Homework for MTH 419H Honors Algebra II
Spring Semester 2016 Section 001

Homework due 01/15/2016: Ch. 8 # 1.1, 2.1, 2.2, 3.1, 3.2, 3.3

Homework due 01/22/2016: Ch. 8 # 3.4, 3.5, 4.1, 4.2, 4.3, 4.4

Homework due 01/29/2016: Ch. 8 # 4.5, 4.6, 4.7, 4.8 , 4.9, 4.10, 4.11, 4.12

Homework due 02/05/2016: Ch. 8 # 4.20, 4.21, 5.2, 5.3, 6.1, 6.2

Homework due 02/12/2016: Ch. 8 # 6.3, 6.4, 6.5, 6.6, 6.12, 6.13

Suggested problems: Ch. 9: # 3.2, 3.3, 3.4

Homework due 02/26/2016: Ch. 11 # 1.1, 1.3, 1.6, 1.8, 2.2 and The Freshman's Dream (see below).

The Freshman's Dream: Prove that in the ring $R = \mathbb{Z}/n\mathbb{Z}$ that $(a+b)^n = a^n + b^n$ for each $a, b \in R$ provided that n is a prime. Is the dream true if n is not prime? What if n is a power of a prime?

Homework due 03/14/2016: Ch. 11 # 3.3 (a,b,c), 3.4, 3.8, 4.1, 4.2, 4.3 (a,b,c)

Homework due 03/18/2016: Ch. 11 # 5.1, 5.4, 5.5, 5.7, 7.1 (try to prove this without assuming that $1 \in R$), 7.3

Homework due 03/30/2016: Ch. 12 # 1.2, 1.3, 1.4, 2.1, 2.2, 2.3, 2.5, 2.6

Homework due 04/11/2016: Ch. 12 #2.7, 2.8, 3.1, 3.2, 3.3, 4.1, 4.2, 4.3

EXAM II is on Thursday, 04/14/2016 at 5:30 p.m.
(This is a change from the original date of 04/072016.)

Homework due 04/20/2016: Ch. 12 # 4.4, 4.9, 4.15, 4.16; Ch. 15 # 2.2, 3.1, 3.3, 3.6

Homework due 04/27/2016: Ch. 15 # 3.7, 3.10, 5.2, 5.3, 6.1, 7.4, 7.8, 10.1

Additional Problems (not collected): Ch. 16 #3.1, 3.2, 4.1, 6.1, 6.2, 7.4, 7.6

Solutions

8.1.1 Show that a bilinear form $\langle , \rangle$ on a real vector space V is a sum of a symmetric form and a skew-symmetric form.

Solution:

$$\langle v, w\rangle = \frac{1}{2}(\langle v, w\rangle + \langle w, v\rangle) + \frac{1}{2}(\langle v, w\rangle - \langle w, v\rangle)$$

8.2.1 Prove that the maximal entries of a positive definite, symmetric, real matrix are on the diagonal.

Solution: Let A be a positive definite symmetric, real matrix. Let $e_1, \ldots, e_n$ be the standard basis vectors. In general, $e_i^t A e_j = e_i^t A_j = a_{ij}$, where A_j is the j-th column of A, i.e. $A_j = (a_{1j}, \ldots, a_{jn})^t$. Since a 1×1 matrix has only one entry, we may assume that $n \geq 2$. For each $1 \leq i \neq j \leq n$,

$$0 < (e_i - e_j)^t A(e_i - e_j) = a_{ii} + a_{jj} - 2a_{ij}$$

since $a_{ij} = a_{ji}$. Therefore,

$$a_{ij} < \frac{1}{2}(a_{ii} + a_{jj}) \leq \max\{a_{ii}, a_{jj}\}.$$

For any finite sets of real numbers $S \subseteq T \subset \mathbb{R}$, $\max S \leq \max T$; therefore, a_{ij} is less than the maximum value of the diagonal entries.

If A was a positive definite, Hermitian matrix, then the diagonal entries are real and $a_{ij} + a_{ji} = a_{ij} + \overline{a_{ij}} = 2\Re(a_{ij})$, i.e. twice the real part of a_{ij}. We conclude that the real part of a positive definite, Hermitian matrix has the same property: the maximal entries occur on the diagonal. This suggests the following question: if $A = B + iC$ is the decomposition of a positive definite, Hermitian matrix into its real and imaginary parts, is B symmetric and positive definite? What about C? See exercise 3.2.

8.2.2 Let A and A' be symmetric matrices related by $A' = P^t AP$ for some invertible matrix P. Are the ranks of A and A' equal?

Solution: Yes. As a linear map $P^t AP : \mathbb{R}^n \to \mathbb{R}^n$. Since P is invertible, it is an isomorphism. Since P^t is also invertible (with inverse equal to the transpose of P^{-1}), it too is an isomorphism. The rank of a linear map is the dimension of its image. It follows that the rank of $P^t AP$ is the rank of A.

8.3.1 Is a complex $n \times n$ matrix A such that X^*AX is real for all X Hermitian?

Solution: Yes. As in exercise 2.1, we choose values of X using standard basis vectors. Since $e_i^t A e_i = a_{ii} \in \mathbb{R}$, we have, in particular, that a_{ii} is real. Since

$$(e_i + e_j)^t A(e_i + e_j) = a_{ii} + a_{ij} + a_{ji} + a_{jj} \in \mathbb{R}$$

and $a_{ii} + a_{jj}$ is real, we have that $a_{ij} + a_{ji}$ is real. In particular, $\Im(a_{ij} + a_{ij}) = 0$, i.e. the imaginary part of $a_{ij} + a_{ji}$ is zero. Therefore,

$$\Im(a_{ij}) = -\Im(a_{ji}) = \Im(\overline{a_{ji}}).$$

Since

$$(e_i + i\, e_j)^t A(e_i + i\, e_j) = a_{ii} + i\, a_{ij} - i\, a_{ji} + a_{jj} \in \mathbb{R}$$

and $a_{ii} + a_{jj}$ is real, we have that $i(a_{ij} - a_{ji})$ is real. Therefore, $\Re(a_{ij} - a_{ji}) = 0$. And so,

$$\Re(a_{ij}) = \Re(a_{ji}) = \Re(\overline{a_{ji}}).$$

Since both the real and imaginary parts are equal, $a_{ij} = \overline{a_{ji}}$. Hence $A = A^*$.

8.3.2 Let $\langle , \rangle$ be a positive definite Hermitian form on a complex vector space V. Restrict scalars to $\mathbb{R}$ so that V is a real vector space. Prove that the real part $\{ , \}$ and the imaginary part $[,]$ of $\langle , \rangle$ define a symmetric, positive definite form and a skew-symmetric form, respectively, on V as a real vector space.

Solution: The *restriction of scalars* is defined formally as follows. Let $\phi : \mathbb{R} \to \mathbb{C}$ be the inclusion $\phi(c) = c + i\, 0 \in \mathbb{C}$. The set V is given the structure of a real vector space using the addition defined by its complex vector space structure and by using the following rule to multiply a vector $v \in V$ by a scalar $c \in \mathbb{R}$: $c.v = \phi(c)v$.

This above sounds more complicated than it needs to be; but it's challenging to say precisely what one means. In particular, one can ask if V becomes an n-dimensional or a $2n$-dimensional real vector space given that V is an n-dimensional complex vector space. In fact, V is a $2n$-dimensional real vector space. Here's a sketch: let $V = \mathbb{C}$, a one dimensional complex vector space. Let $a, b \in \mathbb{R}$. The linear combination $a.1 + b.i = \phi(a)1 + \phi(b)i$ is zero if and only if $\phi(a) = 0$ and $\phi(b) = 0$. Therefore, 1 and i are linearly independent.

Let's now solve the exercise. Let $u, v, w \in V$ and $a, b \in \mathbb{R}$. If $z = x + y\,i$ is a complex number with real part x and imaginary part y, then we write $\Re z = x$ and $\Im z = y$ to express this.

By definition, $\{u, v\} = \Re\langle u, v\rangle$ and $[u, v] = \Im\langle u, v\rangle$. We first prove that $\{,\}$ is a bilinear form on V with scalars restricted to $\mathbb{R}$:

$$\{u+v, w\} = \Re\langle u+v, w\rangle = \Re(\langle u, w\rangle+\langle v, w\rangle) = \Re\langle u, w\rangle+\Re\langle v, w\rangle = \{u, w\}+\{v, w\}$$

and

$$\{a.v, w\} = \Re\langle\phi(a)v, w\rangle = \Re(\overline{\phi(a)}\langle v, w\rangle) = \Re(\phi(a)\langle v, w\rangle) = \phi(a)\{v, w\} = a.\{v, w\}.$$

Verifying linearity in the second coordinate is similar, except one does not need to worry about the conjugation of the scalar. Verifying that $[,]$ is bilinear is similar, but nontrivial. I omit the proof, but you should try to write out an argument if you did not even address whether or not these forms are bilinear in your solution to this problem.

To prove it is symmetric, we compute as follows:

$$\{v, w\} = \Re\langle v, w\rangle = \Re\overline{\langle w, v\rangle} = \Re\langle w, v\rangle = \{w, v\}.$$

Finally, as

$$\{v, v\} = \Re\langle v, v\rangle = \langle v, v\rangle \geq 0,$$

with equality if and only if $v = 0$, we have that $\{,\}$ is positive definite.

As,

$$[v, w] = \Im\langle v, w\rangle = \Im\overline{\langle w, v\rangle} = -\Im\langle w, v\rangle = -[w, v],$$

we have that $[,]$ is skew-symmetric.

8.3.3 The set of $n \times n$ Hermitian matrices forms a real vector space. Find a basis for this space.

Solution: First, let's prove that this is a vector space. If A and B are Hermitian and c is a real number, then $(cA + B)^* = cA^* + B^*$, which proves that the set is closed under addition and scalar multiplication.

Since this set is a subset of the real vector space of all complex $n \times n$ matrices, these are the only two axioms of a vector space that we need to check.

To find a basis, let e_{ij} denote the $n \times n$ matrix with a one in the i, j entry and zeroes in every other entry. Let

- $D = \{e_{ii} \mid 1 \leq i \leq n\}$ (Diagonal),
- $O = \{e_{ij} + e_{ji} \mid 1 \leq i < j \leq n\}$ (Off-diagonal), and
- $IO = \{i \cdot e_{ij} - i \cdot e_{ji} \mid 1 \leq i < j \leq n\}$ (Imaginary Off-diagonal).

The claim is that $D \cup O \cup IO$ is a basis. It is easy to verify that each element of this set is Hermitian.

Suppose that $A = (a_{ij})$ is a Hermitian matrix. Let $x_{ij} = \Re a_{ij}$ and $y_{ij} = \Im a_{ij}$ so that $a_{ij} = x_{ij} + i \cdot y_{ij}$. Then, $A^* = A$ implies that $x_{ij} = x_{ji}$, $y_{ij} = -y_{ji}$ and $y_{ii} = 0$ for all $1 \leq i, j \leq n$. We have that

$$A = \sum_{1 \leq i,j \leq n} a_{ij} e_{ij} = \sum_{1 \leq i,j \leq n} x_{ij} e_{ij} \sum_{1 \leq i,j \leq n} y_{ij} (i \cdot e_{ij})$$

$$= \sum_{e_{ii} \in D} x_{ii} e_{ii} + \sum_{e_{ij} + e_{ji} \in O} x_{ij} (e_{ij} + e_{ji}) + \sum_{i \cdot e_{ij} - i \cdot e_{ji} \in IO} y_{ij} (i \cdot e_{ij} - i \cdot e_{ji})$$

Therefore, $D \cup O \cup IO$ spans this vector space. To see these vectors are linearly independent, suppose we have a linear combination which sums to the zero matrix. Then $a_{ij} = 0$ for all i and j. This implies that the real and imaginary parts of a_{ij} are both zero. And therefore, all of the coefficients in the above linear combination are zero.

8.3.4 Prove that if $A \in \mathrm{GL}_n(\mathbb{C})$, then A^*A is Hermitian and positive definite.

Solution: Since $(A^*A)^* = A^*(A^*)^* = A^*A$, we have that A^*A is Hermitian. Let X be a non-zero column vector. Let $Y = AX$. Since A is invertible, Y is nonzero. A direct computation shows that

$$X^*A^*AX = (AX)^*AX = Y^*Y = \sum_{i=1}^{n} |y_i|^2 > 0.$$

Therefore, A^*A is positive definite.

8.3.5 Let A and B be positive definite Hermitian matrices. Decide which of the following are necessarily positive definite Hermitian:

$$A^2, \quad A^{-1}, \quad AB, \quad A+B.$$

Solution: We first decide whether each of these matrices is Hermitian. (This approach to the problem is less direct, but we will learn more information.) Assume that A and B are Hermitian (but not necessarily positive definite).

(a) We have that $(A^2)^* = (AA)^* = A^*A^* = AA = A^2$ is Hermitian.

(b) $I = I^* = (A^{-1}A)^* = A^*(A^{-1})^* = A(A^{-1})^*$ implies that (A^{-1}) is a (right) inverse of A. Therefore, $(A^{-1})^* = A^{-1}$ is Hermitian.

(c) We see that AB is Hermitian if and only if A and B commute: $AB = (AB)^* = B^*A^* = BA$. To find a counterexample the question at hand, let $P = ((1,0)^t, (1,1)^t)$ and $Q = ((2,0)^t, (0,1)^t)$. Since P and Q have nonzero determinants, we can use the previous exercise (Ch. 8, 3.4) to conclude that $A = P^*P = ((1,1)^t, (1,2)^t)$ and $B = Q^*Q = ((4,0)^t, (0,2)^t)$ are positive definite Hermitian matrices. A direct computation shows that $AB \neq BA$.

(d) We have that $(A+B)^* = A^* + B^* = A + B$ is Hermitian.

Now, we assume that A and B are Hermitian and positive definite.

(a) Using exercise 3.4, we see that $A^2 = AA = A^*A$ is Hermitian and positive definite.

(b) As A is positive definite, A is invertible (since $AX \neq 0$ for all $X \neq 0$). Suppose that $X \neq 0$. Let $Y = A^{-1}X$, so that $X = AY$. Since $Y \neq 0$ and $A = A^*$, we have that

$$X^*A^{-1}X = (AY)^*A^{-1}(AY) = Y^*A^*Y = Y^*AY > 0.$$

Therefore, A^{-1} is also positive definite (and Hermitian by the analysis above).

(c) As above, AB is not necessarily Hermitian.

(d) Since $X^*(A+B)X = X^*AX + X^*BX > 0$ if $X \neq 0$, we see that $A+B$ is positive definite (and Hermitian by the analysis above).

8.4.1 What is the inverse of a matrix whose columns are orthogonal?

Solution: Suppose that $P = (v_1, \ldots, v_n)$ is a matrix whose column vectors $v_1, \ldots, v_n$ are orthogonal. Consider P^tP. Since $v_i^t v_j = 0$ if $i \neq j$ and $v_i^t v_i = \|v_i\|^2$, the length squared, we see that P^tP is diagonal with diagonal entries the squares of the lengths of the vectors. Let Λ the diagonal matrix with diagonal entries $\lambda_{ii} = \|v_i\|^{-2}$. (Note: if $\|v_i\| = 0$ for some i, then $v_i = 0$ and so P is not invertible; so, we may assume that these lengths are nonzero.) It follows that $\Lambda P^t P = I$. Therefore, $P^{-1} = \Lambda P^t$.

