an element α in an extension of F of degree n. Use this procedure to obtain the monic polynomial of degree 3 satisfied by $2^{\frac{1}{3}}$ and by $1 + 2^{\frac{1}{3}} + 4^{\frac{1}{3}}$*

Solution 21. Let A be the matrix of the linear transformation T_α. Now, let $p(\lambda)$ be the characteristic polynomial of T_α. By *Caley-Hamilton* theorem we know that $p(A) = 0$. We know also (since T_α is linear) that $[T_{p(\alpha)}] = p([T_\alpha]) = p(A) = 0$. Since the map ϕ considered above is injective and since under this map $0 \longmapsto 0$ we see that $p(\alpha) = 0$. Hence α is a root of p. This completes the proof.

Now consider $\mathbb{Q}[2^{\frac{1}{3}}]$. The basis of this field consist of $v_1 = 4^{\frac{1}{3}}, v_2 = 2^{\frac{1}{3}}, v_3 = 1$. Now, under the transformation of multiplication by v_2, we see that v_1 is transformed into 2, v_2 is transformed into v_1 and v_3 is transformed into v_2. It is easy to verify that the matrices for $T_{v_1}, \ldots, T_{v_3}$ are given by, respectively,

$$\begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{pmatrix}; \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}; \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

We verify this only for one, say v_2. The rest follows similarly. Let us write:

$$\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 4^{\frac{1}{3}} \\ 2^{\frac{1}{3}} \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 4^{\frac{1}{3}} \\ 2^{\frac{1}{3}} \end{pmatrix}$$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

And, as is evident, we have:

$$2^{\frac{1}{3}} \begin{pmatrix} 4^{\frac{1}{3}} \\ 2^{\frac{1}{3}} \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 4^{\frac{1}{3}} \\ 2^{\frac{1}{3}} \end{pmatrix}$$

From this we have $[T_{v_1+v_2+v_3}] = [T_{v_1}] + [T_{v_2}] + [T_{v_3}]$. So we have

$$[T_{v_1+v_2+v_3}] = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

Computing the characteristic polynomial for this matrix we get: $p(\lambda) = \lambda^3 - 3\lambda^2 - 3\lambda + 1$. This polynomial will be satisfied by $1 + 2^{\frac{1}{3}} + 4^{\frac{1}{3}}$.

Problem 22. *Page 551, #4: Let $a > 1$ be an integer. Prove for any positive integers n, d that d divides n if and only if $a^d - 1$ divides $a^n - 1$. Conclude in particular that $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^n}$ if and only if d divides n.*

Solution 22. In solving this problem we'll be employing the more general result stated in problem 3 on the same page. That is:

Proposition 1. *Given d and n positive integers, $x^d - 1$ divides $x^n - 1$ if, and only if, d divides n (assuming $x \neq 1$).*

Assuming that we're considering these polynomials over some integral domain, we provide the following proof.

Proof. Before we prove this result, we claim first that if m is some (positive) integer and $x^m - 1$ is a polynomial over an integral domain, then

$$x^m - 1 = (x - 1) \sum_{j=0}^{m-1} x^j \tag{0.1}$$

The proof of this is a quite straight forward derivation, so we skip it here.

Suppose that d divides n. Then there is a (positive) integer k such that $n = dk$. Hence we can write $x^n - 1 = (x^d)^k - 1$. Per 0.3 we have

$$(x^d)^k - 1 = (x^d - 1) \sum_{j=0}^{k-1} (x^d)^j \tag{0.2}$$

Since $x^d - 1$ divides the right side of 0.2, it clearly divides the left side of 0.2. Hence $x^d - 1$ divides $x^n - 1$.

Let us now suppose that $x^d - 1$ divides $x^n - 1$. From this assumption it is clear that $d \leq n$. Let us write $n = dq + r$ for some (positive) integers q and $r \geq 0$.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Then we have $x^n - 1 = (x^{dq+r} - x^r) + (x^r - 1)$. Rewritten another way we have: $x^n - 1 = ((x^d)^q - 1)x^r + (x^r - 1)$. Now consider, by 0.3:

$$(x^d)^q - 1 = (x^d - 1)\sum_{j=0}^{q-1}(x^d)^j$$

Hence it is clear that $x^d - 1$ divides $((x^d)^q - 1)x^r$, thus $x^d - 1$ must divide $x^r - 1$. By the Euclidean algorithm, $0 \leq r < d$. Hence the degree of $x^r - 1$ is strictly less than that of $x^d - 1$. Thus $x^r - 1 = 0$ (i.e., $x^r = 1$). So $x^n = x^{dq}$. If we're working in characteristic zero, then $n = dq$ so d divides n. If we're working in characteristic p then $[d]$ divides $[n]$ in $\mathbb{Z}/p\mathbb{Z}$ (i.e., $[d][q] = [n]$ in $\mathbb{Z}/p\mathbb{Z}$). □

Now, on with the solution to the given problem. Given that $a \in \mathbb{Z}$, it is clear that a is a member of an integral domain. Since the polynomials in Proposition 1 are considered over integral domains, and nothing was assumed about x other than $x \neq 1$, the solution follows immediately from the proposition above. In fact, the identical proof would work with a everywhere in place of x; but we need the more general result of Proposition 1 to solve the second part of the problem.

Suppose now that $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ (clearly then $d \leq n$). Consider the polynomials $f(x) = x^{p^d-1} - 1$ and $g(x) = x^{p^n} - 1$ over $\mathbb{F}_{p^n}$. Now, by Corollary 36 on p. 549 we know that $\alpha^{p^d-1} = 1$ for all $\alpha \neq 0$ in $\mathbb{F}_{p^d}$. Hence $f(x)$ splits over $\mathbb{F}_{p^d}$ and hence over $\mathbb{F}_{p^n}$. Similarly $g(x)$ splits over $\mathbb{F}_{p^n}$. The roots of $f(x)$ are then precisely $\mathbb{F}_{p^d}^{\times}$ and the roots of $g(x)$ are precisely $\mathbb{F}_{p^n}^{\times}$. Since $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ it is clear that in $\mathbb{F}_{p^n}[x]$ $f(x)$ divides $g(x)$. In which case, by Proposition 1, $p^d - 1$ divides $p^n - 1$. Hence by the first part of the problem $d|n$.

Suppose on the other hand that $d|n$. In this case, by the first part, $p^d - 1$ divides $p^n - 1$. Consider the field $\mathbb{F}_{p^n}$ and its prime subfield $\mathbb{F}_p$. Let $f(x) = x^{p^d} - x$ and $g(x) = x^{p^n} - x$ be polynomials over $\mathbb{F}_p$. We can rewrite $f(x) = x(x^{p^d-1} - 1)$ and $g(x) = x(x^{p^n-1} - 1)$. Since $p^d - 1$ divides $p^n - 1$, by Proposition 1 $f(x)$ divides $g(x)$. By the exposition presented on pages 549-550, we know that the splitting field of $f(x)$ is $\mathbb{F}_{p^d}$ and the splitting field of $g(x)$ is $\mathbb{F}_{p^n}$. Since $f(x)$ divides $g(x)$ and since splitting fields are unique up to isomorphism, we conclude that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$.

Problem 23. *Page 551, #6: Prove that* $x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^{\times}}(x - \alpha)$. *Conclude that* $\prod_{\alpha \in \mathbb{F}_{p^n}^{\times}} \alpha = (-1)^{p^n}$. *So the product of the nonzero elements of a finite field is +1 if* $p = 2$ *and* -1 *if* p *is odd. For* p *odd and* $n = 1$ *derive Wilson's Theorem:* $(p-1)! \equiv -1(mod p)$.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Solution 23. Consider the polynomial $f(x) = x^{p^n} - x$ over the field $\mathbb{F}_p$. Now, the splitting field of this polynomial is precisely the field $\mathbb{F}_{p^n}$. In fact, all the elements of this field are roots of $f(x)$. Now let's write: $f(x) = x(x^{p^n-1} - 1)$. Since 0 is also a root of $f(x)$, when we exclude 0 we see that $\mathbb{F}_{p^n}^\times$ is precisely the set of roots of $x^{p^n-1} - 1$. Hence we can write:

$$x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha)$$

Now, setting $x = 0$ we have:

$$-1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (-\alpha) = (-1)^{p^n-1} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha$$

by commutativity in $\mathbb{F}_{p^n}$. Multiplying both sides by $(-1)^{p^n-1}$ we obtain:

$$(-1)^{p^n} = ((-1)^2)^{p^n-1} \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha$$

Since $(-1)^2 = 1$ we obtain:

$$(-1)^{p^n} = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} \alpha$$

Now, to summarize for $n = 1$ and p odd, we must have in $\mathbb{F}_p$:

$$\alpha_1 \alpha_2 \cdots \alpha_{p-1} = -1$$

where the elements α_j with $1 \leq j \leq p-1$ are the nonzero elements of $\mathbb{F}_p$. Taking $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ we have: $[1][2]\cdots[p-1] = [-1]$. Hence $(1)(2)\cdots(p-1) \equiv -1(\mod p)$. Hence $(p-1)! \equiv -1(\mod p)$.