8.4.2 Let $\langle , \rangle$ be a bilinear form on a real vector space V, and let $v \in V$ such that $\langle v, v \rangle \neq 0$. What is the formula for the orthogonal projection $\pi : V \to W = v^\perp$?

Solution: We can decompose an arbitrary vector $u \in V$ as $w + cv$ for some scalar c since $V = W \oplus W^\perp$ by Theorem 8.4.5. (Note: Theorem 8.4.5 applies since $\langle v, v \rangle \neq 0$ and so the form is non-degenerate on the span of v.) The projection is given by $\pi(u) = w = u - cv$. Since

$$\langle u, v \rangle = \langle w, v \rangle + c\langle v, v \rangle = 0 + c\langle v, v \rangle,$$

we see that $c = \langle u, v \rangle / \langle v, v \rangle$. Therefore,

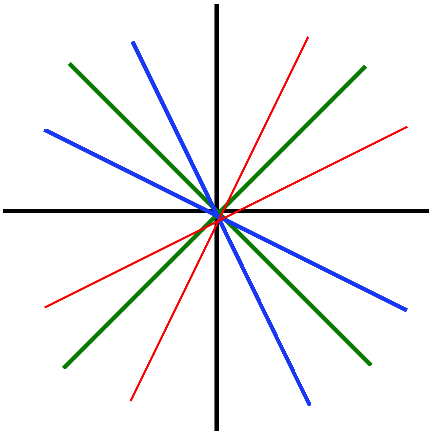
$$\pi(u) = u - \frac{\langle u, v \rangle}{\langle v, v \rangle} v.$$

8.4.3 Let A be a real $m \times n$ matrix. Prove that $B = A^tA$ is positive semidefinite, i.e. $X^tBX \geq 0$ for all X. And prove that A and B have the same rank.

Solution: $X^tBX = X^tA^tAX = (AX)^t(AX) \geq 0$ because $Y^tY \geq 0$ for all $Y \in \mathbb{R}^m$ with equality if and only if $Y = 0$. Thus, $X^tBX = 0$ precisely when $AX = 0$, i.e. X is in the null space (also called the kernel) of A. In particular, if X is in the null space of B, then $X^tBX = 0$ and so $AX = 0$ by the above. Conversely if $AX = 0$, then $BX = A^tAX = 0$. Therefore, the nullity (and, even stronger, the null space) of A and B are the same. Since for both matrices, the nullity plus the rank is equal to n, both matrices have the same rank.

8.4.4 Make a sketch showing the positions of some orthogonal vectors in $\mathbb{R}^2$ when the form is $\langle X, Y \rangle = x_1y_1 - x_2y_2$.

Solution:



In the figure above, the black lines are the x and y axes. These are orthogonal to each other. The green lines are the lines $y = x$ and $y = -x$; each of these is orthogonal to itself. The blue lines are orthogonal to one another; these have equations $y = -2x$ and $y = -x/2$. Finally, the red lines are orthogonal to each other; they have equations $y = 2x$ and $y = x/2$.

8.4.5 Find an orthogonal basis for the forms on $\mathbb{R}$ having matrices A and B as shown below.

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Solution: For A which define $\langle , \rangle$, let $v_1 = [1, 0]^t$. We have that $\langle v_1, v_1 \rangle = 1$. Let $w_2 = [0, 1]^t$. Let

$$v_2 = w_2 - \frac{\langle v_1, w_2 \rangle}{\langle v_1, v_1 \rangle} v_1 = [0, 1]^t - [1, 0]^t = [-1, 1].$$

By design, v_1 and v_2 are orthogonal. They are linearly independent (e.g. compute the determinant of $[v_1, v_2]$) and therefore form a basis.

For B which defines $\langle , \rangle$, let $v_1 = [1, 0, 0]^t$. Again, we have that $\langle v_1, v_1 \rangle = 1$. Let $w_2 = [0, 1, 0]^t$. Let

$$v_2 = w_2 - \frac{\langle v_1, w_2 \rangle}{\langle v_1, v_1 \rangle} v_1 = [0, 1, 0]^t - [0, 0, 0]^t = [0, 1, 0]^t.$$

Again, by design, v_1 and v_2 are orthogonal. We repeat this process. We have that $\langle v_2, v_2\rangle = 2$. Let $w_3 = [0,0,1]^t$. Let

$$v_3 = w_3 - \frac{\langle v_1, w_3\rangle}{\langle v_1, v_1\rangle} v_1 - \frac{\langle v_2, w_3\rangle}{\langle v_2, v_2\rangle} v_2 = [0,0,1]^t - [1,0,0]^t - [0,1/2,0]^t = [-1,-1/2,1]^t.$$

By design, $\{v_1, v_2, v_3\}$ is orthogonal and these form a basis (e.g. compute the determinant of $[v_1, v_2, v_3]$).

8.4.6 Extend the vector $X_1 = \frac{1}{2}(1,-1,1,1)^t$ to an orthonormal basis of $\mathbb{R}^4$.

8.4.7 Apply the Gram-Schmidt procedure to the basis $(1,1,0)^t$, $(1,0,1)^t$, $(0,1,1)^t$ of $\mathbb{R}^3$.

8.4.8 Let $A = (a_{ij})$ be the 2×2 matrix with $a_{11} = a_{22} = 2$ and $a_{12} = a_{21} = 1$. Find an orthonormal basis for $\mathbb{R}^2$ with respect to the form X^tAY.

8.4.9 Find an orthonormal basis for the vector space P of all real polynomials of degree at most 2 with the symmetric form defined by

$$\langle f, g\rangle = \int_{-1}^{1} f(x)g(x)\,dx.$$

8.4.10 Let V be the vector space of real $n \times n$ matrices. Prove that $\langle A, B\rangle = \text{trace}(A^tB)$ defines a positive definite bilinear form on V, and find an orthonormal basis for this form.

Solution: We first show the form is bilinear. Let $A, B, C \in V$ and $\alpha \in \mathbb{R}$:

$$\langle A+B, C\rangle = \text{trace}((A+B)^tC) = \text{trace}(A^tC + B^tC) =$$

$$\text{trace}(A^tC) + \text{trace}(B^tC) = \langle A, C\rangle + \langle B, C\rangle$$

and

$$\langle \alpha A, B\rangle = \text{trace}((\alpha A)^tB) = \alpha\,\text{trace}(A^tB) = \alpha\langle A, B\rangle.$$

To see it is positive definite, we analyze matrix multiplication: if $C = AB$ and $A = (a_{ij})$, $B = (b_{ij})$, and $C = (c_{ij})$, then

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

It follows, that if $C = A^t B$, then

$$c_{ij} = \sum_{k=1}^{n} a_{ki} b_{kj}.$$

Thus, the trace of $C = A^t A$ is

$$\sum_{i=1}^{n} \sum_{k=1}^{n} a_{ki} a_{ki},$$

which is a sum of squares of real numbers in which every entry of the matrix $A = (a_{ij})$ appears exactly once. Therefore, the form is positive definite.

An orthonormal basis is $\{e_{ij}\}_{1 \le i,j \le n}$, where e_{ij} is the matrix whose only nonzero entry has a value of 1 and occurs in the (i,j) position. Using the above formula, we see that

$$\text{trace}(e_{ij}^t e_{ij}) = 1$$

and

$$\text{trace}(e_{ij}^t e_{kl}) = 0$$

if $(i,j) \neq (k,l)$ since each term in the sum appearing in the formula is a product of two entries having exactly the same positions.

8.4.11 Let W_1 and W_2 be subspaces of a vector space V with a symmetric bilinear form. Prove the following properties.

(a) $W_1 + W_2)^\perp = W_1^\perp \cap W_2^\perp$

(b) $W \subset W^{\perp\perp}$

(c) If $W_1 \subset W_2$, then $W_2^\perp \subset W_1^\perp$.

8.4.12 Let $V = \mathbb{R}^{2\times 2}$.

(a) Determine the matrix of the bilinear form $\langle A, B \rangle = \text{tr}(AB)$ with respect to the standard basis e_{ij}.

Solution: Let $\langle A, B \rangle_t = \text{trace}(A^t, B)$, i.e. the form appearing in the previous exercise. Using the results of that exercise, we have that

$$\langle e_{ij}, e_{kl} \rangle = \langle e_{ij}^t, e_{kl} \rangle_t = \langle e_{ji}, e_{kl} \rangle_t,$$

which is 1 if $(j,i) = (k,l)$ and 0 otherwise.

It follows that the matrix of the form on $V = \mathbb{R}^{2\times 2}$ is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where the ordered basis is $(e_{11}, e_{12}, e_{21}, e_{22})$.

(b) Determine the signature of the form above.

Solution: Consider the ordered basis $(e_{11}, e_{22}, (e_{12} + e_{21})/2, (e_{12} - e_{21})/2$. It is straightforward to check that this is an orthogonal basis and the matrix with respect to this ordered basis is, in block form,

$$\begin{pmatrix} I_3 & 0 \\ 0 & -I_1 \end{pmatrix}.$$

Therefore, the signature is $(3, 1)$.

(c) Find an orthogonal basis for this form.

Solution: I did this in part (b).

(d) Determine the signature of the form trace(AB) on $\mathbb{R}^{n\times n}$.

Solution: The set

$$\{e_{11}, \ldots, e_{nn}\} \cup \{p_{ij}, n_{ij}\}_{1\leq i<j\leq n}$$

is an orthogonal basis, where $p_{ij} = (e_{ij} + e_{ji})/2$ and $n_{ij} = (e_{ij} - e_{ji})/2$. As in the 2×2 case, the matrices $\{e_{ii}\}$ and the matrices $\{p_{ij}\}$ pair with themselves to a value of 1. The matrices $\{n_{ij}\}$ pair with themselves to a value of -1. The number of negative ones is $\binom{n}{2}$. Therefore, the signature is

$$\left(n^2 - \binom{n}{2}, \binom{n}{2}\right) = \left(\frac{n^2+n}{2}, \frac{n^2-n}{2}\right).$$

Verification of the above claims is straightforward using the formula for the trace of the product of two matrices.

8.4.20 Prove Sylvester's Criterion for positive definiteness: a real symmetric $n \times n$ matrix $A = (a_{ij})$ is positive definite if and only if for each $k = 1, \ldots, n$ the upper left $k \times k$ minor, $A_k = (a_{ij})_{1\leq i,j\leq k}$, has positive determinant.

Solution: If A is 1×1, then $v^t A v = a_{11} v^2 > 0$ if and only if $a_{11} > 0$ and $v \neq 0$. So, the criterion holds for $n = 1$. Let $n \geq 2$. Assume the criterion holds for $1, \ldots, n-1$, and let A be an $n \times n$ symmetric real matrix.

If A is positive definite, then we can apply Theorem 8.2.5 to deduce that $A = P^t P$ for some invertible matrix P. Then $\det A = (\det P)^2 > 0$. Since A_{n-1} is positive definite (as can be seen by restricting the form to the subspace $W \subset \mathbb{R}^n$ of vectors whose n-th component is zero), we can apply the inductive hypothesis to deduce that $\det A_k > 0$ for $k = 1, \ldots, n-1$. This proves one direction.

Suppose that $\det A_k > 0$ for $k = 1, \ldots, n$. By induction, A_{n-1} defines a positive definite form on the subspace W described above. Therefore, $A_{n-1} = Q^t Q$ for some invertible $(n-1) \times (n-1)$ matrix. Another way of saying this is that there exists an orthonormal basis $\{w_1, \ldots, w_{n-1}\}$ of W with change of basis matrix Q so that $A_{n-1} = Q^t I Q$. Extend this basis to an orthogonal basis of $\mathbb{R}^n$ in the usual way: let u be in the complement of W and let $v = u - \pi(u)$, where π is the orthogonal projection to W. Such a projection exists because the form defined by A is non-degenerate since $\det A \neq 0$. In this way, we obtain an orthogonal basis $\{w_1, \ldots, w_{n-1}, v\}$. Thus, there is a change of basis matrix P such that $A = P^t D P$, where D is diagonal and has $(n-1)$ ones on the diagonal and, after possibly rescaling v, $d_{nn} \in \{-1, 0, 1\}$. Since $\det D = (\det A)(\det P)^2 > 0$, we must have $d_{nn} = 1$. Therefore, $A = P^t P$, and so by Theorem 8.2.5, A is positive definite.

8.4.21 Prove Sylvester's Law: The signature of symmetric form on a real vector space or of a Hermitian form on a complex vector space does not depend on the choice of orthogonal basis.

Hint: Begin by showing that if W_1 and W_2 are subspaces of V and if the form is positive definite on W_1 and negative semi-definite on W_2, then W_1 and W_2 are independent, i.e. $W_1 + W_2$ is a direct sum.

Solution: Suppose that $\mathbf{B} = (v_1, \ldots, v_d)$ and $\mathbf{B'} = (v'_1, \ldots v'_d)$ are two ordered orthogonal bases for a real/complex vector space V equipped with a symmetric/Hermitian form $\langle \, , \rangle$. Suppose that the bases are ordered so that the matrices M and M' of the form have positive entries, followed by negative entries, followed by zero entries along the diagonal. Let (p, n, z) and (p', n', z') be the signatures of these matrices. Since these matrices are in reduced row echelon form, we can see that the ranks are equal to $d - z$ and $d - z'$. As we have seen previously, the ranks of M and M' are equal since there is an invertible $d \times d$ matrix S such that $S^*MS = M'$. Therefore, $z = z'$. We will show that $p = p'$ and, hence, that $n = n'$. Suppose to the contrary that $p > p'$. Then $n < n'$. Let P be the subspace spanned by $\{v_1, \ldots, v_p\}$, so that $\langle\, , \rangle$ is positive definite on P. Let N' be the subspace spanned by $\{v'_{p'+1}, \ldots, v'_{n'}\}$, so that $\langle\, , \rangle$ is negative definite on N'. Let Z and Z' be the subspaces spanned by the last $z = z'$ vectors of the bases $\mathbf{B}$ and $\mathbf{B}'$, respectively. If there were a vector v in $Z - Z'$, then the span of $Z' \cup \{v\}$ would be a vector space on which the form was zero, contradicting the fact that the dimension of such a subspace is at most $d - z = d - z'$. Therefore, $Z = Z'$. Consider $W = (P + Z) \cap (N' + Z')$. This is a vector space of dimension at least $z + 1$. If $w \in W - Z$, then $w \in P \cap N'$. Since $\langle w, w\rangle$ is both positive definite and negative definite on $P \cap N'$, we must have $w = 0$. This implies that the dimension of W is z, which is a contradiction. Therefore, $p = p'$ and $z' = z'$.

Note: The proof is simpler if we assume there are no zeroes on the diagonal, i.e. the nullspace is zero. The proof can be somewhat simplified by using the notion of a quotient vector space. The vector space $V/Z = V/Z'$ is the vector space of cosets of $Z = Z'$. The form descends to V/Z because it vanishes identically on Z. And on V/Z, the nullspace of the form is zero.

8.5.2 Let W be a subspace of a Euclidean space V. Prove that $W = W^{\perp\perp}$.

Solution: If $w \in W$ and $f \in W^\perp$, then $\langle w, f\rangle = 0$ and so w is orthogaonal to every such f. This proves that $W \subset W^{\perp\perp}$. Since V is Euclidean, $V = W \oplus W^\perp$ and $V = W^\perp \oplus W^{\perp\perp}$. It follows that W and $W^{\perp\perp}$ have the same dimension and therefore are equal. Note: We used the assumption that V is finite dimensional.

It is trickier to make this work for an infinite dimensional vector space.

8.5.3 Let $w \in \mathbb{R}^n$ be a vector of length 1, and let U denote the orthogonal space $w^\perp$. The reflection r_w about U is defined by $r_w(v) = -cw + u$, where $v = cw + u$ is the unique way to write $v \in \mathbb{R}w \oplus U$, where $c \in \mathbb{R}$ and $u \in U$.

(a) Prove that $P = I - 2ww^t$ is orthogonal
Solution: Check that $P^t = P$ and $P^tP = I - 4ww^t + 4ww^t = I$.

(b) Prove that multiplication by P is a reflection about U.

Solution: Let $v \in \mathbb{R}^n$. Write $v = cw + u$ as above. Then $w^t v = w^t(cw) = cw^t w = c$ since w has length 1 and $w^t u = 0$ since $U = w^{\perp}$. Computing, we have that

$$Pv = v - 2ww^t v = v - 2wc = -cw + u = r_w(v).$$

(c) Let u, v be vectors of equal length in $\mathbb{R}^n$. Determine a vector w such that $Pu = v$.

Solution: A picture helps. Let $w = u - v$, normalized to be length 1. One can verify algebraically that this works. But it is obvious that this works from a geometric perspective.

8.6.1 Let T be a linear operator on a Hermitian space V, and let T^* be the adjoint operator. Prove that T is Hermitian if and only if $\langle Tv, w\rangle = \langle v, Tw\rangle$ for all $v, w \in V$. And prove that T is unitary if and only if $\langle Tv, Tw\rangle = \langle v, w\rangle$ for all $v, w \in V$.

Solution: Let A be the matrix of T with respect to an orthonormal basis. By definition, T is Hermitian if and only if A is Hermitian, i.e. $A^* = A$. The condition $\langle Tv, w\rangle = \langle v, Tw\rangle$ holds if and only if $(Av)^*w = v^*A^*w = v^*Aw$. This condition holds for all $v, w \in V$ if and only if $A^* = A$ by the usual argument: choose standard basis vectors $v = e_i$ and $w = e_j$ to deduce equality of the (i, j) entry of both A^* and A.

Similarly, by definition, T is unitary if and only if A is unitary, i.e. $U^*U = I$. The condition $\langle Tv, Tw\rangle = \langle v, w\rangle$ holds if and only if $(Av)^*Aw = v^*(A^*A)w = v^*w$. As above, the usual argument shows that this holds if and only if $A^*A = I$.

8.6.2 Let T be a symmetric operator on a Euclidean space. Using Proposition 8.6.9, i.e. T has the property that

$$\langle Tv, w\rangle = \langle v, T^*w\rangle = \langle v, Tw\rangle,$$

prove that if v is a vector such that $T^2v = 0$, then $Tv = 0$.

Solution: If $T^2v = 0$, then $\langle T^2v, v\rangle = 0$. Therefore, $\langle Tv, T^*v\rangle = \langle Tv, Tv\rangle = 0$. But the form is definite; hence, $Tv = 0$.

The result above generalizes as follows: if $T^{2^k}v = 0$ for some $k \geq 1$, then $Tv = 0$. As above, $\langle T^{2^{k-1}}v, T^{2^{k-1}}v\rangle = 0$. Therefore, $T^{2^{k-1}}v = 0$.

By induction, on k (where the base case of $k = 1$ is above) $Tv = 0$. Moreover, if $T^m v = 0$ for some $m \geq 1$, then $T^{2^m} v = 0$; and so, by what was just proved, $Tv = 0$.

8.6.3 What does the Spectral Theorem tell us about a real 3×3 matrix that is both symmetric and orthogonal?

Solution: If A is symmetric and orthogonal, then $A^t = A = A^{-1}$. Therefore, $A^2 = I$. The Spectral Theorem for symmetric operators implies that there is an orthogonal matrix P such that $P^t AP = \Lambda$ is diagonal. Squaring this and using $P^t = P^{-1}$, we find that $\Lambda^2 = P^{-1}P = I$. Therefore, the diagonal entries of Λ are square roots of 1. So, the only eigenvalues of A are 1 and -1. Let's analyze these possibilities when A is a 3×3 matrix. If there are three 1's, then A is conjugate (by P) to I and hence is I. If there are two 1's and one -1, then A is conjugate to the reflection of $\mathbb{R}^3$ in the xy-plane. Therefore, A, itself, is a reflection in a 2-dimensional subspace, namely the image of the xy-plane under P^{-1} (provided the 1's along the diagonal of Λ appear in the first two places). If there is one 1 and two -1's, then A is conjugate to the 180 degree rotation of the xy-plane with the z-axis as its axis of rotation. Therefore, A itself, is a 180 degree rotation in a 2-dimensional subspace. Finally, if there are three -1's, then A is conjugate to $-I$ and hence is equal to $-I$.

8.6.4 What can be said about a matrix A such that A^*A is diagonal?

Solution: Let $A = (v_1, \ldots, v_n)$, where $v_1, \ldots, v_n \in \mathbb{C}^{n \times 1}$ are the columns of A viewed as column vectors. To say that $A^*A = \Lambda$ is diagonal means that $\{v_1, \ldots, v_n\}$ are orthogonal vectors in $\mathbb{C}^n$ with respect to the standard positive definite Hermitian form. In particular, Λ has real entries, each being positive unless the corresponding vector v_i is zero.

8.6.5 Prove that if A is a real skew-symmetric matrix, then $i\,A$ is a Hermitian matrix. What does the Spectral Theorem tell us about a real skew-symmetric matrix?

Solution: We have that $(iA)^* = -iA^* = -iA^t$ because A has real entries. Since A is skew-symmetric, $-iA^t = iA$. Therefore, $(iA)^* = iA$, i.e. iA is Hermitian.

The Spectral Theorem says there is a unitary matrix U such that $U^*(iA)U = \Lambda$ is diagonal and has real entries. Therefore,

$U^*AU = -i\Lambda$ has pure imaginary entries. Therefore, the eigenvalues of a skew-symmetric matrix are pure imaginary numbers.

8.6.6 Prove that an invertible matrix A is normal if and only if A^*A^{-1} is unitary.

Solution: If A is normal and invertible, then $A^*A = AA^*$ implies that

$$(A^*A^{-1})^*A^*A^{-1} = (A^*)^{-1}AA^*A^{-1} = I,$$

and so A^*A^{-1} is unitary. Conversely, if

$$(A^*)^{-1}AA^*A^{-1} = (A^*A^{-1})^*A^*A^{-1} = I,$$

then multiplying on the left and right by A^* and A, respectively, we have that $AA^* = A^*A$ so that A is normal.

8.6.12 Find a unitary matrix P so that P^*AP is diagonal when

$$A = \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}.$$

Solution: To diagonalize the matrix, we look for a basis of eigenvectors. To make sure that P is unitary, we need to normalize the eigenvectors to have length one. That the eigenvectors will be orthogonal follows from the Spectral Theorem: A is Hermitian and so is diagonalizable.

One finds that the eigenvalues are $\lambda = 0, 2$. When $\lambda = 0$, the vector $v_1 = [1/\sqrt{2}, i/\sqrt{2}]^t$ is a unit vector in the kernel of $\lambda I - A = -A$. When $\lambda = 2$, the vector $v_2 = [-1/\sqrt{2}, i/\sqrt{2}]^t$ is in the kernel of $\lambda I - A$. Let $P = [v_1, v_2]$, i.e.

$$P = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ i/\sqrt{2} & i/\sqrt{2} \end{pmatrix}$$

Then

$$P^*AP = \begin{pmatrix} 1/\sqrt{2} & -i/\sqrt{2} \\ -1/\sqrt{2} & -i/\sqrt{2} \end{pmatrix} \begin{pmatrix} 0 & -2/\sqrt{2} \\ 0 & 2i/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$$

8.6.13 Find a real orthogonal matrix P so that P^tAP is diagonal when A is one of the matrices below.

(a)

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Solution: As in the previous problem, we find a basis of eigenvectors and normalize them to have length 1. By the spectral theorem for symmetric operators, the eigenspaces will be orthogonal.

One finds that the eigenvalues are $\lambda = -1, 3$. The unit vectors $v_1 = [1/\sqrt{2}, 1/\sqrt{2}]^t$ and $v_2 = [1/\sqrt{2}, -1/\sqrt{2}]^t$ eigenvectors, respectively. Let $P = [v_1, v_2]$. Then

$$P^tAP = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 3/\sqrt{2} & -1/\sqrt{2} \\ 3/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}$$

(b)

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

The characteristic polynomial factors as $\lambda^2(\lambda - 3)$, so $\lambda = 0, 3$ are eigenvalues, with $\lambda = 0$ having a 2 dimensional eigenspace. To find an orthogonal basis of the 2-dimensional eigenspace, choose one eigenvector and then solve a linear equation to find the other. The following vectors work: $w_1 = [1, -1, 0]^t$, $w_2 = [-1, -1, 2]^t$. The vector $w_3 = [1, 1, 1]^t$ spans the other eigenspace. We normalize these vectors to length 1 to obtain v_1, v_2, v_3 and let $P = [v_1, v_2, v_3]$. The verification that this works is similar to the above. Here is the matrix P:

$$P = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{6} & 1/\sqrt{3} \\ -1/\sqrt{2} & -1/\sqrt{6} & 1/\sqrt{3} \\ 0 & 2/\sqrt{6} & 1/\sqrt{3} \end{pmatrix}$$

(c)

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

The characteristic polynomial is $\lambda^3 - 2\lambda^2 + 1$. You can see that $\lambda = 1$ is a root. And the polynomial factors as $(\lambda - 1)(\lambda^2 - \lambda - 1)$. The other two eigenvalues are

$a = (1+\sqrt{5})/2$ and $b = (1-\sqrt{5})/2$. We find that $v_1 = [0,1,0]^t$ is a unit eigenvalue corresponding to $\lambda = 1$. And we find that $w_2 = [a,0,1]^t$ and $w_3 = [b,0,1]^t$ are eigenvectors corresponding to $\lambda = a, b$, respectively. After normalizing w_2 and w_3 to v_2 and v_3 and setting $P = [v_1, v_2, v_3]$ we have that

$$P = \begin{pmatrix} 0 & a/\sqrt{a^2+1} & b/\sqrt{b^2+1} \\ 1 & 0 & 0 \\ 0 & 1/\sqrt{a^2+1} & 1/\sqrt{b^2+1} \end{pmatrix}$$

9.3.3 Prove that every great circle in SU_2 is a coset of one of the longitudes.

Solution: Every great circle C is the intersection of a 2 dimensional subspace $W \subset \mathbb{R}^4$ with $S^3 = \{x \in \mathbb{R}^4 \mid \|x\| = 1\}$. Let w_1, w_2 be an orthonormal basis of W. We may choose w_2 to lie on the equator since the equator is the intersection of S^3 with a three dimensional subspace. So $w_2 = a\,\mathbf{i} + b\,\mathbf{j} + c\,\mathbf{k}$. Let $w_1 = x_0\,I + x_1\,\mathbf{i} + x_2\,\mathbf{j} + x_3\,\mathbf{k}$. We are given that w_1 and w_2 are orthogonal; therefore, $ax_1 + bx_2 + cx_3 = 0$. To see that C is a coset of a longitude, we multiply on the left by $w_1^{-1} = w_1^* = x_0\,I - x_1, \mathbf{i} - x_2\,\mathbf{j} - x_3\mathbf{k}$. Each element of C has the form $\cos\theta w_1 + \sin\theta w_2$. Each element of $w_1^* C$ has the form $\cos\theta I + \sin\theta w_1^* w_2$. But

$$w_1^* w_2 = (ax_1 + bx_2 + cx_3) + e = 0 + e,$$

for some e in the equator. Therefore, $w_1^* C$ has the form of a longitude. (Viewing the multiplication of the matrices as multiplication of unit quaternions greatly simplifies the above computation.)

9.3.4 Determine the centralizer of $\mathbf{j}$ in SU_2.

Solution: The matrix $\mathbf{j}$ has rows $(0,1)$ and $(-1,0)$. Given an arbitrary matrix A in SU_2 with rows (a,b) and $(-\overline{b}, \overline{a})$, the condition that A commutes with $\mathbf{j}$ implies (after a straight-forward computation) that $a = \overline{a}$ and $b = \overline{b}$. Therefore, a and b must be real. Therefore, the centralizer of $\mathbf{j}$ is the longitude containing $\mathbf{j}$. For, these matrices have the form $\cos\theta I + \sin\theta j$, which corresponds to the first row of A being equal to $(\cos\theta, \sin\theta)$ (with no imaginary components).

Freshman's Dream: Prove that in the ring $R = \mathbb{Z}/n\mathbb{Z}$ that $(a+b)^n = a^n + b^n$ for each $a, b \in R$ provided that n is a prime. Is the dream true if n is not prime? What if n is a power of a prime?

Solution: The usual proof by induction of the binomial theorem goes through for commutative rings. Let R be a commutative ring. Let $a, b \in R$ and let n be a positive integer. Let $C(n, k)$ denote the binomial coefficient $C(n, k) = n(n-1)\cdots(n-k+1)/k!$, which is defined for $0 \le k \le n$. The binomial theorem says that

$$(a+b)^n = \sum_{k=0}^{n} C(n, k)a^{n-k}b^k.$$

Clearly $(a+b)^1 = a+b$ and $C(n, 0) = C(0, n) = 1$, and so the statement is true for $n = 1$. Assuming the statement holds for $n-1$, we expand

$$(a+b)^n = (a+b)(a+b)^{n-1} = (a+b)\sum_{k=0}^{n-1} C(n-k, k)a^{n-k}b^k$$

using the distributive law and grouping like terms. Applying the identity $C(m, j-1) + C(m, j) = C(m+1, j)$, where $1 \le j \le m$, and the "boundary conditions" $C(n, 0) = C(0, n) = 1$ completes the proof.

Now suppose that $R = \mathbb{Z}/n\mathbb{Z}$ and that n is prime. Then $C(n, k) = n(n-1)\ldots n-k+1/k!$, where $1 \le k \le n-1$ is a multiple of n since n is not divisible by any of the factors of $k!$ in the denominator. Therefore, $C(n, k)$ is congruent to 0 modulo n. And, so the only terms which are non-zero in the expansion of $(a+b)^n$ are the first and last terms $k = 0, n$, i.e. $(a+b)^n = a^n + b^n$.

The same argument applies if n is a power of a prime since not every factor of the prime in the numerator is canceled with some factor in the denominator. But this only proves that $(a+b)^n$ is congruent to $a^n + b^n$ modulo p, where $n = p^m$, a power of a prime p. This is different than being congruent to $a^n + b^n$ modulo n. And, indeed, the "dream" is no longer true. Let $n = 4$. Then $(1+1)^4$ is congruent to 0 modulo 4. But $1^4 + 1^4 = 2$ is not congruent to 0 modulo 4.

If n is not a power of a prime, then the statement is false. For example, in $\mathbb{Z}/6\mathbb{Z}$, $(2+1)^6$ is congruent to 3 modulo 6. But $2^6 + 1^6$ is congruent to 5 modulo 6.

11.1.1 Prove that $7 + \sqrt[3]{2}$ and $\sqrt{3} + \sqrt{-5}$ are algebraic numbers.

Solution: Let $\alpha = 7 + \sqrt[3]{2}$. Then $(\alpha - 7)^3 = 2$, so that α is a root of $(x-7)^3 - 2 \in \mathbb{Z}[x]$.