Problem 24. *Page 555, #4: Prove that if $n = p^k m$ where p is a prime and m is relatively prime to p then there are precisely m distinct n^{th} roots of unity over a field of characteristic p.*

Solution 24. It is not stated in the problem, but we shall assume that we're working in characteristic p. In which case we have $x^{p^k m} - 1$ can be written as $(x^m - 1)^{p^k}$. hence the roots of this polynomial are precisely the roots of $x^m - 1$. The derivative of this polynomial if mx^{m-1}. Since p and m are relatively prime, $mx^{m-1} \neq 0$. In which case mx^{m-1} and $x^m - 1$ are relatively prime. Hence $x^m - 1$ is separable. Hence $x^m - 1$ has precisely m distinct roots of unity. Thus $x^{p^k m} - 1$ has exactly m distinct n^{th} roots of unity.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Problem 25. *Page 555, #5: Prove there are only a finite number of roots of unity in any finite extension K of $\mathbb{Q}$.*

Solution 25. We'll take for granted the fact that $\phi(n) \geq \sqrt{n}$ for all $n > 6$. We shall proceed by proving the contrapositive.

Suppose that K, an extension over $\mathbb{Q}$, contains infinitely many roots of unity. Fix any $N \in \mathbb{N}$. Then there exists $n > 6$ such that $n > N^2$ and $\zeta_n \in K$. Now, we know that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) \geq \sqrt{n} > N$. Since $\mathbb{Q}(\zeta_n) \subseteq K$ we must have $[K : \mathbb{Q}] > N$. In particular this can be done for all N in $\mathbb{N}$. Hence K is not an extension of $\mathbb{Q}$ of a finite degree. This completes the proof.

Problem 26. *Page 567, #6: Let k be a field.*

(a) Show that the mapping $\phi : k[t] \longrightarrow k[t]$ defined by $\phi(f(t)) = f(at + b)$ for fixed a, b in k with $a \neq 0$ is an automorphism of $k[t]$ which is the identity on k.

(b) Conversely, let ϕ be an automorphism of $k[t]$ which is the identity on k. Prove that there exist elements a, b of k with $a \neq 0$ such that $\phi(f(t)) = f(at + b)$ as in (a).

Solution 26. By the ring automorphism we mean an isomorphism from the ring in question onto itself. With this in mind, we have for part (a):

Let $f(x), g(x) \in k[x]$. The fact that ϕ is a homomorphism is easily verified:

$$\phi(f(x)g(x)) = f(at + b)g(at + b) = \phi(f(x))\phi(g(x))$$

Similarly for the sum.

GENERAL QUESTION: In situations like this I tend to conclude with "it's obvious." Is that too bold of me? Should I be more pedantic? I always find it difficult to draw the line between what needs to be said, and what can be taken for granted.

Now, ϕ fixes k since each element of k can be regarded as a polynomial of degree zero (i.e., $f(x) = c \in k \implies f(u) = c$ for all $u \in k$ since c is independent of x).

Suppose that $h(x) \in \ker(\phi)$. It is clear that $h(x)$ cannot be a nonzero constant polynomial, since ϕ fixes k (by the above). Hence $h(x)$ is either identically zero or is of degree one or higher. Since $a \neq 0$, $ax + b$ is of degree one. Suppose that $h(x)$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

is of degree, say, $n \geq 1$. Write,

$$h(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0$$

Then we have for $\phi(h(x)) = h(ax+b)$:

$$\alpha_n (ax+b)^n + \alpha_{n-1}(ax+b)^{n-1} + \cdots + \alpha_0$$

Since neither a nor α_n is zero, the polynomial above is of degree n, hence cannot be equal to zero. Thus $h(x) \notin \ker(\phi)$. Hence $\ker(\phi) = \{0\}$. This proves that ϕ is injective.

Pick any $f(x) \in k[x]$. To show that ϕ is surjective, we'll construct $g(x) \in k[x]$ such that $\phi(g(x)) = f(x)$. First of all, since k is fixed by ϕ, we only consider $f(x)$ of degree at least one. Say $\deg(f(x)) = n$. Let us write

$$f(x) = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$$

We claim that there exist $\beta_n, \beta_{n-1}, \ldots, \beta_0$ such that

$$g(x) = \beta_n x^n + \beta_{n-1} x^{n-1} + \cdots + \beta_0$$

such that

$$g(ax+b) = \beta_n (ax+b)^n + \beta_{n-1}(ax+b)^{n-1} + \cdots + \beta_0 = f(x)$$

The construction of such a g reduces then to finding the suitable β_j. In fact, such can be found by expanding each $(ax+b)^j$ above using the binomial theorem (this can always be done over commutative rings) and solving for β_j recursively: first solve for β_n. This can be done easily in terms of a and α_n. Namely: $\beta_n = \alpha_n a^{-1}$ (this is easily verified). Then solve for β_{n-1} in terms of β_n, a and α_{n-1}. The reason this can easily be done is because k is a field (hence contains multiplicative inverses). Continue this process recursevely to solve for β_j in terms of $\beta_n, \beta_{n-1}, \ldots, \beta_{j-1}$, a and α_j. (Back to my general question: it feels that I'm giving here a hand waving argument).

This shows that

$$\begin{aligned} \phi : k[t] &\longrightarrow k[t] \\ t &\mapsto at + b \end{aligned}$$

with $a \neq 0$ is an automorphism.

Conversely, suppose that $\tau : k[t] \longrightarrow k[t]$ is some automorphism that fixes k. Consider any polynomial, say $f(x)$, in $k[x]$. Let us write:

$$f(x) = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_0$$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Then, since τ is in particular a homomorphism, we have

$$\tau(f(x)) = \tau(f_n)\tau(x)^n + \tau(f_{n-1})\tau(x)^{n-1} + \cdots + \tau(f_0)$$

Since τ fixes k, from the above we obtain:

$$\tau(f(x)) = f_n\tau(x)^n + f_{n-1}\tau(x)^{n-1} + \cdots + \tau(f_0)$$

Hence τ is completely determined by its action on x. τ cannot map x to a polynomial of degree less than one (i.e., a constant in k) since in that case the range of τ would not include, say, x; but we know that τ is an automorphism, hence surjective. Suppose that τ maps x to a polynomial of degree $n > 1$, say:

$$g(x) = g_n x^n + g_{n-1}x^{n-1} + \cdots + g_0$$

Pick any polynomial in k, say

$$h(x) = h_m x^m + h_{m-1}x^{m-1} + \cdots + h_0$$

Consider now $\tau(h(x))$:

$$h_m(g(x))^m + h_{m-1}(g(x))^{m-1} + \cdots + h_0$$

Now, if h is of degree zero, then so is its image under τ. If h is of degree greater than zero, then its image under τ is of degree $nm > 1$ since $n > 1$. In either case, then, there does not exist $h(x) \in k[x]$ whose image under τ is x. Hence τ is not surjective. This cannot be! So the degree of $g(x)$ (the image of x under τ) must be greater than 0 but not greater than 1. Hence the degree of $g(x)$ is precisely one! Hence $\tau(x) = ax + b$ for some nonzero a.

This completes our solution.

Problem 27. *Page 567, #7: (a) Prove that if σ is any automorphism of $\mathbb{R}/\mathbb{Q}$ then σ takes squares to squares and positive reals to positive reals. Conclude that $a < b$ implies $\sigma(a) < \sigma(b)$ for every a, b in $\mathbb{R}$.*

(b) Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies that $-\frac{1}{m} < \sigma(a) - \sigma(b) < \frac{1}{m}$ for every positive integer m. Conclude that σ is a continuous map on $\mathbb{R}$.

(c) Prove that any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map, hence $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.

Solution 27. From this point on all lower case latin letters will denote real numbers unless stated otherwise.

(a) Suppose that $a = b^2$. Consider $\sigma(a) = \sigma(b^2) = \sigma(b)\sigma(b) = \sigma(b)^2$ since σ is

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

a homomorphism. Now, suppose $a > 0$. Write $b = \sqrt{a}$. This can always be done in the real numbers. Then we have $\sigma(a) = \sigma(b)^2$. Squares are positive. So $\sigma(a) > 0$ for all a.