Let $\beta = \sqrt{3} + \sqrt{-5} = \sqrt{3} + i\sqrt{5}$. Then $\beta^2 = (3-5) + 2i\sqrt{15} = -2 + 2i\sqrt{15}$. Therefore, $(\beta^2+2)^2 = -60$. Hence, β is a root of $(x^2+2)^2 + 60 \in \mathbb{Z}[x]$.

11.1.3 Let $R = \mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing $\mathbb{Q}$ and $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. Let $\gamma = \alpha + \beta$. Is $R = \mathbb{Q}[\gamma]$? Is $S = \mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\gamma]$?

Solution: We have that $\gamma^3 = 11\sqrt{2} + 9\sqrt{3}$. Thus, $2\sqrt{2} = \gamma^3 - 9\gamma$. Since $1/2 \in \mathbb{Q}$, it follows that $R \subset \mathbb{Q}[\gamma]$; the opposite inclusion is obvious.

The above argument does not work over the integers. But, perhaps we need to consider higher powers of γ:

γ^2	$5 + 2\sqrt{6}$
γ^3	$11\sqrt{2} + 9\sqrt{3}$
γ^4	$49 + 20\sqrt{6}$
γ^5	$109\sqrt{2} + 89\sqrt{3}$
γ^6	$485 + 198\sqrt{6}$

We observe (and can prove— but won't!! — using induction) that the even powers of γ have even multiples of $\sqrt{6}$ and the odd powers of γ have odd multiples of both $\sqrt{2}$ and $\sqrt{3}$.

Suppose that $\sqrt{2} \in \mathbb{Z}[\gamma]$. Then, since $\mathbb{Z}[\gamma]$ is the set of polynomials in γ with integer coefficients, we would have that

$$\sqrt{2} = a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_n\gamma^n$$

for some non-negative integer n. Gathering like terms, we would have that $\sqrt{2} = A + B\sqrt{2} + C\sqrt{3} + D\sqrt{6}$ for some integers A, B, C, and D. But since $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{6}$ are linearly independent over $\mathbb{Z}$, this means that $B = 1$ and $C = 0$. But B and C must have the same parity (even/odd) because each time they appear in a power of γ they have the same parity. Therefore, $\sqrt{2} \notin \mathbb{Z}[\gamma]$.

Note: The proof as written is incomplete since the fact that $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{6}$ are linearly independent over $\mathbb{Z}$, while perhaps easy to believe, requires proof. Here is the missing step: $a\sqrt{2} + b\sqrt{3} + c\sqrt{6} = 0$ with $a, b, c \in \mathbb{Z}$ implies that $2a^2 + 3b^2 + 2ab\sqrt{6} = 6c^2$ which implies that $\sqrt{6}$ is rational, which is a contradiction.

11.1.6 Decide whether S is a subring of R.

(a) $S = \{r \in \mathbb{Q} \mid r = a/b; a, b \in \mathbb{Z}; 3 \nmid b\}$ and $R = \mathbb{Q}$.

Solution: This is a subring. Given $r = a/b, s = c/d \in S$, then $r - s = \frac{ad-bc}{bd}$. It suffices to show that $3 \nmid bd$ to show that $r - s \in S$. If $3 \mid bd$, then $3 \mid b$ or $3 \mid d$ since 3 is prime. But 3 does not divide b or d, and so 3 does not divide bd.

We have that $rs = (ac)/(bd)$. As already shown above, $3 \nmid bd$, and so $rs \in S$. Finally, $1 \in S$. This completes the proof that S is a subring of R.

(b) S is the set of linear combinations of functions in the set $\{1, \cos(nt), \sin(nt) \mid n \in \mathbb{Z}\}$ and R is the set of real valued functions of t.

Solution: This is not a subring. Let $f(t) = \cos t$ and $g(t) = \sin t$. Then $(fg)(t) = \frac{1}{2}\sin(2t)$ by the double angle formula for sine. This function cannot be an integer linear combination of functions in the set above. For instance, those functions are linearly independent over R as can be seen by using the positive definite symmetric bilinear form $\langle f, g\rangle = \int_0^\pi (fg)(t)\,dt$. It follows that there is only one way to write fg as an $\mathbb{R}$ linear combination of these functions. And so there is at most one way to write these as a rational linear combination. In particular, since we have one such linear combination using non-integer coefficients, there are none using integer coefficients.

Note: The solution given above presumes some familiarity with the inner product used when considering Fourier series. The problem will be graded very leniently since you may not have seen these ideas before.

11.1.8 Determine the units in $R = \mathbb{Z}/n\mathbb{Z}$, $n \geq 2$.

Solution: If $\overline{a} \in R$ and there exists $\overline{b} \in R$ such that $\overline{ab} = 1$, then $\overline{a}$ has a representative $0 \leq a' < n$ that is coprime (relatively prime) to n. Here is a proof of this: if there is a prime p that divides a' and n, then $p < n$ and there are integers $0 < k < a'$ and $0 < \ell < n$ such that $a' = pk$ and $n = p\ell$. Therefore,

$$\overline{0} = (\overline{\ell a})\,\overline{b} = \overline{\ell}\,(\overline{ab}) = \overline{\ell}$$

But this means that n divides ℓ, which is impossible since $0 < \ell < n$.

On the other hand, if $\overline{a}$ is coprime to n, then we can choose a representative $0 \leq a' < n$ and apply the Euclidean algorithm to find integers k and ℓ such that $ka' + \ell n = 1$. Therefore, $\overline{k\overline{a}} = \overline{1}$.

Thus, have proven that $\overline{a}$ is a unit if and only if $\overline{a}$ has a representative $0 \leq a' < n$ that is coprime to n.

Note: To say that a' is a representative of $\overline{a}$ means that $\overline{a'} = \overline{a}$. If b is any representative of $\overline{a}$, then $b - a = kn$ for some integer k. It follows that b is coprime to n if and only if a is coprime to n; for if p is a prime dividing b and n, then p divides $a = b - kn$. And analogously, if p is a prime dividing a and n, then p divides $b = a + kn$. So it may seem that there is no reason to use representatives at all; however, you do need to use representatives (at least for the proof I have given) since the argument uses facts about *integers*, not facts about eqvuivalence classes of integers such as $\overline{a}$.

11.2.2 Let F be a field and let $R = F[[t]]$ be the ring of formal power series over F. Show that R is indeed a ring and determine the units of R.

Solution: Let $f, g \in R$. It is clear that $f + g \in R$ by the way in which addition is defined and using the fact that F is closed under addition. The product fg has coefficients c_k, where

$$c_k = \sum_{i+j=k} a_i b_j,$$

where a_i and b_i are the coefficients of f and g, respectively. Since the above sum is finite and F is closed under sums and products, $fg \in R$. The

To see that the remaining axioms holds requires some patience. It is worthwhile to at least think about how one would show that the distributive law holds. (You need to work with the formula displayed above.)

The units in R are precisely those f for which the constant term, a_0, is non-zero. For if $a_0 = 0$, then fg has leading coefficient $c_0 = a_0 b_0 = 0 \neq 1$. But if $a_0 \neq 0$, then we can construct an inverse g as follows: let $b_0 = a_0^{-1}$. Thus, $c_0 = a_0 b_0 = 1$. We want $c_k = 0$ for all $k > 0$. We have that $c_1 = a_0 b_1 + a_1 b_0$. We have already defined b_0. Let b_1 be the solution to the equation $0 = a_0 b_1 + a_1 b_0$, which exists because we need to and can divide by a_0. In general, $c_k = a_0 b_k + \cdots + a_k b_0$. The terms b_i for $i = 1, \ldots, k-1$ will have already been defined. And we define b_k to be the unique solution to the equation $0 = a_0 b_k + \cdots + a_k b_0$ which exists because we can divide by a_0.

11.5.1 Let $f = x^4 + x^3 + x^2 + x + 1$ and let α denote the residue of x in $R = \mathbb{Z}[x]/(f)$. Write $(\alpha^3 + \alpha^2 + \alpha)(\alpha^5 + 1)$ in terms of the basis $(1, \alpha, \alpha^2, \alpha^3)$ of R

Solution: Since $(x^5 - 1) = (x - 1)(x^4 + x^3 + x^2 + x + 1) = (x - 1) \cdot f$, we have that $\alpha^5 + 1 = (\alpha - 1) + 2 = 2$ in R. So, the given expression above is equal to $2\alpha^3 + 2\alpha^2 + 2\alpha$.

11.5.4 Determine the structure of the ring $R' = \mathbb{Z}[\alpha]$, where α is the element adjoined and satisfying the relations below.

(a) $2\alpha = 6$, $6\alpha = 15$.

Solution: We prove that $R' \cong \mathbb{Z}_3$. Since $6\alpha = 18 = 15$, we have that $3 = 0$ in R'. In particular, if the ideal I generated by $2x - 6$ and $6x - 15$ in $\mathbb{Z}[x]$ is equal to $(3, 2x - 6, 6x - 15)$. We first kill the element 3 to deduce that $R' \cong \mathbb{Z}_3[x]/(2x)$. Since 2 is a unit, we have that $(2x) = (x)$ in $\mathbb{Z}_3[x]$. So, $R' \cong \mathbb{Z}_3$.

Here is another proof: let $\phi : \mathbb{Z}[x] \to \mathbb{Z}_3$ be given by $\phi(n) = \overline{n} \in \mathbb{Z}_3$ and $\phi(x) = \overline{0}$. Clearly, $I \subset \ker \phi$. Conversely, if $f \in \ker \phi$, then we divide by x to write $f = xq + r$, where $r \in \mathbb{Z}$. Since $\phi(f) = 0$, $a_0 \equiv 0 \mod 3$ and so $a_0 = 3a$ for some $a \in \mathbb{Z}$. As in the first paragraph above, we have that $3 \in I$. And since $x = 2(2x - 6) + (-x + 4)(3)$, we have that $x \in I$. And so, $p(x) = xq + 3a \in I$. Therefore, $I = \ker \phi$.

(b) $2\alpha - 6 = 0, \alpha - 10 = 0$

Solution: If we first kill $x - 10$, we have that $\mathbb{Z}[x]/(2x - 6, x - 10)$ is isomorphic to $\mathbb{Z}/(20 - 6) = \mathbb{Z}/14\mathbb{Z}$.

Another way to say this is as follows:
$14 = (1)2x - 6 + (-2)(x - 10)$ and
$2x - 6 = (1)(14) + (2)(x - 10)$, so

$$(14, x - 10) = (2x - 6, x - 10).$$

The ring $\mathbb{Z}[x]/(14, x - 10)$ is isomorphic to $\mathbb{Z}/14\mathbb{Z}$, where the residue of x is $\overline{10}$.

(c) $\alpha^3 + \alpha^2 + 1 = 0, \alpha^2 + \alpha = 0$

Solution: Since $1 = (1)(x^3 + x^2 + 1) + (-x)(x^2 + x)$, we have that

$$(x^3 + x^2 + 1, x^2 + x) = (1).$$

Therefore, the quotient ring is the zero ring.

11.5.5 Is there a field F such that $F[x]/(x^2) \cong F[x]/(x^2-1)$?

Solution: Yes. Let $F = \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$. Define a homomorphism $\phi : F[x] \to F[x]/(x^2-1)$ via $\phi(x) = x+1$. (Here, 1 refers to $\overline{1} \in \mathbb{Z}_2$; I will omit the bars.) By the substitution principle, ϕ is a homomorphism extending the composite of the inclusion $\mathbb{Z}_2 \to \mathbb{Z}_2[x]$ and the natural map $\mathbb{Z}_2[x] \to \mathbb{Z}_2[x]/(x^2-1)$. This map is surjective since $\phi(x+1) = x+1+1 = x$. We show that the kernel of ϕ is (x^2). Suppose that $p(x) = a_n x^n + \cdots + a_0 \in F[x]$. Since

$$\phi(x^2) = (x+1)^2 = x^2 + 2x + 1 = 0 \in F[x]/(x^2+1),$$

$\phi(p(x)) = \phi(a_1 x + a_0) = a_1(x+1) + a_0$. If this is equal to zero in $F[x]/(x^2+1)$, then $a_1 = a_0 = 0$. Therefore, $p(x) \in (x^2)$. Conversely, $(x^2) \subset \ker \phi$. By the First Isomorphism Theorem,

$$F[x]/(x^2) \cong F[x]/(x^2+1).$$

11.5.7 Let F be a field and let $R = F[t]$ be the polynomial ring. Let $R' = R[x]/(tx-1)$. Prove that R' can be identified with the ring of Laurent polynomials, i.e. the ring of finite linear combinations of t and t^{-1} where $t^k t^\ell = t^{k+\ell}$ for all $k, \ell \in \mathbb{Z}$.

Solution: The ring of Laurent polynomials in t over F is denoted by $F[t, t^{-1}]$. By definition, its elements are F-linear combinations of integral powers of t where t^0 is identified with $1 \in F$. Multiplication in $F[t, t^{-1}]$ is defined as one would expect.

The ring $R = F[t]$ is a subring of $F[t, t^{-1}]$. By the substitution principle, there is a unique homomorphism $\Phi : R[x] \to F[t, t^{-1}]$ extending the inclusion $R \subset F[t, t^{-1}]$ and mapping x to t^-1. This homomorphism is clearly surjective. And $(tx-1)$ is clearly contained in $\ker \Phi$. However, it seems difficult to apply the first isomorphism theorem since our usual approach using long division does not apply since $tx-1$ is not monic.

*** Update: This can be done, although the output of long division is modified slightly; skip to the end of this solution for the details.

Instead, we let $\phi : R[x]/(tx-1) \to F[t, t^{-1}]$ be defined by $\phi(f(x) + (tx-1)) = \phi(f(x))$. Since $(tx-1) \subset \ker \Phi$, this is well defined.

Next, define a homomorphism $\psi : F[t, t^{-1}] \to R[x]/(tx-1)$ by

$$\psi(\sum a_i t^i) = \sum_{i>0} a_i t^i + a_0 + \sum_{i<0} a_i x^i.$$

It is clear that ψ preserves the additive structure, but it is not obvious that it preserves the multiplicative structure. So, to prove Ψ is a homomorphism, we check that $\psi((\sum a_i t^i)(\sum b_j t^j))$ is congruent modulo $(tx-1)$ to

$$(\sum_{i>0} a_i t^i + a_0 + \sum_{i<0} a_i x^i)(\sum_{j>0} b_j t^j + a_0 + \sum_{j<0} b_j x^j).$$

Indeed, modulo $(tx-1)$, we have that the above product is equal to

$$\sum_{i+j=k<0} a_i b_j t^k + \sum_{i+j=0} a_i b_j + \sum_{i+j=k>0} a_i b_j x^k = \psi((\sum a_i t^i)(\sum b_j t^j)).$$

Given $f(x) \in R[x]$, we can choose $g(x) \in R[x]$ such that

$$g(x) = \sum_{i>0} a_i t^i + a_0 + \sum_{i<0} a_i x^i$$

and $f(x) - g(x) \in (tx-1)$. This is achieved by looking at each monomial $t^j x^k$ appearing in $f(x)$ and replacing it with t^{j-k} if $j-k \geq 0$ or with x^{k-j} if $j-k < 0$.

For such a representative $g(x)$ of $f(x) + (tx-1)$, we have that $\psi(\phi(g(x)) = \psi(\Phi(g(x)) = \psi(\sum a_i t^i) = g(x) + (tx-1)$. Thus, $\psi \circ \phi$ is the identity mapping. This implies that ϕ is injective. Therefore, ϕ is an isomorphism.

*** Here are the details of how to modify long division. The polynomial $tx - 1 \in R[x]$ has leading coefficient $t \in R = F[t]$. Given $f(x,t) \in R[x] = F[t,x]$, we can, by successively eliminating each term of the form $a_{i,j} t^i x^j$ such that $i, j \geq 1$ by subtracting the multiple $a_{i,j}(tx-1)$, write $f(t,x) = q(t,x)(tx-1) + r_1(t) + r_2(x)$, where $r_1(t) \in F[t]$, $r_2(x) \in F[x]$, and the constant term of $r_2(x)$ is zero. If $f(x,t) \in \ker \Phi$, then $r_1(t) + r_2(x) \in \ker \Phi$. This means that $r_1(t) + r_2(t^{-1}) = 0$. This implies that all of the coefficients of both r_1 and r_2 are zero. (Two Laurent polynomials are equal precisely when their coefficients are zero; the zero polynomial has all coefficients equal to zero.) Therefore, $f(x,t)$ is a multiple of $(tx-1)$. Hence, $\ker \Phi = (tx-1)$.

11.7.1 Prove that a finite integral domain (not necessarily containing an identity) is a field.

Solution: Let $R = \{0, r_1, \dots, r_{n-1}\}$ be an enumeration of the elements of R so that $r_i = r_j$ if and only if $i = j$ and $0 \neq r_i$ for any i. Given any nonzero $a \in R$, the mapping $r_i \to ar_i$ is a permutation since R has the cancellation property: $ar_i = ar_j$ if and only if $r_i = r_j$. Thus, this mapping is one-to-one and, since R is finite, onto. By considering this mapping for powers of a, we have that for some k, the mapping $r_i \to a^k r_i$ is the identity mapping. (The positive integer k is the order of the permutation $r_i \to ar_i$ in the symmetric group S_{n-1}.) By re-indexing, we assume that $r_1 = a^k$. Then $r_1 \cdot r_j = r_j$ for all j. Therefore, r_1 is a multiplicative identity for R. Since such an identity is unique if it exists, we can write $r_1 = 1$. If b is a nonzero element of R, then the mapping $r_i \to br_i$ is onto and so there exists a j such that $br_j = r_1 = 1$. Therefore, r_j is an inverse of b. Thus, we have proven the existence of an inverse for any nonzero element. Hence, R is a field.

11.7.3 Is there an integral domain with exactly 15 elements?

Solution: No. By the previous problem, such an integral domain R would be a field. Let n be the least positive integer such that $na = 0$ for all $a \in R$. Such an n exists because R is a finite abelian group under addition. It follows from Lagrange's Theorem that n is a divisor of $|R| = 15$. More precisely, given $a \in R$, the subgroup generated by a has cardinality equal to the order of a; so, by Lagrange's Theorem, the order of a is a divisor of $|R|$. In particular, $15a = 0$ for all $a \in R$. Since 3 and 5 are elements of R (because $1 \in R$ since R is a field), the equation $3(5a) = 0$ implies that $3 = 0$ or $5a = 0$ for all a. So, $3a = 0$ for all $a \in R$ or $5a = 0$ for all $a \in R$. However, $|R| = 15$. Cauchy's theorem implies the existence of elements of order 3 and order 5. But this is impossible since 3 and 5 are coprime.

The subtle point in the above argument is that $1 \in R$ and $1 \neq 0 \in R$, where 0 is the identity of the additive group R.

The above argument generalizes to show that if F is a finite field, then $|F|$ must be a power of a prime number p. Here is the argument. Given $|F| = n$, we have that $na = 0$ for all $a \in F$. If $n = k\ell$ for some pair of coprime integers $k, \ell > 1$, then as above, since $k, \ell \in F$, either $ka = 0$ for all $a \in F$ or $\ell a = 0$ for all $a \in F$. But since $k, \ell > 1$ are coprime, we can select prime divisors p and q of k and ℓ, respectively; by Cauchy's theorem, there exists elements in F of order exactly p and q. But this contradicts $ka = 0$ or $\ell a = 0$ for all a. Therefore, each proper divisor of n must have the same prime divisors. Therefore, n is a power of a prime.

11.7.5 Let S be a subset of an integral domain R and assume that $0 \notin S$ and that S is closed under multiplication. Let R_S be the set of S-fractions, i.e. equivalence classes of fractions of the form a/b, where $b \in S$. Prove that R_S is a ring.

Solution: Let $a, b \in R$ and $c, d \in S$. Then $a/c - b/d = (ad - bc)/(cd)$ and $(a/c)(b/d) = (ab)/(cd)$ are well-defined because $cd \in S$. This is because the equivalence relation on fractions, namely $a/c \sim b/d$ if $ad = bc$, is the same one we used to prove the operations of addition and multiplication are well-defined in the field of fractions of R. Thus, we have shown that R_S is a subring of the field of fractions of R.

11.8.1 Which principal ideals in $\mathbb{Z}[x]$ are maximal?

Solution: Consider $I = (f(x))$, where $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, $a_n \neq 0$. We may assume that $f(x)$ is irreducible and not a unit since units and reducible elements do not generate maximal principal ideals.

If $n = 0$, then $f(x) = p$, where p is a prime. (We may assume $p > 0$ by replacing $f(x)$ with $-f(x)$. Consider the ideal $J = (p, x)$. Then $I \subsetneq J \subsetneq \mathbb{Z}[x]$ since $x \neq I$ and $1 \neq J$. It is clear that $x \neq I$ since every element of I has the form $p \cdot g(x)$ for some $g(x) \in \mathbb{Z}$ and so every coefficient is divisible by p. To see that $1 \notin J$, we observe that if $1 = p \cdot g(x) + xh(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$, then $1 = pb_0$, where b_0 is the constant coefficient of $g(x)$; this is not possible, and so $1 \notin J$.

If $n > 0$, then choose a prime p which does not divide a_n. Since $f(x)$ has degree $n > 0$, $p \notin I$. To see that $J = (f(x), p)$ is not all of $\mathbb{Z}[x]$, consider the quotient ring $\mathbb{Z}[x]/J$. We see this is isomorphic to $\mathbb{F}_p[x]/(f(x))$. This quotient is not the zero ring since p does not divide the leading coefficient of $f(x)$. Therefore, J is a proper ideal of $\mathbb{Z}[x]$.

11.8.3 Prove that $\mathbb{F}_2[x]/(x^3 + x + 1)$ is a field but that $\mathbb{F}_3[x]/(x^3 + x + 1)$ is not a field.

Solution: $x^3 + x + 1$ is irreducible since neither 0 nor 1 is a root; any proper factorization of a cubic must contain a linear factor and hence the polynomial would be a root. Therefore $(x^3 + x + 1)$ is maximal and so the first ring above is a field.

The polynomial $x^3 + x + 1$ is not irreducible over $\mathbb{F}_3$ since 1 is a root. Therefore, $(x^3 + x + 1)$ is not maximal and so the second ring above is not a field.

12.1.2 (*partial fractions*)

Write $7/24$ in the form $a/8 + b/3$.

Solution: This is equivalent to solving the equation $7 = 3a + 8b$ since we will need a common denominator of 24. Since $\gcd(3, 8) = 1$, we can find $x, y \in \mathbb{Z}$ such that $3x + 7y = 1$ and then multiply this by 7. Indeed, $3(3) + 8(-1) = 1$ and so $3(21) + 8(-7) = 7$. So, $a = 21$ and $b = -7$ are solutions.

There are many other solutions. Indeed, $3(3 + 8m) + 8(-1 - 3m) = 1$ for every integer m. Conversely, if $3x + 8y = 1$, then $3x \equiv 1 \pmod 8$ and so $x \equiv 3 \pmod 8$. To see this, note that $x \in \mathbb{Z}/8\mathbb{Z}$ must be a unit and so we only need to check which values in $\{1, 3, 5, 7\}$ solve the equation. Trial and error shows that $x = 3$ is the only solution in this set.

(b) Prove that if $n = uv$ and u and v are relatively prime, then $q = m/n$ can be written as $q = a/u + b/v$.

Solution: As in (a), the problem involving fractions is equivalent to finding a solution to $m = av + bu$. Since u and v are relatively prime, there exist integers x and y such that $ux + vy = 1$. Therefore, $m = v(my) + u(mx)$. Hence, $a = my$ and $b = mx$ are solutions.

12.1.3 (*Chinese remainder theorem*)

(a) Let m and n be relatively prime integers, and let a and b be arbitrary integers. Prove that there is an integer x that solves the simultaneous congruence $x \equiv a \pmod m$ and $x \equiv b \pmod n$.

Solution: We are looking for an integer x such that $x = a + km$ and $x = b + \ell n$ for some $k, \ell \in \mathbb{Z}$. If $a = b$, then we can take $k = \ell = 0$ so that $x = a = b$ is a solution.

We may assume hence forth that $a \neq b$. Subtracting the two equations above, we have that

$$0 = a - b + km - \ell n.$$

And, re-writing, we have that

$$(b-a) = mk + n(-\ell).$$

We can solve this equation just as we did in the previous problem. Since m and n are relatively prime, there exist integers λ and μ such that $m\lambda + n\mu = 1$. Multiply through by the non-zero integer $(b-a)$. Then, it is clear that if $k = \lambda(b-a)$ and $-\ell = \mu(b-a)$, then $x = a + km = b + \ell n$ solves the simultaneous congruences. Thus,

$$x = a + m\lambda(b-a) = b + n\mu(a-b)$$

is a solution. The above formula is also correct if $a = b$.

(b) Determine all of the solutions to the above simultaneous congruences.

Solution: Suppose that x_1 and x_0 are solutions to the simultaneous congruences. Then $(x_1 - x_0)$ is both congruent to 0 modulo m and congruent to 0 modulo n. Since m and n are relatively prime, $(x - 1 - x_0)$ is congruent to 0 modulo mn. (Proof: $x_1 - x_0 = km$ and $n \mid km$ together with $\gcd(m, n) = 1$ implies that $n \mid k$. Therefore, $x_1 - x_0 = \ell mn$ for some $\ell \in \mathbb{Z}$.) Moreover, if x_0 is a solution to the simultaneous congruences and $\ell \in \mathbb{Z}$, then $x_1 = x_0 + \ell mn$ is also a solution: it is congruent to x_0 modulo m and to x_0 modulo n.

Thus, we have proved that the set of solutions to the simultaneous congruences is

$$\{x_0 + \ell mn \mid \ell \in \mathbb{Z}\},$$

where x_0 is a particular solution.

12.1.4 Solve the following systems of equations:

(a) $x \equiv 3 \pmod 8$, $x \equiv 2 \pmod 5$

Solution: Since $1 = (-3)(8) + (5)(5)$ and $b - a = 2 - 3 = -1$, we find that $x_0 = 3 + (3)(8) = 27$ is a solution. Therefore, all other solutions are of the form $x_0 = 27 + 40t$ for some integer t by the previous problem.

(b) $x \equiv 3 \pmod{15}$, $x \equiv 5 \pmod{8}$, $x \equiv 2 \pmod{7}$

Solution: Since $1 = (-1)(15) + 2(8)$ and $b - a = 5 - 3 = 2$, we find that $x_0 = 3 + (-2)(15) = -27$ is a solution to the first two congruences. To find a solution to the last congruence, we can add multiples of $15 \times 8 = 120$ until we find one. Indeed, $93 = -27 + 120$ satisfies, $93 \equiv 2 \pmod{7}$. Therefore, all other solutions are of the form $x_0 = 93 + 840t$.

(c) $x \equiv 13 \pmod{43}$, $x \equiv 7 \pmod{71}$

Solution: Since $1 = (-33)(43) + (20)(71)$ and $b - a = 7 - 13 = -6$, we find that $x_0 = 13 + (-6)(-33)(43) = 8527$ is a solution. Therefore, all other solutions are of the form $x_0 = 8527 + 3053t$ for some integer t by the previous problem. (For a solution in $[0, 3053]$, let $x_0 = 2421$.)

12.2.1 Factor into irreducibles in $\mathbb{F}_p[x]$:

(a) $x^3 + x^2 + x + 1$, $p = 2$

Solution: Since $3 \equiv 1 \pmod{2}$, we see that $(x+1)^3$ is equal to the polynomial above. And $x + 1$ is clearly irreducible.

(b) $x^2 - 3x - 3$, $p = 5$

Solution: $(x + 3)(x + 4) = x^2 + 7x + 12 = x^2 + 2x + 2 = x^2 - 3x - 3$ in $\mathbb{F}_5$. And $(x + 3)$ and $(x + 4)$ are irreducible.

(c) $x^2 + 1$, $p = 7$

Solution: $\mathbb{F}_3 = \{0, 1, 2, 3, -3, -2, -1\}$, and we can check that $x^2 + 1 \neq 0$ if $x \in \{0, \pm 1, \pm 2, \pm 3\}$ in $\mathbb{F}_3$. Therefore, $x^2 + 1$ is irreducible, for otherwise it would have a linear factor and therefore a root (since we are working in a field).

12.2.2 Compute the gcd of $x^6 + x^4 + x^3 + x^2 + x + 1$ and $x^5 + 2x^3 + x^2 + x + 1$ in $\mathbb{Q}[x]$.

Solution: Observe that

$$x^6+x^4+x^3+x^2+x+1 = (x^2+1)x^4+(x^2+1)x+(x^2+1)(1) = (x^2+1)(x^4+x^2+1).$$

We find that $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$. These two factors are irreducible in $\mathbb{Q}[x]$ since the roots are imaginary.

And observe that

$$x^5+2x^3+x^2+x+1 = (x^2+1)x^3+(x^2+1)x+(x^2+1)(1) = (x^2+1)(x^3+x+1).$$

We see that x^2+1 and x^3+x+1 are irreducible in $\mathbb{Q}[x]$: the first because the roots are imaginary and the second because it has no rational roots (as the only possibilities are ± 1).

We have thus found factorizations into irreducbiles. Since $\mathbb{Q}[x]$ is a UFD, we have that x^2+1 is the gcd.

The above is not the intended solution. For that, you should use the Euclidean algorithm. But the above solutions illustrates the familiar method of finding the gcd by factoring into primes.

12.2.3 How many roots does the polynomial x^2-2 have modulo 8?

Solution: None. We can verify this by letting x range over the elements of $\mathbb{Z}/8\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, 4 = -4\}$ and verifying that x^2-2 is never equal to zero.

12.2.5 (*partial fractions for polynomials*)

(a) Prove that every element of $\mathbb{C}(x)$ can be written as a sum of a polynomial and a $\mathbb{C}$-linear combination of functions of the form $1/(x-a)^k$, where $k \in \mathbb{N}$.

Solution: We will prove this in several steps. We assume the fundamental theorem of algebra so that every polynomial in $\mathbb{C}[x]$ factors into a product of linear factors or is a constant polynomial.

STEP 1: Suppose that $f(x), g(x) \in \mathbb{C}[x]$ have no common root. Then $f(x)$ and $g(x)$ have no common divisors of degree greater than zero. Therefore, $f(x)$ and $g(x)$ are relatively prime. Since $\mathbb{C}[x]$ is a PID, there exist $a(x), b(x) \in \mathbb{C}[x]$ such that

$$a(x)f(x) + b(x)g(x) = 1.$$

STEP 2: Let $f(x) \in \mathbb{C}(x)$ so that $f(x) = p(x)/q(x)$ for some $p(x), q(x) \in \mathbb{C}[x]$ with $q(x) \neq 0$. We will prove that $f(x)$ is equal to a polynomial plus a $\mathbb{C}[x]$-linear combination of functions of the form $1/(x-a)^k$.