Suppose $a < b$. Then $b - a > 0$. Hence by the above $\sigma(b - a) > 0$. Since σ is a homomorphism, we have $\sigma(b) - \sigma(a) = \sigma(b - a) > 0$. Hence $\sigma(b) > \sigma(a)$.

(b) Suppose that m is a positive integer. Suppose $a - b > -\frac{1}{m}$. Then we have $(a - b) + \frac{1}{m} > 0$. By part (a) we have $\sigma(a - b) > \sigma(-\frac{1}{m})$. Since σ fixes $\mathbb{Q}$, we have $\sigma(a - b) > -\frac{1}{m}$. So $\sigma(a) - \sigma(b) > -\frac{1}{m}$. Exact same argument establishes the other inequality.

Fix any point a in $\mathbb{R}$. Pick any $\epsilon > 0$. Then there exists $n \in \mathbb{N}$ such that $\epsilon > \frac{1}{n}$. Set $\delta = \frac{1}{n}$. Consider (by the first part of (b) above):

$$-\frac{1}{n} < x - a < \frac{1}{n} \implies -\frac{1}{n} < \sigma(x) - \sigma(a) < \frac{1}{n}$$

for all x. Equivalently,

$$|x - a| < \delta \implies |\sigma(x) - \sigma(a)| < \delta < \epsilon$$

This establishes continuity of σ at a. Since a was chosen arbitrarily, we conclude that σ is continuous on $\mathbb{R}$.

Suppose that f is a continuous map on $\mathbb{R}$ which is the identity map on $\mathbb{Q}$. Pick $r \in \mathbb{R} - \mathbb{Q}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists a sequence $\{q_n\} \subset \mathbb{Q}$ such that $q_n \longrightarrow r$ as $n \longrightarrow \infty$. Now consider, since f is continuous:

$$\lim_{n\to\infty} f(q_n) = f\left(\lim_{n\to\infty} q_n\right) = f(r)$$

And, since f is the identity on $\mathbb{Q}$:

$$\lim_{n\to\infty} f(q_n) = \lim_{n\to\infty} q_n = r$$

Since limits are unique in any Housdorff space, we conclude that $f(r) = r$. Since r was arbitrary we conclude that f is the identity on $\mathbb{R}$.

Since σ was established to be continuous on $\mathbb{R}$ in part (b) and since σ fixes $\mathbb{Q}$, by part (c) we conclude that σ is the identity on $\mathbb{R}$. Hence $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.

Problem 28. *Page 567, #8: Prove that the automorphisms of the rational function field $k(t)$ which fix k are precisely the fractional linear transformations* determined by $t \mapsto \frac{at+b}{ct+d}$ for a, b, c, d in k such that $ad - bc \neq 0$.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Solution 28. Consider any $\frac{p(x)}{q(x)}$ in $k(x)$. We can write for $\frac{1}{q(x)} = q(x)^{-1}$. So $\frac{p(x)}{q(x)} = p(x)q(x)^{-1}$. Suppose now that $\tau : k(x) \longrightarrow k(x)$ is an automorphism. Write $p(x)$ as

$$p_n x^n + p_{n-1}x^{n-1} + \cdots + p_0$$

Similarly for $q(x)$:

$$q_m x^m + q_{m-1}x^{m-1} + \cdots + q_0$$

Now we have for $\tau(\frac{p(x)}{q(x)}) = \tau(p(x)q(x)^{-1})$ since τ is a homomorphism:

$$\tau(p(x)q(x)^{-1}) = (\tau(p_n)\tau(x)^n + \cdots + \tau(p_0))(\tau(q_m)\tau(x)^m + \cdots + \tau(q_0))^{-1}$$

Since τ fixes k, from the above we obtain:

$$\tau(p(x)q(x)^{-1}) = (p_n\tau(x)^n + p_{n-1}\tau(x)^{n-1} + \cdots + p_0)(q_m\tau(x)^m + q_{m-1}\tau(x)^{m-1} + \cdots + q_0)^{-1}$$

Hence τ is completely determined by its action on x.

Now, we observe immediately that under τ the field $k(x)$ is isomorphic to the field $k\left(\frac{p(x)}{q(x)}\right)$. By exercise 18(c) in section 13.2 we know that

$$\left[k(x) : k\left(\frac{p(x)}{q(x)}\right)\right] = \max\{\deg(p(x)), \deg(q(x))\}$$

Since $k(x)$ and $k\left(\frac{p(x)}{q(x)}\right)$ are isomorphic, we know that the degree of the extension above must be precisely one. Hence we know $p(x) = ax + b$ and $q(x) = cx + d$ with either a or c not zero, and either b or d not zero; for if both b and d were zero, then $\frac{p(x)}{q(x)} = \frac{a}{c}$ (i.e., t maps to a constant, which cannot be true since then the range of τ would be a subset of k, but τ is surjective). Hence the restriction $ad - bc \neq 0$.

Problem 29. *Page 567, #10: Let K be an extension of the field F. Let $\phi : K \to K'$ be an isomorphism of K with field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \phi\circ\sigma\circ\phi^{-1}$ defines a group isomorphism* $\mathrm{Aut}(K/F) \simeq \mathrm{Aut}(K'/F')$.

Solution 29. Let us for convinience write $\tau(\sigma) = \phi \circ \sigma \circ \phi^{-1}$. Please note that σ in this case is an *arbitrary* automorphism of K/F but fixed throughout the proof. Hence anything we show for $\tau(\sigma)$ will generally hold true for $\tau(\alpha)$ for any automorphism α on K/F. The diagram below shows that $\tau(\sigma)$ is a map from K' to K' (we don't verify this formally for it's quite obvious).
Before we attempt to show that τ so defined is a group isomorphism, let us first show that $\tau(\sigma)$ is an automorphism of K'/F' (that fixes F').

We first verify that $\tau(\sigma)$ is a homomorphism from K'/F' to K'/F' that fixes F' (i.e., that $\tau(\sigma)$ preserves the field operations). We verify this only for addition in K'/F' since the exact same argument will produce the desired result for multiplication.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Consider a, b in K'/F'. We have:

$$(\phi \circ \sigma \circ \phi^{-1})(a+b) = \phi(\sigma(\phi^{-1}(a+b)))$$

Since ϕ is an isomorphism from K/F to K'/F', we know that ϕ^{-1} is an isomorphism from K'/F' to K/F. So we have from the above:

$$(\phi \circ \sigma \circ \phi^{-1})(a+b) = \phi(\sigma(\phi^{-1}(a) + \phi^{-1}(b)))$$

Since σ is an automorphism (in particular a homomorphism) on K/F we have from the above:

$$(\phi \circ \sigma \circ \phi^{-1})(a+b) = \phi(\sigma(\phi^{-1}(a)) + \sigma(\phi^{-1}(b)))$$

Finally, since ϕ is an isomorphism,

$$(\phi \circ \sigma \circ \phi^{-1})(a+b) = \phi(\sigma(\phi^{-1}(a))) + \phi(\sigma(\phi^{-1}))$$

Hence we have

$$(\phi \circ \sigma \circ \phi^{-1})(a+b) = (\phi \circ \sigma \circ \phi^{-1})(a) + (\phi \circ \sigma \circ \phi^{-1})(b)$$

So $\tau(\sigma)$ preserves addition. Similarly it preserves multiplication.

Now, let f' be an element of F'. Since ϕ maps F onto F' and is injective, we know that ϕ^{-1} maps F' onto F. So $f = \phi^{-1}(f')$ is an element of F. Since σ fixes F we know that $\sigma(f) = f$. Finally, since ϕ is an isomorphism, $\phi(f) = f'$. Hence $\tau(\sigma)$ fixes F'. All that is remaining to show is that $\tau(\sigma)$ is bijective.

Since ϕ^{-1}, σ and ϕ are injective functions whose composition is well-defined (i.e., the domain of one is the range of the other), we conclude that their composition is also an injective function (this I know from basic set theory).

Pick any a in K'/F'. Consider $b = (\phi \circ \sigma^{-1} \circ \phi^{-1})(a)$. A routine calculation will verify that b is an element of K'/F' and $\tau(\sigma)(b) = a$. So $\tau(\sigma)$ is surjective.

Finally we conclude that $\tau(\sigma)$ is an automorphism on K'/F'. We're ready to attack τ and show that it in turn is an isomorphism from Aut(K/F) to Aut(K'/F').