We may assume that $p(x)$ and $q(x)$ have no common roots, for otherwise we could reduce the fraction. We may also assume that $q(x)$ has degree greater than 0, for otherwise $f(x)$ is a polynomial and we are done.

If the degree of $p(x)$ is greater than or equal to $q(x)$, we can perform long division so that $p(x) = g(x) + h(x)/q(x)$ for polynomials $g(x), h(x) \in \mathbb{C}[x]$ where $h(x)$ has smaller degree than $q(x)$ or $h(x)$ is zero.

If $h(x)$ is a zero, then we are done: $f(x)$ is a polynomial.

If $h(x)$ is nonzero, let r be a root of $q(x)$. And write $q(x) = (x-r)^k t(x)$ where $t(x) \in \mathbb{C}[x]$ and $t(r) \neq 0$. By STEP 1, there exist $a(x), b(x) \in \mathbb{C}[x]$ such that $a(x)(x-r)^k + b(x)t(x) = 1$. Therefore,

$$\frac{1}{q(x)} = \frac{a(x)}{t(x)} + \frac{b(x)}{(x-r)^k}.$$

And so,

$$f(x) = \frac{p(x)}{q(x)} = g(x) + \frac{h(x)}{q(x)} = g(x) + \frac{a(x)h(x)}{t(x)} + \frac{b(x)h(x)}{(x-r)^k}.$$

If $t(x)$ above is a constant polynomial, then we are done with STEP 2. Otherwise, $t(x)$ has fewer distinct roots than $q(x)$. We can then apply mathematical induction on the number of distinct roots of the denominator. The base case is trivial.

STEP 3: We have now expressed $f(x)$ as a polynomial plus as $\mathbb{C}[x]$-linear combination of functions of the form $1/(x-a)^k$. Moreover, the coefficients of the functions do not have a as a root, for otherwise we could reduce the fraction.

So, it remains to show that if $s(x) \in \mathbb{C}[x]$, $a \in \mathbb{C}$, $s(a) \neq 0$, and $k \in \mathbb{N}$, then $s(x)/(x-a)^k$ is a polynomial plus a $\mathbb{C}$-linear combination of function of the form $1/(x-a)^j$. By performing long-division, we can reduce the degree of $s(x)$ below that of k at the expense of introducing a polynomial summand. Since $1, (x-a), (x-a)^2, \ldots, (x-a)^{k-1}$ forms a basis of the vector space of polynomial of degree less than k, we can write $s(x)$ uniquely as

$$s(x) = A_k + A_{k-1}(x-a) + \cdots + A_1(x-a)^k,$$

for some $A_1, \ldots, A_k \in \mathbb{C}$. Therefore,

$$\frac{s(x)}{(x-a)^k} = \frac{A_k}{(x-a)^k} + \cdots + \frac{A_1}{(x-a)}.$$

This completes the proof.

(b) Find a basis for the field $\mathbb{C}(x)$ as a $\mathbb{C}$-vector space.

Solution: By part (a), $\mathbb{C}$ is spanned by polynomials together with all functions of the form $1/(x-a)^k$. The polynomials are spanned by $1, x, x^2, \ldots$. We claim that

$$\{x^k \mid k \in \{0\} \cup \mathbb{N}\} \cup \{(x-a)^{-k} \mid a \in \mathbb{C}, k \in \mathbb{N}\}$$

is a basis for $\mathbb{C}(x)$ as a $\mathbb{C}$-vector space.

It remains to show these are linearly independent. Suppose that

$$\sum_{i=0}^{M} c_i x^i + \sum_{j=1}^{N} \frac{b_j}{(x-a_j)^{k_j}} = 0.$$

Suppose that $a \in \{a_j \mid 1 \leq j \leq N\}$. Let $k = k_*$ be the maximum of $\{k_j \mid a_j = a\}$. Multiply the above equation by $(x-a)^k$ and then let $x = a$. The resulting equation is $b_* = 0$. It follows that $b_j = 0$ whenever $a_j = a$. Since a was arbitrary, $b_j = 0$ for each $j = 1, \ldots, N$. Thus, the above equation is a linear combination of $1, x, x^2, \ldots, x^M$. Therefore, $c_0 = c_1 = \cdots = c_M = 0$. This completes the proof.

12.2.6 Prove that the following rings are Euclidean domains.

(a) $\mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3}$.

Solution: The ring is an integral domain since it is a subring of the field of complex numbers. We use the norm $N(z) = |z|^2 = a^2 + b^2$, where $z = a + bi \in \mathbb{C}$. We have that $N(zw) = N(z)N(w)$ for all $z, w \in \mathbb{C}$.

Suppose that $\alpha, \beta \in R = \mathbb{Z}[\omega]$ and $\alpha \neq 0$. We are to show that there are elements $q, r \in R$ such that $\beta = \alpha q + r$, where $r = 0$ or $N(r) < N(\alpha)$. Let $q' = \beta/\alpha \in \mathbb{C}$. Let $q \in R$ be an element which is closest to q'. We claim that if $r = \beta - \alpha q$, then $N(r) < N(\alpha)$. Since

$$N(r) = N(\beta - \alpha q' + \alpha q' - \alpha q) = N(0 + \alpha(q' - q)) = N(\alpha)N(q' - q),$$

it remains to show that $N(q' - q) < 1$. This is clear from a sketch of the lattice R: the lattice points lie at the vertices of the equilateral triangle tiling of the plane with fundamental domain (a generating tile of the tiling) having vertices 0, 1, and $1+\omega$. The point farthest from these vertices is the centroid, which is $(0+1+(1+\omega))/3 = (2+\omega)/3$. It follows that

$$N(q'-q) \leq N((2+\omega)/3) = (4+\omega\overline{\omega})/9 = 5/9 < 1.$$

(b) $\mathbb{Z}[\sqrt{-2}]$.

Solution: The proof is the same as in part (a) except for the last part where we consider the lattice. The lattice in this case is rectangular: the lattice points lie at the vertices of the tiling of the plane with fundamental domain a rectangle with vertices 0, 1, $\sqrt{2}i$, $1+i\sqrt{2}$. The point farthest from these vertices is again the centroid, which is $(1+i\sqrt{2})/2$. Since this has norm equal to $3/4 < 1$, this ring is also a Euclidean domain.

12.2.7 Let $a, b \in \mathbb{Z}$. Prove that the gcd of a and b in $\mathbb{Z}$ is the same as their gcd in $\mathbb{Z}[i]$.

Solution: Let d be the gcd of a and b in $\mathbb{Z}$ and let e be the gcd of a and b in $\mathbb{Z}[i]$. Both $\mathbb{Z}$ and $\mathbb{Z}[i]$ are PID's, and so there exist $x, y \in \mathbb{Z}$ and $w, z \in \mathbb{Z}[i]$ such that $d = ax+by$ and $e = aw+bz$. Since d divides a and b in $\mathbb{Z}$, d divides both in $\mathbb{Z}[i]$. Therefore, from the equation $e = aw+bz$, we have that d divides e in $\mathbb{Z}[i]$. Since e divides a and b in $\mathbb{Z}[i]$ and since the equation $d = ax+by$ is true in $\mathbb{Z}[i]$, we have that e divides d in $\mathbb{Z}[i]$. Thus, there exist $q_1, q_2 \in \mathbb{Z}[i]$ such that $e = q_1 d$ and $d = q_2 e$. Therefore, $e = q_1 q_2 e$. Since $e \neq 0$, $1 = q_1 q_2$ and so both q_1 and q_2 are units. Therefore, d and e are associates. And so the gcd's coincide in $\mathbb{Z}[i]$. (The gcd is only defined up to associates.)

12.2.8 Describe a systematic method for performing long division in $\mathbb{Z}[i]$ and apply your method to to divide $4+36i$ by $5+i$.

Solution:

12.3.1 Let $\phi : \mathbb{Z}[x] \to \mathbb{R}$ be given by (a) $\phi(x) = 1+\sqrt{2}$ or (b) $\phi(x) = \frac{1}{2}+\sqrt{2}$. In each case, determine whether the kernel of ϕ is a principal ideal. If the answer is yes, then give a generator.

Solution: Both homomorphisms, say ϕ_1 and ϕ_2, have the effect of evaluating a polynomial $f(x) \in \mathbb{Z}$ at the given value, say $a_1 = 1+\sqrt{2}$ or $a_2 = \frac{1}{2}+\sqrt{2}$, respectively. So, $f(x)$ is in the kernel of ϕ_i precisely, when $f(a_i) = 0$.

We claim that if a_i is a root, then so is it's conjugate, where $\overline{a_1} = 1 - \sqrt{2}$ and $\overline{a_2} = \frac{1}{2} - \sqrt{2}$. One way to see this is observe that there is a homomorphism $\psi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ given by $\psi(a + b\sqrt{2}) = a - b\sqrt{2}$, where $a, b \in \mathbb{Q}(\sqrt{2})$. The image of each ϕ_i is contained in $\mathbb{Q}(\sqrt{2})$.

Suppose that $\phi_i(f(x)) = 0$, where $f(x) \in \mathbb{Z}[x]$. Then $\psi(\phi(f(x))) = 0$. This implies that $\overline{a_i}$ is a root of $f(x)$ also.

Therefore, if $f(x) \in \ker \phi_1$, then the monic polynomial

$$(x - 1 - \sqrt{2})(x - 1 + \sqrt{2}) = (x-1)^2 - 2 = x^2 - 2x - 1$$

is a factor of $f(x)$. Clearly if this is a factor of some $f(x)$, then $f(x)$ belongs to $\ker \phi_1$. Therefore, the kernel of ϕ_1 is the principal ideal $(x^2 - 2x - 1)$.

If $f(x) \in \ker \phi_2$, we might hope to use the same approach:

$$(x - \frac{1}{2} - \sqrt{2})(x - \frac{1}{2} + \sqrt{2}) = (x - \frac{1}{2})^2 - 2 = x^2 - x - \frac{7}{4}.$$

So, we hope that $4x^2 - 4x - 7 \in \mathbb{Z}[x]$ is a generator for $\ker \phi_2$.

If $4x^2 - 4x - 7$ is a factor of $f(x)$, then $f(x) \in \ker \phi_2$. If $f(x) \in \ker \phi_2$, then by the above, $4x^2 - 4x - 7$ is a factor of $f(x)$ in $\mathbb{Q}[x]$ (because we can perform divison using rational coefficients. Now apply Gauss's Lemma. The polynomial $4x^2 - 4x - 7$ is primitive. And so, Gauss's Lemma applies and we can conclude that since it is a divisor of $f(x)$ in $\mathbb{Q}[x]$ that it is also a divisor of $f(x)$ in $\mathbb{Z}[x]$. Therefore, $\ker \phi_2$ is the principal ideal $(4x^2 - 4x - 7)$.

12.3.2 Prove that two polynomials in $\mathbb{Z}[x]$ are relatively prime in $\mathbb{Q}[x]$ if and only if they generate an ideal in $\mathbb{Z}[x]$ which contains an integer.

Solution: If $f, g \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}$ is such that $n \in (f, g) \subset \mathbb{Z}[x]$, then we have that $n = a(x)f(x) + b(x)g(x)$ for some $a(x), b(x) \in \mathbb{Z}[x]$. Therefore, in $\mathbb{Q}[x]$, we can divide this equation by n to write 1 as a $\mathbb{Q}[x]$-linear combination of f and g. Therefore, f and g are relatively prime.

Conversely, if f and g are relatively prime in $\mathbb{Q}[x]$, then 1 is a $\mathbb{Q}[x]$-linear combination of f and g. By clearing denominators, we obtain an integer in $(f, g) \subset \mathbb{Z}[x]$.

12.3.3 State and prove a version of Gauss's Lemma for Euclidean domains.

Solution: The usual definitions involved are as follows: if $f(x) \in R[x]$, the *content* of $f(x)$ is the gcd of the coefficients of $f(x)$. For this to make sense, we need to work in a ring in which the gcd always exists for $a, b \in R$, not both zero. Let's assume that R is a Euclidean domain. In particular, R has gcd's, is commutative, and has 1. We say that $f(x)$ is *primitive* if it has content 1. The generalization of Gauss's Lemma is that if $f(x)$ and $g(x)$ are primitive in $R[x]$, then $f(x)g(x)$ is primitive.

In a Euclidean domain, primes and irreducibles coincide. (This is true, more generally, in any PID.) In particular, the gcd of a pair of elments $a, b \in R$ is not 1 if and only if there is a prime p such that p divides both a and b.

Suppose p is a prime dividing some coefficient of $f(x)g(x)$. If $f(x)$ and $g(x)$ are primitive, then both have a smallest index coefficient which is not divisible by p. Let $a_0, \ldots, a_n$ and $b_0, \ldots, b_m$ be the coefficients of $f(x)$ and $g(x)$, resepectively. So, we have p divides $a_0, \ldots, a_{i-1}$ and p divides $b_0, \ldots, b_{j-1}$, but p does not divide a_i or b_j. But then, p does not divide the coefficient of x^{i+j}: this coefficient is $b_{i+j}a_0 + \cdots + b_j a_i + \cdots + b_0 a_{i+j}$ (where coefficients exceeding the degree of the polynomials are understood to be zero). All of these terms except $b_j a_i$ are divisible by p. And so this coefficient cannot be divisible by p. This contradiction proves Gauss's Lemma.

The above proof was the same as one of the proofs presented in class. The other proof also can be adopted to this context. If $f(x)$ and $g(x)$ have content zero, and $f(x)g(x)$ did not, then we could consider the image of $f(x)g(x)$ in $R/(p)[x]$, where p is a prime dividing the coefficients of $f(x)g(x)$. Since p is prime and R is a PID, p is irreducible. Since R is a PID, it follows that (p) is a maximal ideal: any overideal is a principal and so a generator is a divisor of p. Therefore $F = R/(p)$ is a field and therefore, $F[x]$ is an integral domain. Thus, the image of $f(x)$ or the image of $g(x)$ must be zero. This means that p divides all the coefficients of $f(x)$ or all the coefficients of $g(x)$. This is a contradiction and so Gauss's Lemma is proved.

12.4.1 (a) Factor $x^9 - x$ and $x^9 - 1$ in $\mathbb{F}_3[x]$.

Solution: By looking for a difference of squares, we can factor

$x^9 - x$ over $\mathbb{Z}[x]$ as follows:

$$x(x^8-1) = x(x^4-1)(x^4+1) = x(x^2-1)(x^2+1)(x^4+1) =$$

$$x(x-1)(x+1)(x^2+1)(x^4+1).$$

The polynomial x^2+1 is irreducible in $\mathbb{F}_3[x]$ since it has no roots in $\mathbb{F}_3$. The other irreducible quadratic polynomials in $\mathbb{F}_3[x]$ are x^2+x-1, x^2-x+1, and x^2-x-1. One finds that

$$(x^2+x-1)(x^2-x-1) = (x^2-1)^2 - x^2 = x^4+1$$

in $\mathbb{F}_3$. Thus,

$$x^9 - x = x(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1).$$

The polynomial $(x-1)^9$ has coefficients $\binom{9}{k}$ for $k = 0, \ldots, 9$. except for the first and last, these are all multiples of 3. Therefore, $(x-1)^9 = x^9 - 1$ in $\mathbb{F}_3[x]$.

(b) Factor $x^{16} - x$ in $\mathbb{F}_2[x]$.

Solution: $x^{16} - x = x(x^{15}-1) = x(x-1)(x^{14}+x^{13}+\cdots+x+1)$. Attempting to divide by the irreducible quadratic polynomial x^2+x+1, we find a factorization

$$x(x+1)(x^2+x+1)(x^{12}+x^9+x^6+x^3+1).$$

At this point, one might try to divide by other irreducible polynomials in $\mathbb{F}_2[x]$. Neither of the irreducible cubic polynomials divides $x^{12}+x^9+x^6+x^3+1$. But the first quartic irreducible polynomial on p. 373, x^4+x^3+1 does. One then finds a complete factorization as follows:

$$x(x+1)(x^2+x+1)(x^4+x^3+1)(x^4+x+1)(x^4+x^3+x^2+x+1).$$

This is not a very satisfying solution. But, perhaps the point is that we are being asked to factor an element into prime factors, a task we already know from experience is very difficult over the ring of integers.

A idea might be the following: factorization in $\mathbb{F}_2[x]$ seems simliar to factoring integers given by a binary representation. The polynomial $x^{12}+x^9+x^6+x^3+1$, when $x=2$, represents the integer 4681 which has 31 and 151 its only prime factors. The polynomial $x^4+x^3+x^2+x+1$, when $x=2$, represents 31. And so, $x^4+x^3+x^2+x+1$ is a divisor in $\mathbb{F}_2[x]$.

12.4.2 Prove that the following polynomials are irreducible:

(a) $x^2 + 1 \in \mathbb{F}_7[x]$.
Solution: It has no roots in $\mathbb{F}_7$.

(b) $x^3 - 9$ in $\mathbb{F}_{31}[x]$.
Solution: It has no roots in $\mathbb{F}_{31}$. To see this, we can use the following trick. Suppose that $a \in \mathbb{F}_{31}$ were a root. Then $a^3 \equiv 9 \pmod{31}$ and so $a^{30} \equiv 9^{10} \pmod{31}$. By Euler's theorem (using $\phi(31) = 30$ since 31 is prime), $a^{30} \equiv 1 \pmod{31}$. On the other hand, $9^{10} = 3^{20}$. We find that $3^3 = 27 \equiv -4 \pmod{31}$ and, therefore, $3^5 \equiv -36 \equiv -5 \pmod{31}$. Therefore, $3^{10} \equiv 25 \equiv -6 \pmod{31}$. And, therefore, $3^{20} \equiv 36 \equiv 5 \pmod{31}$. Since 1 is not congruent to 5 modulo 31, there is no solution to the equation $x^3 = 9$ in $\mathbb{F}_{31}$.

12.4.3 Decide whether or not the polynomial $x^4 + 6x^3 + 9x + 3$ generates a maximal ideal in $\mathbb{Q}[x]$.

Solution: We can apply Eisenstein's Criterion with $p = 3$ to deduce that this polynomial is irreducible. Since $\mathbb{Q}[x]$ is a PID, an ideal generated by an irreducible element is a maximal ideal.

12.4.4 Factor the polynomial $x^5 + 2x^4 + 3x^3 + 3x + 5$ modulo 2, modulo 3, and in $\mathbb{Q}$.

Solution: Modulo 2, the polynomial is $x^5 + x^3 + x + 1$ which is equal to $(x+1)(x^4 + x^3 + 1)$. The polynomial $x^4 + x^3 + 1$ has no linear factors since it has no roots in $\mathbb{F}_2$. The only quadratic irreducible polynomials in $\mathbb{F}_2[x]$ is $x^2 + x + 1$. And we can verify that $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Therefore $x^4 + x^3 + 1$ is irreducible. Incidentally, there is an easy way to compute the square of a polynomial in $\mathbb{F}_2[x]$: the identity

$$(a_1 + \cdots + a_n)^2 = \sum_{i=1}^{n} a_i^2 + 2 \sum_{1 \le i < j \le n} a_i a_j$$

implies that $(a_1 + \cdots + a_n)^2 = a_1^2 + \cdots + a_n^2$ in $\mathbb{F}_2$.

Modulo 3, the polynomial is $x^5 + 2x^4 + 2$. Since -1 is a root modulo 3, we find a factorization $(x+1)(x^4 + x^3 + 2x^2 + x + 2)$. Again -1 is a root, and we factor again: $(x+1)^2(x^3 + 2x + 2)$. Since neither 1 nor -1 is a root of $x^3 + 2x + 2$ modulo 3, this factor is irreducible (as a reducible cubic polynomial must have a root when the coefficient ring is a field).

Finally, in $\mathbb{Q}[x]$, we see that -1 is a root and find that the polynomial factors as

$$(x+1)(x^4+x^3+2x^2-2x+5).$$

The factor $x^4+x^3+2x^2-2x+5$ is congruent to x^4+x^3+1 modulo 2. This is an irreducible polynomial in $\mathbb{F}_2$. We can now apply Proposition 12.4.3: since $p=2$ does not divide the leading coefficient of $x^4+x^3+2x^2-2x+5$ and since its residue is irreducible in $\mathbb{F}_p[x]$, it must be irreducible in $\mathbb{Q}[x]$.

12.4.9 For which primes p and which integers n is the polynomial x^n-p irreducible in $\mathbb{Q}[x]$?

Solution: We will assume that $n \geq 1$. Then $f(x)=x^n-p$ is irreducible for any prime p. This follows from Eisenstein's criterion: p does not divide the leading coefficient, p divides all other coefficients, and p^2 does not divide the constant coefficient.

12.4.15 Suppose that $f(x) \in \mathbb{Z}[x]$. Let p be a prime and let $\overline{f}(x)$ be the residue of $f(x)$ in $\mathbb{F}_p[x]$. What can be said about the irreducibility of $f(x)$ when $\overline{f}(x)$ satisfies the given conditions below and one considers a criterion similar to Eisenstein's Criterion?

(a) Suppose $\overline{f}(x)$ is constant. Thus, p divides every coefficient of $f(x)$ except possibly the constant coefficient. If p divides all coefficients, then $f(x)$ factors as $p \cdot \frac{1}{p} f(x)$ and is therefore reducible. If p does not divide the constant coefficient and p^2 does not divide the leading coefficient, then we can apply Eisenstein's criterion to $g(x)=\sum_{k=0}^{n} a_{n-k}x^k$, where $f(x)=\sum_{k=0}^{n} a_k x^k$. If $f(x)$ were reducible, then $g(x)$ would be reducible. Therefore, $f(x)$ is irreducible. If p^2 divides the leading coefficient, then we cannot deduce that $f(x)$ is irreducible; for example,

$$f(x)=(px+1)^2=p^2x^2+2px+1$$

is reducible and $\overline{f}$ is a constant.

(b) Suppose $\overline{f}(x) = x^n + \overline{b}x^{n-1}$. Let's assume that

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

so that $\overline{a_n} = \overline{1}$, $\overline{a_{n-1}} = b$ and $\overline{a_k} = \overline{0}$ for $k = 1, \ldots, n-2$. If $f(x)$ were reducible, say $f = gh$ for some $g, h \in \mathbb{Z}[x]$, then we may assume that $\overline{g}(x) = x^k$ for some $k \in \{1, \ldots, n-1\}$ and that $\overline{h}(x) = x^{n-k}(x - \overline{b})$.

If $k < n-1$, then both $g(x)$ and $h(x)$ must have a constant coefficient which is congruent to 0 modulo p. It follows that $p^2 \mid a_0$.

If $k = n-1$, then the above need not be true. However, in this case, $\overline{g}(x) = x^{n-1}$ so, in particular, $g(x)$ has degree $n-1$ and therefore $h(x)$ has degree 1. (It is important that we have assumed $f(x)$ to have degree n; in general, the degree of $\overline{f}$ can be strictly less than the degree of f.) Since we have assumed that $f(x)$ is monic, $h(x)$ can be assumed to be monic as well. Therefore, $h(x) = x - c$ for some integer c, where $\overline{c} = \overline{b}$. So, $f(x) = g(x) \cdot (x - b)$ for some integer c such that $c \equiv b \pmod{p}$ in this case.

Thus, we can deduce from the above that if $f(x)$ is monic, p^2 does not divide a_0, and $f(x)$ does not have a root in $\mathbb{Z}$ which is congruent to b modulo p, then $f(x)$ is irreducible in $\mathbb{Z}[x]$ and also in $\mathbb{Q}[x]$ (by Gauss's Lemma).

12.4.16 Factor $x^{14} + 8x^{13} + 3$ in $\mathbb{Q}[x]$.

Solution: We can apply part(b) of the previous problem with $p = 3$. The polynomial has residue $x^{14} + \overline{2}x^{13}$ in $\mathbb{F}_3$. The given polynomial is monic, p^2 does not divide the constant coefficient, and the polynomial does not have a root in $\mathbb{Z}$ which is congruent to 2. The first two claims are clear; the third is true because $f(x)$ does not have any root in $\mathbb{Z}$. We can deduce this from the rational roots theorem and by verifying that none of 1, -1, 3, or -3 is a root of $x^{14} + 8x^{13} + 3$. The only one which is non-trivial to verify is that -3 is not a root:

$$(-3)^{14} + 8(-3)^{13} + 3 = 3 \cdot 3^{13} - 8 \cdot 3^{13} + 3 = -5 \cdot 3^{13} + 3 \neq 0.$$

Therefore, this polynomial is irreducible in $\mathbb{Q}[x]$.

12.5.9 Let $R = \mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3}$. Let p be a prime integer such that $p \neq 3$. Imitate the proof of Theorem 12.5.2 to prove the following statements:

(a) The polynomial $x^2 + x + 1$ has a root in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 3$.

Solution: Let $p \in \mathbb{Z}$ be prime. If $p \equiv 0 \pmod 3$, then $p = 3$. If $p \equiv 1 \pmod 3$, then $3 \mid (p-1) = |\mathbb{F}_p^\times|$, where the latter is the group of units in $\mathbb{F}_p$. By Sylow's theorem, there is an element $a \in \mathbb{F}_p^\times$ of order 3. (Really, we are only using a special case of Sylow's first theorem; this special case is often referred to as Cauchy's theorem.) Therefore, $a^3 - 1$ and $a \neq 1$. From the factorization $x^3 - 1 = (x-1)(x^2 + x + 1)$, we see that a is a root of $x^2 + x + 1$. Therefore, Conversely, if $x^2 + x + 1$ has a root $a \in \mathbb{F}_p$, then $a \neq 0$ (clearly) and $a \neq 1$ (because $p \neq 3$). Therefore, a is a nontrivial element of $\mathbb{F}_p^\times$. Since a has order 3 in this group, 3 is a divisor of the order of this group, i.e. $3 \mid (p-1)$.

(b) The ideal (p) is a maximal ideal in R if and only if $p \equiv -1 \pmod 3$.

Solution: From part (a), we have that $x^2 + x + 1$ is irreducible in $\mathbb{F}_p[x]$ if and only if p is not congruent to 0 or 1 modulo 3. Therefore, $p \equiv -1 \pmod 3$ if and only if $x^2 + x + 1$ is irreducible in $\mathbb{F}_p[x]$. Since $R = \mathbb{Z}[\omega] = \mathbb{Z}[x]/(x^2 + x + 1)$, we see that $Q = R/(p) \cong \mathbb{Z}_p/(x^2 + x + 1)$. Therefore, Q is a field if and only if $x^2 + x + 1$ is irreducible which is true if and only if (p) is a maximal ideal in Q.

(c) The prime p has a proper factorization in R if and only if $p = a^2 + ab + b^2$ for some $a, b \in \mathbb{Z}$.

Solution: If p factors in R, then p is a product of primes $\pi_1, \dots, \pi_k \in R$. Therefore, $p^2 = p\overline{p} = (\pi_1\overline{\pi_1}) \cdots (\pi_k\overline{\pi_k})$. Since factoriztion into primes in $\mathbb{Z}$ is unique (up to units), $k \leq 2$. So, if p factors in $\mathbb{R}$, then $p = \pi\overline{\pi}$ for some prime $\pi = a - b\omega \in R$, where $a, b \in \mathbb{Z}$. (The choice of the negative sign becomes clear in a moment.) Therefore,

$$p = (a - b\omega)(a - b\overline{\omega} = a^2 + b^2 - ab(\omega + \overline{\omega} = a^2 + b^2 + ab.$$

Conversely, if $p = a^2 + b^2 + ab$ for some integers $a, b \in \mathbb{Z}$, then we can factor p as above in R. The units in R are $\pm 1, \pm\omega, \pm\overline{\omega}$. In terms of the lattice basis $(1, \omega)$ of R, the units are $\pm 1, \pm\omega, \pm(1 + \omega)$. It follows that if $a - b\omega$ were a unit in R, then

$$(a, b) \in \{(\pm 1, 0), (0, \pm 1), \pm(1, -1)\}.$$

Since these possibilities imply that $p = 1$ (not prime) or $p = 3$ (we are assuming $p \neq 3$ in the given statement of the problem), we conclude that $p = (a + b\omega)(a + b\overline{\omega}$ is a proper factorization in R.

13.1.4 Let d and d' be integers. When are the fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d'}$ distinct?

Solution: Suppose that $\sqrt{d} = s \in \mathbb{Z}$. Then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(s) = \mathbb{Q}$. So, this case is straightforward. Suppose that $\sqrt{d} \notin \mathbb{Z}$. Then d can be uniquely expressed in the form $d = n^2 s$, where $n, s \in \mathbb{Z}$, $n > 0$ and s is square-free, meaning that if $m \in \mathbb{Z}$ and $m^2 \notin \{0, 1\}$, then m^2 does not divide s. In particular, s is non-zero. The claim is that the fields coincide precisely when $s = s'$, where $d' = (n')^2 s'$ is the analogous decomposition for an integer d' such that $\sqrt{d'} \notin \mathbb{Z}$.a non-zero integer d'.

To see, this we observe that if $x \in \mathbb{Q}(\sqrt{d})$, then $x = a + b\sqrt{d}$ for some rational numbers a and b. Thus, $x = a + (bn)\sqrt{s} \in \mathbb{Q}(\sqrt{s})$. Since $\mathbb{Q}(\sqrt{s})$ is clearly a subset of $\mathbb{Q}(\sqrt{d})$, these two rings coincide. Analogously, $\mathbb{Q}(\sqrt{d'}) = \mathbb{Q}(\sqrt{s'})$. Therefore, it remains to determine when $\mathbb{Q}(\sqrt{s}) = \mathbb{Q}(\sqrt{s'})$. Clearly these are equal if $s = s'$. If $s \neq s'$, we argue that $\sqrt{s} \notin \mathbb{Q}(\sqrt{s'})$. Suppose to the contrary that $\sqrt{s} = a + b\sqrt{s'}$ for some rational numbers a and b. Squaring both sides and re-arranging we have that $2ab\sqrt{s'} = s - a^2 - b^2 s'$. Unless $a = 0$ or $b = 0$, we have a contradiction since $\sqrt{s'}$ is irrational. If $b = 0$, then the original equation says that $\sqrt{s}$ is rational, which is not true. So, $a = 0$, and therefore $\sqrt{s} = b\sqrt{s'}$. Thus, $s = b^2 s'$. Therefore, b^2 divides s. Since s is square-free, we must have that $b = \pm 1$. Therefore, $\sqrt{s} = \pm\sqrt{s'}$. This can only happen if $s = s'$.