For amy two automorphisms α, β of K/F, consider:

$$(\phi \circ \alpha \circ \phi^{-1}) \circ (\phi \circ \beta \circ \phi^{-1}) = \phi \circ (\alpha \circ \beta) \circ \phi^{-1} = \tau(\alpha \circ \beta)$$

The second equality above follows from associativity of $\circ$. Hence τ preserves composition.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Suppose now that there is an automorphism of K/F, call it α, different from the identity on K/F. Pick an element in K'/F', say f, such that $\alpha(\phi^{-1}(f)) \neq \phi^{-1}(f)$. This can be done since α is not the identity and ϕ^{-1} is surjective. Consider:

$$\tau(\alpha)(f) = \phi(\alpha(\phi^{-1}(f)))$$

Now, say $g = \phi^{-1}(f)$ in K/F. Then we have $\alpha(g) \neq g$. So we have $\phi(\alpha(g)) \neq f$. So $\tau(\alpha)$ is not the identity on K'/F'. Hence the kernel of τ consists exclusively of the identity on K/F. Hence τ is injective.

Pick any automorphism, say β, of K'/F'. Consider $\alpha = \phi^{-1}\beta\phi$. Then we have $\tau(\alpha) = \beta$ (we don't verify that α so defined is in fact an automorphism of K/F since the exact same proof that we did to verify that $\tau(\sigma)$ is an automorphism on K'/F' will verify this; neither do we verify that $\tau(\alpha) = \beta$. This is a trivial calculation). So τ is surjective.

Grand finale: τ is an isomorphism from $\mathrm{Aut}(K/F)$ to $\mathrm{Aut}(K'/F')$. This completes our solution. Phew!

Problem 30. *Page 582, #4: Let p be a prime. Determine the elementsof the Galois group of $x^p - 2$.*

Solution 30. Let $r = \sqrt[p]{2}$ and ζ_p be the primitive p-th root of unity. Let us label for convenience $p(x) = x^p - 2$. Now, it is clear that both, r and ζ_p satisfy $p(x) = 0$. We also know that $E = \mathbb{Q}(r, \zeta_p)$ is the splitting field of $p(x)$ over $\mathbb{Q}$ (we don't prove this). Our first claim is the following. $[E : \mathbb{Q}] = p(p-1)$.

To prove this claim, we show that the degree of E over $\mathbb{Q}$ is at most $p(p-1)$. Then we show that both, p and $p-1$ divide the degree of E over $\mathbb{Q}$.

Consider: $E = \mathbb{Q}(\zeta_p)(r)$. Hence $[E : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}(r)][\mathbb{Q}(r) : \mathbb{Q}]$. We know that $[\mathbb{Q}(r) : \mathbb{Q}] = p$. Now, consider $p(x)$ over $\mathbb{Q}(r)$. Then we can write:

$$p(x) = (x - r)\sum_{k=0}^{p-1} x^{p-1-k}r^k \tag{0.3}$$

Set

$$f(x) = \sum_{k=0}^{p-1} x^{p-1-k}r^k \tag{0.4}$$

This is a polynomial of degree $p-1$ which is satisfied by ζ_p. Hence the minimal polynomial $m_{\mathbb{Q}(r),\zeta_p}$ is of degree at most $p-1$. Hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(r)]$ is at most $p-1$. Hence $[E : \mathbb{Q}]$ is at most $p(p-1)$.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Now, it is true that $E = \mathbb{Q}(\zeta_p)(r)$ and $E = \mathbb{Q}(r)(\zeta_p)$ (i.e., the order in which we adjoin roots of $p(x)$ to $\mathbb{Q}$ in constructing the splitting field of $p(x)$ does not matter). Hence

$$[E : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}(r)][\mathbb{Q}(r) : \mathbb{Q}]$$

And

$$[E : \mathbb{Q}] = [\mathbb{Q}(r) : \mathbb{Q}(\zeta_p)][\mathbb{Q}(\zeta_p) : \mathbb{Q}]$$

Hence we have

$$[E : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}(r)]p$$

And

$$[E : \mathbb{Q}] = [\mathbb{Q}(r) : \mathbb{Q}(\zeta_p)]\phi(p) = [\mathbb{Q}(r) : \mathbb{Q}(\zeta_p)](p-1)$$

Hence the degree of E is divisible by p and by $p-1$. Therefore, since the degree of E is at most $p(p-1)$, we conclude that the degree of E is precisely $p(p-1)$. Hence the Galois group of E will contain precisely this many elements. We shall use this shortly.

Now we claim that the polynomial $p(x)$ remains irreducible in $\mathbb{Q}(\zeta_p)$. To see this, consider: the degree of the extension $K = \mathbb{Q}(\zeta_p)(r)/\mathbb{Q}(\zeta_p)$ is precisely p. To see this, simply remember that the degree of E is $p(p-1)$. By construction of K we have $[E : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_p)](p-1)$. Now, we know that the degree of K is the degree of the minimal polynomial over $\mathbb{Q}(\zeta_p)$ satisfied by r. Since $x^p - 2$ is a polynomial satisfied by r whose degree is p and which itself is monic, we conclude that it is precisely the minimal polynomial, hence irreducible.

Now, we claim that $f(x)$ from 0.4 remains irreducible over $\mathbb{Q}(r)$. The argument is similar to the one given above. The degree of the extension $K = \mathbb{Q}(r)(\zeta_p)/\mathbb{Q}(r)$ is precisely $p-1$ (by reasoning given above). In $\mathbb{Q}(r)$ $p(x)$ factors as in 0.3. So we can write $p(x) = (x - \sqrt[n]{2})f(x)$. Now, the minimal polynomial has degree $p-1$. Since $f(x)$ is monic of degree $p-1$ satisfied by ζ_p, $f(x)$ is the minimal polynomial, hence is irreducible.

Both, $f(x)$ and $p(x)$ split completely over $mathbbQ(r, \zeta_p)$ since as we stated in the beginning, $\mathbb{Q}(r, \zeta_p)$ is the splitting field of $p(x)$ over $\mathbb{Q}$.

Now, let us consider the automorphisms of $\mathbb{Q}(r, \zeta_p)$, σ and τ_k given by:

$$\sigma : \begin{cases} r & \mapsto & \zeta_p r \\ \zeta_p & \mapsto & \zeta_p \end{cases} ; \tau_k : \begin{cases} r & \mapsto & r \\ \zeta_p & \mapsto & {\zeta_p}^k \end{cases}$$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

For $1 < k \leq p-1$. Then σ^n (for $1 \leq n \leq p$) are identities on $\mathbb{Q}(\zeta_p)$ and τ_k (with k restricted as above) and σ^p are identities on $\mathbb{Q}(r)$. Our next claim is that these automorphisms generate the Galois group of $\mathbb{Q}(r, \zeta_p)$.

Since σ is an automorphism, σ^n is for all n (the restriction on n above is only for convenience). τ_k (with te restriction on k as above) is also an automorphism for all k (we don't show this; a routine calculation will establish this). Which means that compositions of these automorphisms also form automorphisms. That is, all the maps of the form $\tau_k\sigma^n$ are automorphisms. Now, for $i \neq j$, $\tau_i \neq \tau_j$ (this is clear from definition of τ_k). Similarly when $n \neq m$ we have $\sigma^n \neq \sigma^m$. Now consider the map

$$\tau_k\sigma^n : \begin{cases} r & \mapsto & ({\zeta_p}^{nk})r \\ \zeta_p & \mapsto & {\zeta_p}^k \end{cases}$$

(nk above is taken modulo p for convenience). Clearly from the above, when $i \neq j$ we have $\tau_i\sigma^n \neq \tau_j\sigma^m$ for any n, m. Suppose now that $i = j$ and $n \neq m$ (and $1 \leq n, m \leq p$). Then since $in \neq jm$ taken modulo p because $n \neq m$, we have ${\zeta_p}^{in} \neq {\zeta_p}^{jm}$. Hence $\tau_i\sigma^n \neq \tau_j\sigma^m$. Hence τ_k, σ^n, and $\tau_k\sigma^n$ are all distinct (for $1 < k \leq p-1$ and $1 \leq n \leq p$). There are precisely $p(p-1)$ of them, all of which are automorphisms (σ^n account for p of them, τ_k account for $p-2$ of them, and $\tau_k\sigma^n$ account for $p(p-2)$ of them for the total of $p(p-1)$). So these are the elements of the Galois group of $\mathbb{Q}(r, \zeta_p)$.

Problem 31. *Page 582, #5: Prove that the Galois group of $x^p - 2$ for p a prime is isomorphic to the group of matrices*

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

where a, b are in $\mathbb{F}_p$, $a \neq 0$.