13.2.2 For which negative integers $d \equiv 2 \pmod 4$ is the ring of integers in $\mathbb{Q}[\sqrt{d}]$ a UFD?

Solution: Suppose that d is a negative integer congruent to 2 modulo 4. We can assume that d is square free by the previous exercise. The ring of integers is thus $R = \mathbb{Z}[\sqrt{d}]$ (by Proposition 13.1.6) and the group of units is $\{\pm 1\}$ (by Proposition 13.2.2). Let $\delta = \sqrt{d}$. Let $e = (4 - d)/2 \in \mathbb{Z}$. Then $2e = 4 - d = (2 - \delta)(2 + \delta)$.

We need to decide whether the above factorization is indeed a factoriztaion into irreducibles. If $d = -2$, then it is not since $3 = (1 + \delta)(1 - \delta)$ is not irreducible. In fact, the same argument as was used to show that $\mathbb{Z}[i]$ and $\mathbb{Z}[e^{2\pi i/3}]$ are Euclidean domains works to show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain. Therefore, when $d = -2$, R is a unique factorization domain.

Let $N(a + b\delta) = a^2 - b^2 d$ be the norm in R. By the above, we can assume that $d \leq -6$. In this case, we have that $N(a+b\delta) \geq 1 - d \geq 7$ if $a^2, b^2 \geq 1$. If $a = 0$ and $b = \pm 1$, then $N(a + b\delta) = -d \geq 6$. If $a = \pm 1$ and $b = 0$, then $a + b\delta = \pm 1$ is a unit. If 3 were reducible in R, it would factor as a product of two elements whose norms multiply to $9 = N(3)$. From the above analysis and the fact that norms are non-negative integers, we conclude that 3 is irreducible in R. If R were a UFD, then 3 must divide $(2 + \delta)$ or $(2 - \delta)$. If $3(a + b\delta) = (2 + \delta)$, for some integers a and b, then $3a - 2 = (1 - b)\delta$. Since the right hand side of this equation is irrational, $b = 1$. But this forces $3a - 2 = 0$ and so a is not an integer.

Thus, we have proved that R is not a UFD if $d \equiv 2 \pmod 4$, $d < 0$, and $d \neq -2$.

13.3.2 Let $\delta = \sqrt{-5}$. Decide whether or not the lattice of integer linear combinations of the given vectors is an ideal in $R = \mathbb{Z}[\delta]$.

(a) $(5, 1 + \delta)$

Solution: It is not an ideal. The element $\delta(1 + \delta) = \delta - 5$ is not in the lattice, for if $5a + (1 + \delta)b = \delta - 5$ then $5a + b = -5$ and $b = 1$. Therefore, $a = -6/5$, which is not an integer.

(b) $(7, 1 + \delta)$

Solution: It is not an ideal. The same method as above works.

(c) $(4 - 2\delta, 2 + 2\delta, 6 + 4\delta)$

Solution: It is an ideal. It is easy to see that all elements of the ideal generated by these three elements will be sums of even numbers and even multiples of δ. So, it suffices to show that both 2 and 2δ belong to the lattice. Indeed,
$2 = (-2)(2 + 2\delta) + (1)(6 + 4\delta)$ and
$2\delta = (3)(2 + 2\delta) + (-1)(6 + 4\delta)$.

15.2.2 Let $f(x) = \sum_{k=0}^{n} a_k x^k$ be an irreducible polynomial over a field F. Let α be a root of f in an extension field K. Write $\alpha^{-1} \in K$ in terms of the coefficients of f.

Solution: Because f is irreducible, $a_0 \neq 0$; otherwise, x would divide f. We can solve the equation $f(\alpha) = 0$ for a_0 in K and then divide by a_0, to obtain the following equation:

$$1 = a_0^{-1}(-a_n\alpha^{n-1} - a_{n-1}\alpha^{n-2} - \cdots - a_2\alpha - a_1)\alpha.$$

Thus, α^{-1} is the left factor in the right-hand side of the above equation.

15.3.1 Let F be a field and suppose that $F(\alpha)$ is a degree 5 extension. Prove that $F(\alpha^2) = F(\alpha)$.

Solution: Since $\alpha^2 \in F(\alpha)$, $F(\alpha^2) \subset F(\alpha)$. If it were a proper subfield, then its degree over F would be a proper divisor of 5, namely 1. In this were so, then, $F(\alpha^2) = F$. This would imply that $\alpha^2 \in F$. And, therefore, $x^2 - \alpha^2 \in F[x]$. But then $F(\alpha)$ would be at most a degree 2 extension of F, which is a contradiction. Hence, $F(\alpha^2)$ is not a proper subset of $F(\alpha)$ and so $F(\alpha^2) = F(\alpha)$.

15.3.3 Let $\zeta_n = e^{2\pi i/n}$. Prove that $\zeta_5 \notin \mathbb{Q}(\zeta_7)$.

Solution: The irreducible polynomial for ζ_p, where p is a prime is $x^{p-1} + x^{p-2} + \cdots + x + 1$. (It is irreducible by the $x = y + 1$ trick so that Eisenstein's criterion applies.) Therefore $\mathbb{Q}(\zeta_7)$ is a degree 6 extension of $\mathbb{Q}$. Since 4 is not a divisor of 6, $\mathbb{Q}(\zeta_5)$ cannot be a subfield of $\mathbb{Q}(\zeta_7)$.

15.3.6 Let a be a positive rational number that is not a square in $\mathbb{Q}$. Prove that $\sqrt[4]{a}$ has degree 4 over $\mathbb{Q}$.

Solution: Since a is not a square in $\mathbb{Q}$, $x^2 - a$ has no roots in $\mathbb{Q}$ and is, therefore, irreducible. Therefore, $\mathbb{Q}(\sqrt{a})$ is a degree 2 extension of $\mathbb{Q}$. This extension is a subfield of $\mathbb{Q}(\sqrt[4]{2}$. Therefore, $\mathbb{Q}(\sqrt[4]{2})$ is an even degree extension of $\mathbb{Q}$. It is not a degree 2 extensions, because if it were then it would be equal to $\mathbb{Q}(\sqrt{a})$ and then we would have an equaation

$$\sqrt[4]{2} = p + q\sqrt{a}$$

for some $p, q \in \mathbb{Q}$. Squaring this equation and solving for $\sqrt{a}$ we find that $\sqrt{a} = (p^2 + aq^2)/(1 - 2pq)$. The denominator is not zero; if it were, then $0 = p^2 + aq^2$ implies that $a \leq 0$, contrary to the hypothesis. Thus, the solution for $\sqrt{a}$ reveals that $\sqrt{a}$ is rational, which is also a contradiction. We have prove that the degree of $\mathbb{Q}(\sqrt[4]{2})$ is even and degree at least 4. It has degree equal to 4 because $\sqrt[4]{2}$ is a root of $x^4 - 2$. (We did not need to prove directly that $x^4 - 2$ is irreducible in $\mathbb{Q}[x]$; but one could also solve the problem by doing so.)

15.3.10 Let K/F and L/K be algebraic extensions. Prove that K/F is an algebraic extension.

Solution: Let $\alpha \in K$. We are to show that α is algebraic over F. We will use the **fact** that α is algebraic over F if and only if α belongs to a finite extension of F.

(Proof of this **fact**: If α is a root of an irreducible polynomial $f \in F[x]$ of degree n, then $\alpha \in F(\alpha)$ and $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis; so $F(\alpha)$ has finite dimension over F. Conversely, if $\alpha \in M$, a finite extension of F, then for some $n \in \mathbb{N}$, $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ must be a linearly dependent subset of M, and so there exist scalars $a_0, \ldots, a_n \in F$, not all zero, such that $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} = 0$; and so α is a root of a nonzero polynomial in $F[x]$.)

Since α is algebraic over L, there is a nonzero polynomial $f \in L[x]$ such that $f(\alpha) = 0$. Let $a_0, \ldots, a_n \in L$ be the coefficients of f. Since each a_i is algebraic over F, $F(a_0, \ldots, a_n)$ is a finite extension of F. Since $f \in F(a_0, \ldots, a_n)[x]$, the field $F(\alpha, a_0, \ldots, a_n)$ is a finite exension of F. Therefore, α is algebraic over F.

15.5.2 Prove that the regular pentagon is constructible by (a) field theory and by (b) an explicit construction.

Solution to part (a): The regular pentagon is construtible if and only if $\alpha = \cos 2\pi/5$ belongs to a tower of degree two extensions of $\mathbb{Q}$. A good source of trigonmetric identities can be found by comparing real an imaginary parts in de Moivre's formula:

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin\theta.$$

From this with $n = 5$ and the pythaogrean identity, $\cos^2\theta + \sin^2\theta = 1$, we obtain the following:

$$\cos 5\theta = 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta.$$

To obtain a polynomial relation of degree 4, we will consider the angle $\theta = \pi/10$ and let $\beta = \cos\theta$. The above formula implies that

$$0 = 16\beta^5 - 20\beta^3 + 5\beta = \beta(16\beta^4 - 20\beta^2 + 5).$$

Since $\beta \neq 0$, we have that $0 = 16\beta^4 - 20\beta^2 + 5$, which we can view as a quadratic in β^2. Therefore, $\mathbb{Q}(\beta^2)$ is a quadratic extension of $\mathbb{Q}$.

By using the half-angle formula, we find that $\cos\pi/5 = 2\beta^2 - 1$ and, therefore, by the half-angle formula again, we find that $\alpha = 2(2\beta^2 - 1) - 1 \in \mathbb{Q}(\beta^2)$. Therefore, α is constructible. In fact, we have obtained an exact formula: $\alpha = \frac{1}{4}(\sqrt{5} - 1)$.

15.5.3 Decide whether or not a regular 9-gon is constructible.

Solution: Let $\alpha = \cos 2\pi/9$. The 9-gon is constructible if and only if α is constructible. Let's use a formula involving $\cos 3\theta$. We find (see the previous problem) that

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Use $\theta = 2\pi/9$. Thus, $-\frac{1}{2} = \cos 2\pi/3 = 4\alpha^3 - 3\alpha$. The polynomial $f(x) = 8x^3 - 6x + 1$ is irreducible in $\mathbb{Q}[x]$ (by the rational roots test and the fact that it is cubic). Therefore, $\mathbb{Q}(\alpha)$ is a degree 3 extension of $\mathbb{Q}$. Therefore, α does not belong to a tower of degree 2 extensions of $\mathbb{Q}$. Therefore, the 9-gon is not constructible.

15.6.1 Let F be a field of characteristic zero. Suppose that $g(x) \in F[x]$ is irreducible and is a common divisor of f and f', where $f(x) \in F[x]$. Prove that g^2 divides f.

Solution: We may assume that g has positive degree since the conclusion is clearly true if f has degree zero since F is a field. Since $g \mid f$, there is an $h \in F[x]$ such that $f = gh$. By the product rule, $f' = g'h + gh'$. Since $g \mid f'$ and $g \mid g$, we must have that $g \mid g'h$. Since F has characteristic zero and g has positive degree, g and g' are relatively prime. Since $F[x]$ is a PID, g, being irreducible, is also a prime. Therefore, $g \mid g'h$ implies that $g \mid h$. Therefore, there exists a $k \in F[x]$ such that $h = kg$. Hence, $f = kg^2$ and so $g^2 \mid f$.

15.7.8 The polynomials $f(x) = x^3 + x + 1$ and $g(x) = x^3 + x^2 + 1$ are irreducible over $\mathbb{F}_2$ and so define extensions K and L by adjoining a root of $f(x)$ and $g(x)$, respectively. Give an explicit description of an isomorphism $K \to L$. How many such isomorphisms are there?

Solution: Let $F = \mathbb{F}_2$. Let $M = \mathbb{F}_8$. Since this is a degree 3 extension of F which consists of all of the roots of $x^8 - x$, which has both f and g as factors, we know that both f and g split completely over M and both have exactly 3 roots. (This follows from our previous analysis of M.)

Let $\alpha \in M$ be a root of $f(x)$ and let $K = F(\alpha)$. Similarly, let $\beta \in M$ be a root of $g(x)$ and let $L = F(\beta)$. Any isomorphism $\phi : K \to L$

must take 1 to 1 and so ϕ is the identity when restricted to the prime subfield F. Therefore, ϕ is determined completely by $\phi(\alpha)$ by the substitution principle. (Remember that $F[\alpha] = F(\alpha)$, so the substitution principle applies.)

To be a well-defined homomorphism, we must have that $\phi(\alpha)$ satisfies $f(\alpha) = 0$ in L. Thus, α must map to a root of $f(x) \in L[x]$. And mapping α to a root will necessarily define an isomorphism since the image will be a degree three extension of F and hence is all of L. Therefore, there are exactly 3 such isomorphisms.

We can determine one by brute force since we know all of the elements of L:

$$L = \{0, 1, \beta, \beta + 1, \beta^2, \beta^2 + 1, \beta + \beta^2, 1 + \beta + \beta^2\},$$

where $g(\beta) = 0$.

We find that $\beta + 1$ is a root of $f(x)$:

$$f(\beta + 1) = \beta^3 + \beta^2 + \beta + 1 + \beta + 1 + 1 = \beta^3 + \beta^2 + 1 = 0.$$

Therefore, $\phi(\alpha) = \beta + 1$ defines an isomorphism $K \to L$.

15.3.7 (a) Is i in the field $\mathbb{Q}(\sqrt[4]{-2})$? (b) Is $\sqrt[3]{5} \in \mathbb{Q}(\sqrt[3]{2}$?

Solution to part (a): Let $F = \mathbb{Q}$, $L = F(\sqrt[4]{2})$, and $K = L(i)$. Since $x^4 - 2$ is irreducible over F (by Eisenstein with $p = 2$), $[L : F] = 4$. Since L is a subfield of $\mathbb{R}$, $i \notin L$. Since $x^2 + 1$ is irreducible over L, $[K : L] = 2$ and so $[K : F] = 8$. Let $M = \mathbb{Q}(\sqrt[4]{-2})$. Since $x^4 + 2$ is irreducible over F, $[M : F] = 4$. If $i \in M$, then $M = M(i)$. But we will prove that $M(i) = K$, which provides a contradiction since K has degree 8 over F.

It sufficies to prove that $\sqrt[4]{2} \in M(i)$. Let $\omega = e^{i\pi/4}$. Then $\omega\sqrt[4]{2}$ is a 4th root of -2 since $\omega^4 = -1$. Since $(\sqrt[4]{-2})^2 = \sqrt{-2} = \pm i\sqrt{2}$, it follows that $\sqrt{2} \in M(i)$. And from this, it follows that $\omega = \frac{1}{\sqrt{2}}(1 + i) \in M(i)$. And, therefore, $\sqrt[4]{2} \in M(i)$. Thus, we have shown that $M = K$.

Solution to part (b):

15.7.4 Determine the number of irreducible polynomials of degree 3 over $\mathbb{F}_3$ and over $\mathbb{F}_5$.

Solution: Let p be a prime and let K be the field of $q = p^3$ elements. The elements of K correspond to the roots of $x^q - x$ in some splitting field. If $g(x)$ is an irreducible factors of $x^q - x$, then $\mathbb{F}_p[x]/(g)$ is isomorphic to a subfield of K. Since $[K : \mathbb{F}_p] = 3$, the degree of g must be 1 or 3. There are exactly p irreducible factors of degree 1, each corresponding to an element of $\mathbb{F}_p$. After factoring these from $x^q - x$, we are left with another factor of degree $q - p$. All irreducible factors of this must have degree 3. Therefore, there are $(q - p)/3$ of them.

If $p = 3$, then there are 8; if there are $p = 5$, then there are 40.