Solution 31. Consider the automorphisms in the solution to the previous problem. Each such automorhpism, say α acts as follows

$$\alpha : \begin{cases} r & \mapsto & ({\zeta_p}^b)r \\ \zeta_p & \mapsto & {\zeta_p}^a \end{cases}$$

for a and b taken modulo p and $a \neq 0$. Let us consider the map T from $\mathrm{Aut}(\mathbb{Q}(r, \zeta_p))$ to S, the set of matrices given in the problem description, given by

$$T : \alpha \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Let β be another automorphism, say,

$$\alpha : \begin{cases} r & \mapsto & (\zeta_p{}^d)r \\ \zeta_p & \mapsto & \zeta_p{}^c \end{cases}$$

Then composing α and β we get:

$$\alpha\beta : \begin{cases} r & \mapsto & (\zeta_p{}^{ad+b})r \\ \zeta_p & \mapsto & \zeta_p{}^{ac} \end{cases}$$

as a routine calculation will verify. On the other hand,

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

Hence T is a homomorphism. The kernel of this homomorphism is $\{\sigma^p\}$ (recall, by definition of σ we have σ^p is in fact the identity on $\mathbb{Q}(r, \zeta_p)$). To see this, consider all the elements that map to the identity matrix. These elements (by definition of T) are precisely the automorphisms that act as follows

$$\begin{cases} r & \mapsto & \zeta_p{}^0 r \\ \zeta_p & \mapsto & \zeta_p{}^1 \end{cases}$$

We could have p as the exponent in place of 0 above, as the exponents are taken modulo p. But since all automorphisms are determined by their action on r and on ζ_p, from the above we conclude that there is only one such automorphism: the identity!

Now, the matrices introduced in the problem statement can be formed in p^2 ways: for each b (there are precisely p such distinct in $\mathbb{F}_p$) we select an a (also in p possible ways). But since a is not allowed to take on the value of zero, we can select a in only $p-1$ possible ways. Hence S contains precisely $p(p-1)$ elements. Now, since T is injective and since the domain of T contains $p(p-1)$ elements and so does S, we conclude that T is surjective. Hence T is an isomorphism.

Problem 32. *Page 582, #8: Suppose K is a Galois extension of F of degree p^n for some prime p and some $n \geq 1$. Show there are Galois extensions of F contained in K of degrees p and p^{n-1}.*

Solution 32. Theorem (1) on page 188 of Dummit and Foote states that if G is a group of order p^n then G has normal subgroups of all orders $a \in \{0, \ldots, n\}$. Applying this to the problem at hand, we immediately conclude that the Galois group under consideration must have normal subgroups of orders p and p^{n-1}. But by the *F.T.G.T.* we conclude that there must exist Galois extensions of F (subfields of K) of degrees p and p^{n-1}.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Problem 33. *Page 582, #11: Suppose that $f(x)$ in $\mathbb{Z}[x]$ is an irreducible quartic whose splitting field has Galois group S_4 over $\mathbb{Q}$. Let θ be a root of $f(x)$ and set $K = \mathbb{Q}$. Prove that K is an extension of $\mathbb{Q}$ of degree 4 which has no proper subfields. Are there any Galois extensions of $\mathbb{Q}$ of degree 4 with no proper subfields?*

Solution 33. By *Gauss's Lemma*, $f(x)$ remains irreducible over $\mathbb{Q}$. In this case it is obvious that K is an extension of degree 4, since K is formed by adjoining to $\mathbb{Q}$ a root of an irreducible polynomial (over $\mathbb{Q}$) of degree 4.

Let E be the splitting field of $f(x)$ over $\mathbb{Q}$. By hypothesis we know that the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to S_4. Now, suppose that there exists a proper subfield of K containing $\mathbb{Q}$. Call this subfield F. But this means that the extensions F over $\mathbb{Q}$ and K over F must be of degree 2, since we have:

$$4 = [K : \mathbb{Q}] = [K : F][F : \mathbb{Q}]$$

Since the containment of F in K and of $\mathbb{Q}$ in F is proper, we have $[K : F] > 1$ and $[F : \mathbb{Q}] > 1$. Hence there must exist a normal subgroup, say N, of $\mathrm{Gal}(E/\mathbb{Q})$ of index 2. Hence there must exist an isomorphic copy of N in S_4 of index 2. The only such copy is A_4 (the set of all even permutations on 4 letters). Further, we know that the subgroup of $\mathrm{Gal}(E/\mathbb{Q})$ corresponding to K is contained in the subgroup of $\mathrm{Gal}(E/\mathbb{Q})$ corresponding to F. Furthermore, this containment is of index 2. Hence A_4 must contain a subgroup of index 2. But this is not the case! (see the subgroup lattice of A_4 on page 111 of Dummit and Foote).

As to the second part: the answer is no! The proof relies on the following result: if n is even and G is a group of order n, then G contains a subgroup of order 2. The proof of this result is outlined below.

Suppose that G is a group and that n even is its order. Then there are precisely $n-1$ non-identity elements in G, and $n-1$ is odd. We can couple each non-identity element with its inverse. Since there is an odd number of them, at least one must be its own inverse, say the element a. Then $\{1, a\}$ is clearly a subgroup of order 2.

Applying this result to a group of order 4, we see that this group contains a proper, normal subgroup. Since by the above this group must contain a subgroup of order 2, the index of this subgroup is 2. Hence this subgroup is normal and properly contained.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Applying this in the context of Galois theory: Suppose that E over $\mathbb{Q}$ is a Galois extension of degree 4. Then there exist proper subfields of this extension since the Galois group of $E/\mathbb{Q}$ contains a proper, normal subgroup.

Problem 34. *Page 582, #13: Prove that if the Galois group of the splitting field of a cubic, say $f(x)$, over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.*

Solution 34. First of all, notice that any polynomial of an odd degree has at least one real root (this can be proved analytically by showing that any such polynomial must attain positive and negative values; hence by the intermediate value theorem it must have a real root). Suppose that E is the splitting field of $f(x)$ over $\mathbb{Q}$. Suppose further that $f(x)$ is reducible. But then $f(x)$ can be written as $h(x)g(x)$ such that $h(x)$ is of degree 1. Hence $f(x)$ has a root in $\mathbb{Q}$. But then the splitting field E must be at most of degree 2. So the Galois group must be at most of order 2. This violates the hypothesis.

So suppose that $f(x)$ is irreducible. Let r be a real root of $f(x)$. Since r is not in $\mathbb{Q}$, we know that $\mathbb{Q}(r)$ must be an extension of degree 3. Since the Galois group of E over $\mathbb{Q}$ is of order 3, we conclude that $E = \mathbb{Q}(r)$. Since $f(x)$ splits in E we conclude that all roots of $f(x)$ are real.

Problem 35. *Page 582, #16: (a) Prove that $f(x) = x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$*
(b) Show the roots of this quartic are

$$\alpha_1 = \sqrt{1+\sqrt{3}} \quad \alpha_3 = -\sqrt{1+\sqrt{3}}$$
$$\alpha_2 = \sqrt{1-\sqrt{3}} \quad \alpha_4 = -\sqrt{1-\sqrt{3}}$$

(c) Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$, and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F$.
(d) Prove that K_1, K_2 and K_1K_2 are Galois over F with Gal(K_1K_2/F) the Klein 4-group. Write out the elements of this group explicitely. Determine all the subgroups of the Galois group and give their corresponding fixed subfields of K_1K_2 containing F.
(e) Prove that the splitting field of $f(x)$ over $\mathbb{Q}$ is of order 8 with digedral Galois group.

Solution 35. *(a) Consider $P =< 2 >$ a prime ideal of $\mathbb{Q}$. Then all but the leading coefficient of $f(x)$ are members of P. Now, 2, the constant term of $f(x)$, is not an element of P^2. So $f(x)$ satisfies the Eisenstein's Criterion.* Hence $f(x)$ is irreducible.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

(b) We can solve this equation using the quadratic formula: rewrite $f(x)$ as

$$f(x) = (x^2)^2 + 2(x^2) + 2$$

We can now use the quadratic formula to obtain solutions for x^2 (two of them). These will be α_1^2 and α_2^2. Taking square roots of the two, we obtain $\alpha_1, \ldots, \alpha_4$ as the solutions for x.

(c) We prove below that K_1 and K_2 both contain F. For now let us take it for granted. In view of this containment, we can consider K_1 and K_2 as extensions over F. We also take for granted that F is a degree 2 extension over $\mathbb{Q}$ (indeed this is trivial, by considering $x^2 - 3$ over $\mathbb{Q}$, which is irreducible in $\mathbb{Q}$ and splits in F). Hence K_1 and K_2 are degree 2 extensions over F since we have, say for K_1:

$$[K_1 : \mathbb{Q}] = [K_1 : F][F : \mathbb{Q}]$$

By the above, $[F : \mathbb{Q}] = 2$, and since $K_1 = \mathbb{Q}(\alpha_1)$, we know that $[K_1 : \mathbb{Q}] = 4$, we conclude that $[K_1 : F] = 2$. Similarly $[K_2 : F] = 2$.

Set $D_1 = 1 + \sqrt{3}$ and $D_2 = 1 - \sqrt{3}$. These are elements of F (this is trivial). Further, these are not squares in F. We prove this only for D_1. The proof for D_2 is similar. Since $[K_1 : F] = 2$, there exists an irreducible polynomial over F of degree 2 satisfied by D_1. Now, $x^2 - D_1$ is a polynomial satisfied by D_1 that is of degree 2. By uniqueness of the minimal polynomial, we conclude that $x^2 - D_1$ is precisely the minimal polynomial (hence irreducible) in F. But if D_1 was a square in F then the polynomial above could be reduced: $(x - \sqrt{D_1})(x + \sqrt{D_1})$. Hence D_1 is not a square in F.

$D_1 D_2 = (1 + \sqrt{3})(1 - \sqrt{3}) = -2$ which is clearly not a square in F (since F is a subset of $\mathbb{R}$).

Using this and the fact that $K_1 = F(\sqrt{D_1})$ and $K_2 = F(\sqrt{D_2})$, by problem 8 on page 530 of Dummit and Foote we concnlude that $[F(\sqrt{D_1}, \sqrt{D_2}) : \mathbb{Q}] = 4$. Hence $K_1 \neq K_2$.

Now, since α_1 is in K_1, we know that $\alpha_1^2 - 1 = \sqrt{3}$ is in K_1. Similarly $1 - \alpha_2^2 = \sqrt{3}$ is in K_2. So $K_1 \cap K_2$ contains $\mathbb{Q}(\sqrt{3})$. To show containment the other way, it will suffice to show that $[K_1 \cap K_2 : F] = 1$. Now, from the above we know that $[K_1 : F] = 2$. We also know that K_1 contains $K_1 \cap K_2$. We also know that $K_1 \cap K_2$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

contains F. So we have the following:

$$[K_1 : F] = [K_1 : K_1 \cap K_2][K1 \cap K_2 : F]$$

$$2 = [K_1 : K_1 \cap K_2][K1 \cap K_2 : F]$$

Now set $n = [K_1 : K_1 \cap K_2]$ and $m = [K1 \cap K_2 : F]$. Then either $n = 2$ and $m = 1$ or $m = 2$ and $n = 1$. If $n = 1$ then we're done. If $n = 2$ and $m = 1$, we must have $[K_1 \cap K_2 : \mathbb{Q}] = 2n = 4$ by the following:

$$[K_1 \cap K_2 : \mathbb{Q}] = [K_1 \cap K_2 : F][F : \mathbb{Q}] = 2n = 4$$

But $K_1 \cap K_2 \subseteq K_1$ and $[K_1 : \mathbb{Q}] = 4$. Hence we must have $K_1 \cap K_2 = K_1$. But this cannot be, since we proved above that K_1 is not contained in K_2. Hence $n = 1$. Hence $K_1 \cap K_2 = F$.

(d) As we showed above, $K_1 = F(\sqrt{D_1})$. We also showed that $\sqrt{D_1}$ was a root of an irreducible polynomial over F. We also showed that this polynomial split complitely over K_1. Since F is a field of characteristic 0 (since it contains $\mathbb{Q}$ which is of characteristic 0), we know that this polynomial must be separable since it's irreducible, and K_1 is its splitting field over F. So we conclude that K_1 over F is a Galois extension. Similarly K_2 is Galois over F.

Now, let $f(x)$ and $g(x)$ be the minimal polynomials satisfied by D_1 and D_2 over F, respectively. Then K_1 is the splitting field of $f(x)$ and K_2 is the splitting field of $g(x)$ (we showed this above). K_1K_2, as the smallest field that contains K_1 and K_2 can be viewed as the splitting field of $f(x)g(x)$. As we've seen above, $f(x)$ and $g(x)$ are irreducible over F. Since F is of characteristic zero, any product of irreducible polynomials over F must be separable. So K_1K_2 is the splitting field of a separable polynomial over F. So K_1K_2 must be Galois over F.

Problem 36. *Page 344, #8:* Let R be a ring and M an $R-$ module. Let $\text{Tor}(M) = \{m \in M : rm = 0 \text{ for some nonzero r in } R\}$.

(a) Prove that if R is an integral domain then $\text{Tor}(M)$ is a submodule of M.
(b) Give an example of a ring R and an R-module M such that $\text{Tor}(M)$ is not a submodule.
(c) If R has zero divisors show that every nonzero R-module has nonzero torsion elements.

Solution 36. (a) Suppose that M is a (nonzero) R-module. For convenience we'll use T for torsion of M. Now, T is nonempty, since 0_M is in T. We take for granted that $r(-m) = -rm$ for all m in M and r in R. Now, suppose that a, b are elements

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

of T. Then there exist elements r, s of R, both nonzero, such that $ra = 0_M$ and $sb = 0_M$ (notice also that sr is not zero since R is an integral domain). Consider: $rs(a-b) = rs(a) - rs(b)$. Since R is commutative (it's an integral domain), we have $rs(a-b) = s(ra) - r(sb) = 0$. So $a - b$ is in T for all a, b in T. So T is a subgroup of M. Suppose now that m is in T and r is in R. Since m is in T, there exists s, nonzero, in R such that $sm = 0$. So $s(rm) = r(sm) = 0$ since R is commutative. So rm is again in T. So T is a submodule of M.

(b) Consider $R = M_2(\mathbb{R})$ (the ring of 2×2 real matrices) as a module over itself. Now, it is clear that the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ belong to the torsion of R, since both are nonzero and their product is zero (they commute, so we can take product only one way). However, their sum is the 2×2 identity matrix, which certainly does not belong to the torsion of R. So the torsion of R is this case is not a submodule (it's not even a subgroup of R). This is because in this ring we have zero divisors.

(c) Suppose that R has zero divisors, say r, s. Now, suppose that M is an R-module. Let m be nonzero in R. If rm is zero, we're done. If not, consider: $s(rm) = (sr)m = 0_R m = 0_M$ since $sr = 0$ and s is not zero. Hence the torsion of M contains nonzero elements.

Problem 37. *Page 350, #8:* Let $\phi : M \to N$ be an R-module homomorphism. Prove that $\phi((\mathrm{Tor}(M)))$ is contained in $(\mathrm{Tor}(M)))$.

Solution 37. Let m be an element of the torsion of M. Then there exists a nonzero r in R such that $rm = 0$. Since ϕ is a homomorphism, we have, $0_N = \phi(rm) = r\phi(m)$ (zero is mapped to zero). Since r is nonzero, $\phi(m)$ is in the torsion of N. So the image of the torsion of M under ϕ is a subset of the torsion of N.

Problem 38. *Page 350, #11:* Let I be a nilpotent ideal in a commutative ring R, let M and N be R-modules and let $\phi : M \to N$ be an R-module homomorphism. Show that if the induced map $\overline{\phi} : M/IM \to N/IN$ is surjective, then so is ϕ.

Solution 38. We solve this problem only for the case where $I^2 = (0)$. The general case can then be obtained inductively by imploying the exact same algorithm, itterating n times.

Now, pick any $n + IN$ in N/IN. Since $\overline{\phi}$ is surjective, there exists $m + IM$ in M/IM such that $\overline{\phi}(m + IM) = n + IN$. That is, $\phi(m) + IN = n + IN$ by definition of $\overline{\phi}$. So $\phi(m) - n = in'$ where i is in I and n' is in N. Actually, this isn't

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

quite true. In place of in' we should have a finite sum whose terms are of them form in'. But for simplicity we'll write just one term. The result will hold true for ANY finite sum of the aforementioned form.

Now, similarly, there exists m' in M such that $\phi(m') - n' = i'n''$. From this,

$$n' = \phi(m') - i'n''$$

So

$$\phi(m) - n = i(\phi(m') - i'n'')$$

Since ϕ is a homomorphism, from above we get

$$\phi(m) - n = \phi(im') - ii''n''$$

Since $I^2 = 0$, $ii'' = 0$, so from above,

$$\phi(m) - n = \phi(im')$$

So, since ϕ is a homomorphism,

$$\phi(m - im') = n$$

Clearly $m - im'$ is in M. So ϕ is surjective.

Again, we did a very, very special case: $I^2 = 0$ and we used finite sums consisting of only one term! However, the exact same proof will work for any finite sum, and can be carried inductively to any n such that $I^n = 0$. It's just a mess to write out. The idea is exactly the same.

Problem 39. *Page 356, #3:* Show that the $F[x]$-modules in Excercises 18 and 19 of Section 1 (page 344) are both cyclic.

Solution 39. Well, suppose that $V = \mathbb{R}^2$. Suppose that $T : V \to V$ is a linear transformation defined by rotation about the origin clockwise by $\pi/2$ radians. Pick any v, not zero, in V. Notice that v and $T(v)$ are orthogonal (by definition of T). So clearly $\{v, T(v)\}$ form a basis for V. Pick any u in V. Then there exist a, b in $\mathbb{R}$ such that $aT(v) + bv = u$. Let $f(x) = ax + b \in F[x]$. Now viewing V as an $F[x]$-module, we see that $f(x)v = u$. So that V, as an $F[x]$-module is generated by v (in fact, by ANY nonzero v, which makes V into an irreducible $F[x]$-module and automatically answers the question of Excercise 18 in Section 1).

Let V be as above and let $T : V \to V$ by defined by projection onto the second coordinate. Pick $v = (1, 1)$. To show that v generates V it will suffice to show that $T(v)$ and v are linearly independent. Then the exact same argument as above

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

will do.

Now, by definition $T(v) = (0, 1)$. Consider: $c_1(1, 1) + c_2(0, 1) = 0$. Then $c_1 = 0$ and $c_1 + c_2 = 0$. So both, c_1 and c_2 are equal to zero. Hence v and $T(v)$ are linearly independent. By the argument we used above, v generates V.

Problem 40. *Page 356, #3:* Show that an R-module M is irreducible if, and only if, M is generated by every nonzero element. Determine all the irreducible $mathbbZ$-modules.

Solution 40. Suppose that M is irreducible. Then $M \neq 0$ by definition. Let m be a nonzero element of M. Clearly $< m >$ is a submodule of M. Since $1m = m$, and m is not zero, we know that $< m >$ is not zero. Since M is irreducible, it must be that $< m >= M$. So M is generated by any nonzero element.

Suppose that M can be generated by any nonzero element. Let N by a submodule of M that is not the trivial submodule. Then there exists a nonzero element n in N. Then also n is in M. Since M is generated by any nonzero element, we see that $M =< n >$. Since $< n >$ is a subset of N, we see that $N = M$. So that every sobmodule of M is either trivial or is all of M.

Now, we claim that all the irreducible $\mathbb{Z}$-modules are isomorphism classes of $\mathbb{Z}/p\mathbb{Z}$ for p ranging over primes.

Let M be a (nontrivial) $\mathbb{Z}$-module. We know exactly how $\mathbb{Z}$ acts on M: suppose m is in M and $n > 0$ is in $\mathbb{Z}$. Then $nm = (1 + 1 + \cdots + 1)(\text{n-times})m = m + m + \cdots + m$ n-times. Similarly for $n < 0$, $nm = -m + (-m) + \cdots + (-m)$ (n-times). Suppose that M is not finite. Then we can select nonzero m and n in M such that they are not inverses of each other. Since both, n and m generate M, there exists $|k|, |k'| \neq 1$ such that $kn = m$ and $k'm = n$. Hence $kk'm = m$. Hence $(kk'-1)m = 0$. Now, since $|k|$ and $|k'|$ are not equal to 1, $kk'-1$ is not zero. The, by action of $\mathbb{Z}$ on M, we know that the order of m in M is finite! But since m generates M, we know that M must be finite! Contradiction. Hence we know that M is finite.

So, M is a finite abelian group such that every nonzero element of M generates M (as an abelian group - we know this by way $\mathbb{Z}$ acts on M from above). Then, first of all, all such groups have a prime number of elements (if not, there would exist an element with order p where p divides the order of the group (Cauchy's Theorem); so p would generate a proper subgroup - contradiction). In which case

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

all such groups are isomorphism classes of $\mathbb{Z}/p\mathbb{Z}$ (any two cyclic groups of the same order are isomorphic - send the generator of one to the generator of the other).

Problem 41. *Page 356, #10:* Assume that R is commutative. Show that an R-module M is irreducible if, and only if, M is isomorphic (as an R-module) to R/I where I is a maximal ideal of R.

Solution 41. Suppose that R is commutative.

Suppose that I is a maximal ideal of R. Now, viewing R/I and R as R-modules, we know that, by the Lattice Isomorphism Theorem, there is a correspondence between submodules of R/I and those of R that contain I. We also know that there is a correspondence between the ideals of R and submodules of R. Indeed, every ideal of a RING R is a submodule of the MODULE R simply by the structure of ideals (they are additive abelian subgroups and absorb multiplication). Now, since R is maximal, the only ideals of R that contain I are R and I itself. Hence the only submodules of R that contain I are R and I itself. Hence the only submodules of R/I are (0) and R/I (by the Lattice Isomorphism Theorem, (0) corresponds to I and R/I corresponds to R). So R/I is irreducible. But R/I is isomorphic to M, so M is also irreducible (we show this below).

Conversely, suppose that M is irreducible. Now fix some nonzero m in M. Consider the map (viewing R as an R-module):

$$\phi : R \to M$$

defined by $r \mapsto rm$. Since m is nonzero, M is generated by m. Hence ϕ is surjective. We won't show that ϕ defines a homomorphism (trivial). By the First Isomorphism Theorem, ϕ is an isomorphism from R/I to M where I is the kernel of ϕ when ϕ maps R to M. Now, certainly I is a submodule of R. By the structure of I, I is also an ideal of R when R is viewed as a ring.

Now, R/I is irreducible since it is isomorphic to M which is irreducible. Again, by the Lattice Isomorphism Theorem, the submodules of R/I correspond to those of R containing I. But since R/I is irreducible, the only submodules of R/I are (0) and R/I. Now, R/I corresponds to R and (0) to I under the Lattice Isomorphism. So the only submodules of R containing I are R and I itself. However, as above, each ideal of R when R is viewed as a ring is a submodule of R when R is viewed as a module. But since the only submodules of R that contain I are R and I itself, the only ideals of R (when R is viewed as a ring) containing I are R and I itself. So I is maximal.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Problem 42. *Page 582, #17:*Let K/F be any finite extension and let $\alpha \in K$. Let L be a Galois extension of F containing K and let $H \leq \mathrm{Gal}(L/F)$ be the subgroup corresponding to K. Define the *norm* of α from K to F to be

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha)$$

where the product is taken over all the embeddings of K into an algebraic closure of F (so over a set of cosets representatives for H in $\mathrm{Gal}(L/F)$ by the Fundamental Theorem of Galois Theory). This is a product of Galois conjugates of α. In particular, if K/F is Galois this is $\prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$.

(a) Prove that $N_{K/F}(\alpha)$ is an element of F.
(b) Prove that $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$, so that the norm is a multiplicative map from K to F.
(c) Let $K = F(\sqrt{D})$ be a quadratic extension of F. Show that $N_{K/F}(a + b\sqrt{D}) = a^2 - Db^2$.
(d) Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ in $F[x]$ be the minimal polynomial for $\alpha \in K$ over F. Let $n = [K : F]$. Prove that d divides n, that there are d distinct Galois canjugates of α which are all repeated n/d times in the product above and conclude that $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$.

Solution 42. (a) Let us take any element, say τ, in $\mathrm{Gal}(L/F)$. Observe that $\tau(\sigma(\alpha))$ is also a Galois conjucate of α. In fact, since τ is injective, $\tau(N_{K/F}(\alpha)) = N_{K/F}(\alpha)$ since we have:

$$\tau(N_{K/F}(\alpha)) = \tau\left(\prod_{\sigma} \sigma(\alpha)\right) = \prod_{\sigma} \tau(\sigma(\alpha))$$

since τ preserves multiplication. But as we've pointed out, since τ is injective, the product immediately on the right above is simply a rearrangement of terms of the product defined in the problem above. Since we're working in a field, multiplication is commutative (and associative), hence any rearrangement of the terms of a product yeilds the same product. So every τ in $\mathrm{Gal}(L/F)$ fixes $N_{K/F}(\alpha)$. But we know that the fixed field of all automorphisms in $\mathrm{Gal}(L/F)$ is precisely F. Hence $N_{K/F}(\alpha)$ must belong to F.

(b) This is immediate, since each imbedding of K is in particular a homomorphism:

$$N_{K/F}(\alpha\beta) = \prod_{\sigma} \sigma(\alpha\beta) = \prod_{\sigma} \sigma(\alpha)\sigma(\beta)$$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

We can rearrange the terms of the product above in any way, since multiplication is associative and commutative. A suitable rearrangement yeilds:

$$\prod_{\sigma} \sigma(\alpha)\sigma(\beta) = \left(\prod_{sigma} \sigma(\alpha) \right) \left(\prod_{sigma} \sigma(\beta) \right)$$

Which by definition is $N_{K/F}(\alpha)N_{K/F}(\beta)$

(c) Since in this case K/F is Galois, the product is taken over all the members of Gal(K/F). There are just two such members: the identity, say σ and the map determined by $\sqrt{D} \mapsto -\sqrt{D}$ (this map fixes F, of course), say τ. With this in mind we have:

$$N_{K/F}(a + b\sqrt{D}) = \sigma(a + b\sqrt{D})\tau(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D$$

Now on to the part that took me 2 days (having a surprisingly simple solution!):

(d) Consider the tower $F \subseteq F(\alpha) \subseteq K$. Then we have:

$$[K : F] = [K : F(\alpha)][F(\alpha) : F] = [K : F(\alpha)]d \tag{0.5}$$

Hence d divides $[K : F]$. Now, since L/F is a Galois extension, we know that L/F is a separable extension. We know that every irreducible polynomial with coefficients in F is separable. Since $m_\alpha(x)$ is such a polynomial, it must be separable. Further, since α, a root of $m_\alpha(x)$, is in L, then all conjucates of α are also in L. Hence $m_\alpha(x)$ has precisely d distinct roots, all of which are in L (all of the above are immediate consequences of Theorem 13 on page 572).

Now, let us set $k = [K : F(\alpha)]$. We know from 0.5 that $k = n/d$. We'll need this shortly. Now, consider F', a field isomorphic to F under some isomorphism ϕ. Of course F' exists (F is one such F'). We know that there exists σ, an isomorphism from $F(\alpha)$ to $F'(\alpha')$, where α' is a root of the isomorphic image of $m_\alpha(x)$ in F', such that σ extends ϕ. We also know that there exists K', an extension of $F'(\alpha)$ of degree k such that K is isomorphic to K' under an isomorphism τ that extends σ. The question we ask is this: how many such possible extensions τ are there? In fact, when we take $F' = F$ and $K' = K$, the number of such extensions is precisely the number of times each σ appears in the product defining $N_{K/F}(\alpha)$ (since all such extensions τ are precisely all the imbeddings of K considered in the definition of $N_{K/F}(\alpha)$). Well, the isomorphism extension theorem tells us that for each σ, there are precisely k extensions τ. As we saw above, $k = n/d$. Hence each

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

σ in the product of $N_{K/F}(\alpha)$ will appear precisely n/d times!

(There MUST be a more precise, more elegant and shorter way of saying what I've just said above).

Now, since there are d distinct conjucages of α, we know that there exist imbeddings of K, $\sigma_1, \ldots, \sigma_d$ (one of them being the identity) such that all the conjugates of α are in $\{\sigma_1(\alpha), \ldots, \sigma_d(\alpha)\}$. Since $m_\alpha(x)$ splits in L, we can write,

$$m_\alpha(x) = \prod_{j=1}^{d} (x - \sigma_j(\alpha))$$

When we expend the product above, we get a polynomial of the form,

$$p(x) = x^d - \left(\sum_{j=1}^{d} \sigma_j(\alpha)\right) x^{d-1} + \cdots + (-1)^d \prod_{j=1}^{d} \sigma_j(\alpha) \tag{0.6}$$

The reason we wrote it in such form above will become apparent in a moment (we'll use this in the next problem too).

Notice that the polynomial above is monic of degree d and is satisfied by α. Further, we know that in L, this polynomial divides $m_\alpha(x)$. But since both are monic, and both are satisfied by α, we conclude that $m_\alpha(x) = p(x)$. In which case the constant term of $p(x) = a_0$, the constant term of $m_\alpha(x)$. So we have:

$$a_0 = (-1)^d \prod_{j=1}^{d} \sigma_j(\alpha)$$

Multiplying both sides by $(-1)^d$ we obtain

$$(-1)^d a_0 = \prod_{j=1}^{d} \sigma_j(\alpha)$$

Rasing each side to the power n/d (which is an integer, since as we saw above, $d|n$), we obtain

$$(-1)^n a_0^{n/d} = \left(\prod_{j=1}^{d} \sigma_j(\alpha)\right)^{n/d}$$

Remember, as we saw above, each σ_k is repeated precisely n/d times in the product of $N_{K/F}(\alpha)$. So if we distribute the exponent n/d over the product above, we end up exactly with $N_{K/F}(\alpha)$. Hence the conclusion: $(-1)^n a_0^{n/d} = N_{K/F}(\alpha)$.

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

Problem 43. *Page 582, #18:*With notation as in the previous problem, define the *trace* of α from K to F to be

$$Tr_{K/F}(\alpha) = \sum_{\sigma} \sigma(\alpha)$$

a sum of Galois conjugates of α.

(a) Prove that $Tr_{K/F}(\alpha)$ is in F.
(b) Prove that $Tr_{K/F}(\alpha + \beta) = Tr_{K/F}(\alpha) + Tr_{K/F}(\beta)$.
(c) Let $K = F(\sqrt{D})$ be a quadratic extension of F. Show that $Tr_{K/F}(a + b\sqrt{D}) = 2a$.
(d) Let $m_\alpha(x)$ be as in the previous problem. Prove that $Tr_{K/F}(\alpha) = -\frac{n}{d}a_{d-1}$.

Solution 43. (a) As in the previous problem, it will suffice to show that $Tr_{K/F}(\alpha)$ is fixed by every element τ of $\mathrm{Gal}(L/F)$. So consider any such τ acting on $Tr_{K/F}(\alpha)$:

$$\tau(Tr_{K/F}(\alpha)) = \tau\left(\sum_{\sigma} \sigma(\alpha)\right) = \sum_{sigma} \tau(\sigma(\alpha))$$

since τ is a homomorphism. Since each $\sigma(\alpha)$ above is a conjugate of α, $tau(\sigma(\alpha))$ must also be a conjugate of α. Hence τ simply rearranges the terms of the sum of $Tr_{K/F}(\alpha)$. But since addition in this case is commutative and associative, any rearrangement will yeild the same result. Hence $Tr_{K/F}(\alpha)$ is fixed by each τ of $\mathrm{Gal}(L/F)$. This shows that $Tr_{K/F}(\alpha)$ is in F.

(b) Consider:

$$Tr_{K/F}(\alpha + \beta) = \sum_{\sigma} \sigma(\alpha + \beta) = \sum_{\sigma} (\sigma(\alpha) + \sigma(\beta))$$

since each σ is a homomorphism. Since addition is commutative and associative, we can write the last sum above as

$$\sum_{\sigma} \sigma(\alpha) + \sum_{\sigma} \sigma(\beta)$$

which is precisely $Tr_{K/F}(\alpha) + Tr_{K/F}(\beta)$.

(c) Just as in the previous problem, in this case K/F is a Galois extension. Hence the sum in $Tr_{K/F}(\alpha)$ is taken over the elements of the Galois group of K/F. There are precisely two such elements: the identity σ and the automorphism $\tau : \sqrt{D} \mapsto -\sqrt{D}$. So we have:

$$Tr_{K/F}(a + b\sqrt{D}) = \sigma(a + b\sqrt{D}) + \tau(a + b\sqrt{D}) = (a + b\sqrt{D}) + (a - b\sqrt{D}) = 2a$$

More solutions manual at www.DumbLittleDoctor.com
Thanks to the William's work!

since τ fixes F and is a homomorphism.

(d) As we know from part (d) of the previous problem, $m_\alpha(x) = p(x)$ ($p(x)$ as defined above). So from 0.6 we conclude that

$$a_{d-1} = -\sum_{j=1}^{d} \sigma_j(\alpha)$$

where $\sigma_k, 1 \leq k \leq d$ were defined in the solution to part (d) of the previous problem. Hence we have

$$-a_{d-1} = \sum_{j=1}^{d} \sigma_j(\alpha)$$

Hence

$$-\frac{n}{d}a_{d-1} = \frac{n}{d}\sum_{j=1}^{d} \sigma_j(\alpha) = \sum_{j=1}^{d} \frac{n}{d}\sigma_j(\alpha)$$

But we know that each σ_k in the sum above repeats n/d times in the sum defining $Tr_{K/F}(\alpha)$. Hence the conclusion $Tr_{K/F}(\alpha) = -\frac{n}{d}a_{d-1}$.